



## **Implementación de Infraestructura de Clave Pública (PKI) en Sistemas SCADA**

Alumno: Leonardo Andrés Scussolin

Tutor Técnico: Lic. Jorge Alejandro Kamlofsky

Profesora Trabajo Final: Dra. Marcela Samela

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

(Diciembre, 2024)

---

## Resumen

Los Sistemas de Supervisión, Control y Adquisición de Datos (SCADA) facilitan la gestión, control y supervisión de los sistemas de automatización y control de procesos mediante la recopilación y análisis de datos en tiempo real. Originalmente, estos sistemas fueron diseñados para operar en entornos industriales desconectados de la red IT. Pero en los últimos años ante el avance de los sistemas ERP e Internet las redes IT y OT se integraron, lo que resultó en la falta de capacidad de los componentes SCADA para hacer frente a amenazas propias de las redes empresariales, tales como los ciberataques, el malware y demás peligros, por lo que surgió la necesidad de analizar sus vulnerabilidades para mitigar los potenciales riesgos.

En esta propuesta de intervención en el campo profesional se estudiará el marco demográfico mundial y las revoluciones industriales para explicar las necesidades funcionales que justificaron la convergencia entre las redes IT y OT. Se abordarán las características principales de los sistemas SCADA, sus componentes principales, los protocolos de comunicación más utilizados en la industria, conceptos fundamentales de criptografía y ciberseguridad en entornos industriales.

La propuesta analizará la forma más eficiente de implementar infraestructura PKI en un sistema SCADA, los roles de los usuarios y los circuitos administrativos recomendados para la gestión de certificados digitales, así como también una posible solución para el cifrado de las comunicaciones de los PLC.

*Palabras clave:* IIoT, Industria 4.0, PKI, PLC, Scada

---

## Abstract

Supervisory Control and Data Acquisition (SCADA) systems facilitate the management, control and monitoring of automation and process control systems by collecting and analyzing data in real time. Originally, these systems were designed to operate in industrial environments disconnected from the IT network, but in recent years with the advancement of ERP systems and the Internet, IT and OT networks were integrated, which resulted in the lack of capacity of SCADA components to deal with threats inherent to enterprise networks, such as cyber-attacks, malware and other dangers, so the need arose to analyze their vulnerabilities to mitigate potential risks.

In this proposal for intervention in the professional field of work, the global demographic framework and industrial revolutions will be studied to explain the functional needs that justified the convergence between IT and OT networks.. It will address the main characteristics of SCADA systems, their main components, the most used communication protocols in industry, fundamental concepts of cryptography and cybersecurity in industrial environments.

The proposal will analyze the most efficient way to implement PKI infrastructure in a SCADA system, user roles and recommended administrative circuits for digital certificate management, as well as a possible solution for encrypting PLC communications.

*Keywords:* IIoT, Industry 4.0, PKI, PLC, Scada

---

### **Dedicatoria**

Este trabajo se lo dedico a mi esposa Melina y a mis hijos Delfina, Santino y Mateo por la paciencia y fuerza para lograr este objetivo. También a mis padres Norma y Néstor por la educación brindada y la insistencia para no bajar los brazos y cerrar este ciclo.

---

## **Reconocimientos**

Gracias a la UAI (Universidad Abierta Interamericana) y una gran mención por su dedicación a mi tutor Jorge Kamlofsky y Marcela Samela, docente universitaria quienes fueron los que me guiaron y acompañaron en este proyecto hasta lograr la aprobación de mi trabajo final.

Por último, a mis compañeros de estudio, colegas de trabajo y amistades.

---

## **Estructura General del Trabajo Final**

### **Capítulos**

En el capítulo II, se abordará el estado del arte. Se analizará la información necesaria para el cumplimiento de los objetivos del presente trabajo, abordando en primera instancia las cuestiones relacionadas a las tecnologías IT/OT actuales y la convergencia de las mismas en entornos industriales. Por otro lado, también se abordarán cuestiones de ciberseguridad en sistemas SCADA y las características principales de la infraestructura PKI.

En el capítulo III, se mencionará la evolución histórica demográfica mundial y de qué forma las revoluciones industriales afectaron la ciberseguridad en los entornos industriales. Asimismo, se analizarán diversas estructuras de sistemas SCADA, mencionando sus características principales para luego enfatizar en cuestiones de criptografía y dispositivos de cifrado existentes.

En el capítulo IV, se detallará la propuesta con las acciones a seguir para el cumplimiento de los objetivos primario y secundarios, así como también los recursos necesarios que serán requeridos para la implementación de la infraestructura PKI en un sistema SCADA.

---

## Índice General

<b>Resumen.....</b>	<b>1</b>
<b>Abstract.....</b>	<b>2</b>
<b>Dedicatoria.....</b>	<b>3</b>
<b>Reconocimientos.....</b>	<b>4</b>
<b>Estructura General del Trabajo Final .....</b>	<b>5</b>
<b>Capítulos .....</b>	<b>5</b>
<b>Capítulo 1 - Introducción .....</b>	<b>12</b>
<b>1.1 Descripción del Problema .....</b>	<b>12</b>
<b>1.2 Justificación de la Propuesta .....</b>	<b>12</b>
<b>1.3 Marco Institucional .....</b>	<b>13</b>
<b>1.4 Objetivos del Trabajo Final de Carrera .....</b>	<b>13</b>
<b>1.4.1 Objetivo General.....</b>	<b>13</b>
<b>1.4.2 Objetivos Específicos .....</b>	<b>13</b>
<b>1.5 Contribuciones Principales .....</b>	<b>13</b>
<b>1.6 Metodología de Investigación .....</b>	<b>14</b>
<b>Capítulo 2 – Estado del Arte .....</b>	<b>15</b>
<b>2.1 Tecnologías IT/OT .....</b>	<b>15</b>
<b>2.1.1 Convergencia IT/OT en entornos industriales .....</b>	<b>16</b>
<b>2.1.2 Entornos OT basados en SCADA .....</b>	<b>18</b>
<b>2.1.3 IIoT .....</b>	<b>20</b>
<b>2.2 Ciberseguridad en Entornos Industriales.....</b>	<b>21</b>
<b>2.2.1 Introducción .....</b>	<b>21</b>
<b>2.2.2 Tipos de Ciberataques .....</b>	<b>23</b>
<b>2.2.3 Vulnerabilidades Explotadas en Sistemas de Control Industrial .....</b>	<b>25</b>
<b>2.2.4 Casos de ciberataques en ICS .....</b>	<b>26</b>
<b>2.2.5 Impacto de la Pandemia COVID-19 en la Ciberseguridad .....</b>	<b>28</b>
<b>2.2.6 Mitigación de Riesgos en OT.....</b>	<b>30</b>
<b>Marco de Ciberseguridad en sistemas industriales.....</b>	<b>31</b>
<b>Ciber-resiliencia .....</b>	<b>33</b>
<b>2.3 PKI .....</b>	<b>35</b>
<b>2.3.1 Características Principales.....</b>	<b>35</b>

Microsoft Active Directory Certificate Services.....	38
OpenSSL CA .....	39
2.3.2 Dispositivos criptográficos .....	40
Capítulo 3 – Marco Teórico .....	44
3.1 Introducción .....	44
3.2 Evolución Histórica de los Sistemas IT/OT .....	44
3.3 Marco Demográfico y Revoluciones Industriales .....	45
3.3.1 Industria 4.0.....	50
Niveles de Automatización en la Industria .....	52
3.4 Sistemas SCADA.....	55
3.4.1 Introducción .....	55
3.4.2 Arquitectura y Componentes de Hardware .....	57
HMI .....	57
MTU (Master Terminal Unit).....	58
RTU (Remote Terminal Unit).....	58
Red de Comunicación .....	59
Instrumentos de Campo .....	60
PLC .....	60
3.4.3 OpenScada .....	65
3.5 Principales Protocolos Industriales de Comunicación .....	67
3.5.1 Introducción .....	67
Modelo OSI.....	68
3.5.2 Modbus.....	72
Modbus RTU y ASCII .....	74
Modbus TCP/IP .....	76
Modbus Plus .....	80
3.5.3 DNP3 .....	81
3.5.4 IEC 60870-5-104.....	83
3.5.5 Profibus.....	85
3.6 Criptografía y Dispositivos de Seguridad .....	87
3.6.1 Introducción a la Criptografía.....	87
3.6.2 Algoritmos de Cifrado .....	90
Simétricos.....	90



<b>Asimétricos .....</b>	<b>91</b>
<b>3.6.3 Funciones hash criptográficas.....</b>	<b>93</b>
<b>MD5 .....</b>	<b>95</b>
<b>Familia SHA .....</b>	<b>96</b>
<b>Capítulo 4 – Propuesta de Intervención.....</b>	<b>98</b>
<b>4.1 Introducción .....</b>	<b>98</b>
<b>4.2 Propuesta de implementación PKI en la red SCADA .....</b>	<b>100</b>
<b>4.2.1 Arquitectura de servidores.....</b>	<b>100</b>
<b>4.2.2 Seguridad en las terminales SCADA.....</b>	<b>102</b>
<b>4.2.3 Dispositivos Criptográficos Tokens .....</b>	<b>102</b>
<b>4.2.4 Gestión Administrativa de Certificados Digitales .....</b>	<b>103</b>
<b>4.3 Utilización del Protocolo Modbus TCP/IP con TLS .....</b>	<b>105</b>
<b>4.4 Protección de las Terminales SCADA.....</b>	<b>106</b>
<b>4.5 Concientización al usuario final.....</b>	<b>108</b>
<b>4.6 Recursos a utilizar.....</b>	<b>109</b>
<b>4.7 Cronograma de Tareas .....</b>	<b>109</b>
<b>4.8 Factores Externos Condicionantes .....</b>	<b>110</b>
<b>4.9 Evaluación del Proyecto .....</b>	<b>112</b>
<b>4.9.1 Matriz FODA de la Propuesta de Intervención .....</b>	<b>112</b>
<b>4.9.2 Análisis de Costos.....</b>	<b>113</b>
<b>Conclusiones .....</b>	<b>116</b>
<b>Trabajos Futuros por Realizar .....</b>	<b>119</b>
<b>Acrónimos.....</b>	<b>120</b>
<b>Referencias.....</b>	<b>124</b>

---

## Índice de Figuras

Figura 1. Ejemplo de una fábrica con sistemas TI y OT .....	16
Figura 2. Ejemplo de obstáculos humanos que surgen en torno a un concepto de producto.....	18
Figura 3. Ejemplo de arquitectura de seguridad para un sistema SCADA.....	19
Figura 4. Mensaje del ransomware CriptoLoker solicitando el pago de un rescate .....	24
Figura 5. Cybersecurity Framework Version 1.1 .....	33
Figura 6. Ilustración de cómo funciona una Infraestructura de Clave Pública.....	35
Figura 7. Modelos de dispositivos token (a la izquierda) y smartcard (a la derecha).....	42
Figura 8. HSM de la empresa Thales.....	43
Figura 9. Población mundial en miles de millones de personas .....	47
Figura 10. Evolución cronológica de las revoluciones industriales.....	49
Figura 11. Los cinco niveles de automatización y las tecnologías que suele utilizar .....	54
Figura 12. Representación de un sistema SCADA .....	56
Figura 13. Diagrama de flujo en el ciclo de trabajo de un PLC.....	63
Figura 14. PLC marca Schneider Electric modelo M221 .....	65
Figura 15. Conexión simple de la estación SCADA y el servidor con una base de datos demo..	67
Figura 16. Modelo OSI .....	69
Figura 17. Pila de Comunicación Modbus.....	73
Figura 18. Ejemplo de arquitectura de red MODBUS.....	74
Figura 19. Protocolo Modbus serie comparado con el modelo OSI.....	75
Figura 20. Modbus/TCP ADU .....	77
Figura 21. mbap PDU encapsulado in TLS .....	78
Figura 22. Ejemplo de certificado x.509 v3 con extensión de función.....	79
Figura 23. Estructura modular del protocolo DNP3 .....	83
Figura 24. Arquitectura Maestro-Esclavo IEC 60870-5-104.....	84
Figura 25. Utilización de las capas del modelo OSI en el protocolo Profibus .....	87
Figura 26. Origen de la Criptografía.....	88
Figura 27. Clasificación de la Criptografía.....	89
Figura 28. Criptografía Simétrica .....	90
Figura 29. Criptografía Asimétrica .....	92

Figura 30. Cálculo del costo de dos servidores para la implementación de esta propuesta ..... 114

---

## Índice de Tablas

Tabla 1. Relaciones entre principios y componentes.....	52
Tabla 2. Disposición estándar seleccionada de la norma complementaria de telecontrol definida .....	84
Tabla 3. Planificación de actividades.....	109
Tabla 4. Matriz FODA de la propuesta de intervención .....	113
Tabla 5. Cálculo del costo para el personal a contratar .....	115

### 1.1 Descripción del Problema

Desde hace varios años, especialmente con el auge de la Industria 4.0, las empresas han comenzado a integrar diversos dispositivos operacionales en sus redes corporativas para automatizar los procesos industriales y mejorar la eficiencia de los recursos humanos y activos en general. Estos sistemas no solo proporcionan previsibilidad y ahorro en insumos, sino que también ofrecen estadísticas en tiempo real y facilitan la detección temprana de problemas y errores en los procesos productivos.

Actualmente, el sistema SCADA es la solución líder para la automatización, control y análisis de procesos de fabricación a nivel mundial. Conecta la red corporativa de PCs y servidores con la red de autómatas industriales e incluso con Internet. Esta interconexión ha expuesto los sistemas de control industrial (ICS, por sus siglas en inglés) a amenazas y vulnerabilidades inherentes a las redes corporativas y sistemas operativos.

### 1.2 Justificación de la Propuesta

En base a la problemática identificada en el apartado anterior, se propone un esquema de protección de los sistemas SCADA y sus componentes basado en infraestructura PKI y cifrado en las comunicaciones de los PLC, así como también recomendar un escenario de buenas prácticas y controles preventivos para minimizar el riesgo de potenciales ciberataques a infraestructuras críticas.

### **1.3 Marco Institucional**

Este trabajo está destinado a las industrias e infraestructuras críticas que utilizan sistemas SCADA en sus operaciones a fin de incrementar el nivel de seguridad informática en sus procesos informáticos.

### **1.4 Objetivos del Trabajo Final de Carrera**

#### **1.4.1 Objetivo General**

El presente trabajo tiene por objetivo principal implementar una solución basada en infraestructura PKI para establecer un marco de ciberseguridad en los entornos industriales, debido a las vulnerabilidades que se originaron en la convergencia de las redes IT/OT.

#### **1.4.2 Objetivos Específicos**

- Desarrollar un mecanismo de cifrado en las comunicaciones de los dispositivos PLC.
- Evaluar medidas paliativas para prevenir ciberataques originados por vulnerabilidades conocidas en redes IT.

### **1.5 Contribuciones Principales**

El presente trabajo contribuye a diseñar un marco de seguridad informática en los procesos automatizados de las industrias donde son utilizados los sistemas SCADA, a fin de gestionar y controlar la operatoria de las líneas de producción.

Gracias a esta iniciativa, no solo las industrias podrán contar con una implementación de PKI basada en buenas prácticas sino también las infraestructuras críticas de las naciones, tales como plantas potabilizadoras de agua, generación de energías, etc.

## **1.6 Metodología de Investigación**

Este trabajo final de carrera se encuentra orientado dentro de un enfoque cualitativo, el cual es particularmente adecuado para investigar áreas emergentes y complejas como la ciberseguridad en sistemas SCADA. La investigación cualitativa permite explorar en profundidad las percepciones, experiencias y conocimientos de expertos y actores clave en el campo de la ciberseguridad, capturando la complejidad del tema en su contexto específico. Esto es fundamental cuando se busca comprender fenómenos que son dinámicos y altamente contextualizados, como es el caso de las vulnerabilidades y amenazas en sistemas SCADA.

Según lo que sugiere realizar Sampieri et al. (2006), los datos fueron recolectados mediante análisis de documentación relevante, como reportes de incidentes de ciberseguridad y políticas de seguridad recomendadas como buenas prácticas. El análisis de los datos se llevó a cabo mediante la técnica de análisis temático, el cual es una técnica flexible y útil para identificar, analizar e informar patrones dentro de los datos cualitativos. Se realizó un enfoque holístico centrado en estudiar los fenómenos como un todo, comprendiendo la totalidad de éstos en su propio ambiente natural. De esta manera, el análisis interpretativo de los datos permite ser subjetivo basándose en las percepciones obtenidas.

### 2.1 Tecnologías IT/OT

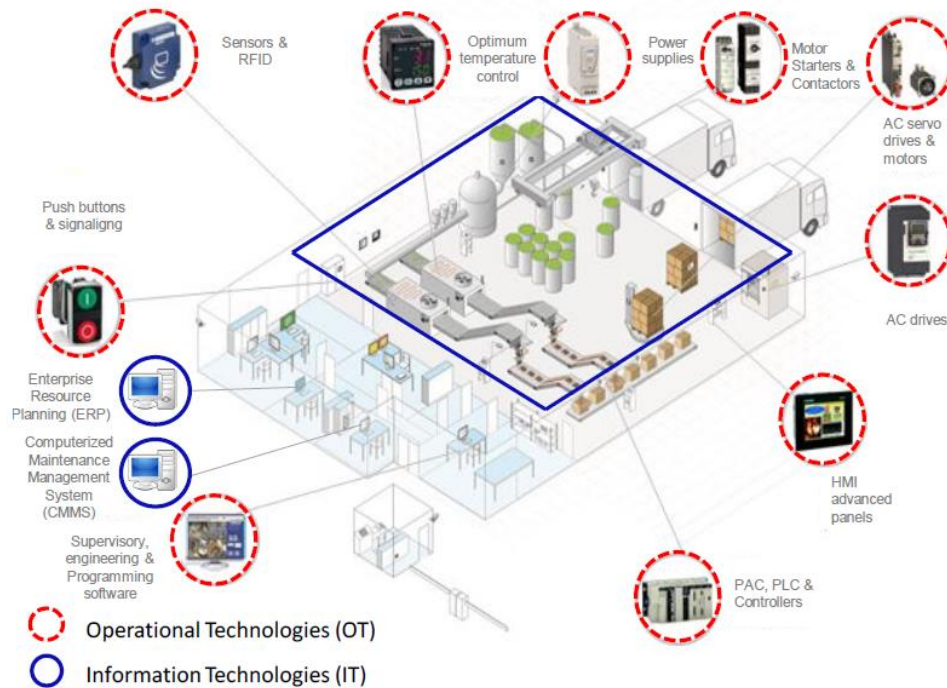
Según explican Bonnetto et al. (2016), las Tecnologías Operativas (OT) son sistemas de control y mando compuestos por hardware y software destinados a supervisar y controlar plantas y equipos. Comprenden, entre otros, sensores, PAC (controlador programable de automatización), PLC (controlador lógico programable) y demás unidades de control tal como se muestran en la Figura 1. La función principal de las OT es enviar órdenes de actuación a los medios de producción y recopilar información sobre el progreso de los procesos industriales.

En cambio, las Tecnologías de la Información (TI) son sistemas cuya función es recopilar y procesar información empresarial y son utilizados en diversas tareas empresariales como marketing, ventas, fabricación, logística, compras, finanzas o recursos humanos. De esta manera, se gestiona la información generada, utilizada y transformada por los procesos de fabricación y logística y se utilizan en la planificación de recursos empresariales (ERP) o el sistema informatizado de gestión del mantenimiento (Bonnetto y otros, 2016).



**Figura 1**

*Ejemplo de una fábrica con sistemas TI y OT*



Nota. Obtenido de *A Categorization of Customer Concerns for an OT Front-End of Innovation Process in IT/OT Convergence Context*, por Bonnetto et. al., 2016

### 2.1.1 Convergencia IT/OT en entornos industriales

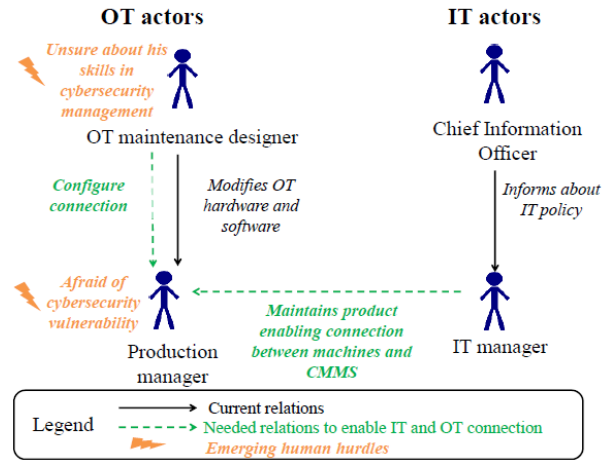
Como se ilustró en la Figura 1, los sistemas de IT y OT en un contexto industrial desempeñan un papel importante. Bonnetto et al. (2016) indica que para utilizar o implantar ambas tecnologías se necesitan dos tipos diferentes de agentes. Por ejemplo, los diseñadores de mantenimiento de OT modifican el hardware y el software de OT, mientras que un director de producción programa las actividades de la fábrica. Por el lado de las IT, un Director de Información (CIO) elabora la política y los indicadores de IT. Luego, los comunica al responsable de IT quien organiza las infraestructuras informáticas en consecuencia.

Hoy en día, las IT y las OT están cada vez más entrelazadas. Esta tendencia se denomina convergencia IT/OT. Esta convergencia permite a las IT poner datos como las órdenes de producción o las existencias de material disponibles para las máquinas en tiempo real. Una aplicación directa es que las máquinas se beneficien de las capacidades de procesamiento de datos de los sistemas informáticos para optimizar los procesos de producción.

Bonnetto et al. (2016) también indica que los nuevos conceptos de productos o servicios contribuyen a esta convergencia. Implican a diferentes partes interesadas en función de las soluciones propuestas. Por ejemplo, un jefe de producción tiene un problema: anticiparse a los fallos de una máquina. Puede que necesite controlar el tiempo de funcionamiento del activo. Si un proveedor de automatización ofreciera un concepto de producto que conectara los controladores a uno de mantenimiento (GMAO), el GMAO podría generar una orden de mantenimiento cuando el tiempo de funcionamiento superara un umbral. El responsable de producción tendría que conceder al responsable informático derechos de acceso a los datos de las máquinas. Y los diseñadores de mantenimiento OT tendrían que utilizar las especificaciones de las máquinas para configurar una conexión con el concepto de producto. Sin embargo, en la mayoría de los casos sería reacio a permitirlo porque esto crearía brechas de ciberseguridad. Es prerrogativa del director de producción preservar la integridad de los datos de OT. Esto sería un desencadenante para rechazar el concepto y pone de manifiesto el conflicto de intereses entre estos dos actores de la empresa. Estos obstáculos se ilustran en la Figura 2:

**Figura 2**

*Ejemplo de obstáculos humanos que surgen en torno a un concepto de producto*



Nota. Obtenido de *A Categorization of Customer Concerns for an OT Front-End of Innovation Process in IT/OT Convergence Context*, por Bonnetto et. al., 2016

### 2.1.2 Entornos OT basados en SCADA

La Figura 3 muestra un ejemplo de implementación de defensa en profundidad para un sistema SCADA que supone que la organización ya ha abordado las Capas 1 y 2. Para la Capa 3, la organización debe integrar diversas capacidades en la arquitectura de seguridad. Es fundamental segmentar la red en diferentes zonas o regiones para aplicar una estrategia de defensa en profundidad en el entorno SCADA. Esta segmentación debe extenderse a los sistemas de seguridad, como la supervisión física, controles de acceso, puertas, cámaras, sistemas VoIP y lectores de tarjetas (NIST, 2023).

También es importante incorporar dispositivos de seguridad, como firewalls, entre las regiones para gestionar y supervisar las comunicaciones entre los segmentos de la red. Estos firewalls pueden ofrecer mejor compatibilidad con protocolos específicos de OT y fortalecer la

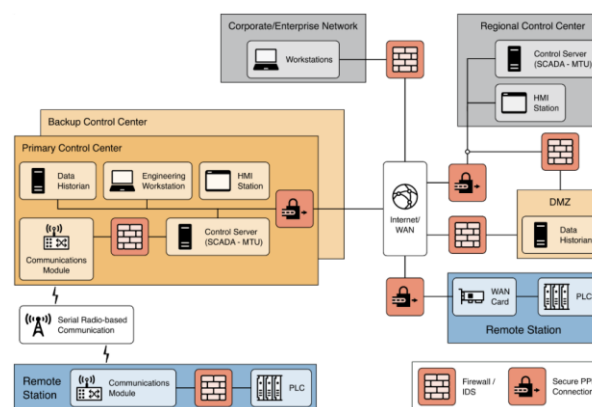
protección de dispositivos como PLCs y controladores. Se deben establecer reglas claras para asegurar que solo las comunicaciones autorizadas transiten entre regiones.

Además, la empresa NIST (2023) recomienda usar conexiones seguras, como túneles VPN, canales cifrados o conexiones punto a punto, para interconectar segmentos de red, tales como entre centros regionales y centros de control principales, o entre estaciones remotas y centros de control. Para ubicaciones distantes, es posible establecer conexiones seguras a través de Internet o redes WAN. Los dispositivos en los segmentos de la red deben conectarse a otros segmentos exclusivamente a través de estas conexiones seguras y tener el acceso a Internet restringido.

Por último, se debe implementar una DMZ (Zona Desmilitarizada) para separar los centros de control de la red empresarial. Toda comunicación entre la red de la empresa y los centros de control debe pasar por servicios situados en la DMZ. Dado que la DMZ se conecta con entornos externos, sus servicios deben ser monitoreados y protegidos para evitar que atacantes potenciales accedan al entorno OT sin ser detectados (NIST, 2023).

### Figura 3

#### *Ejemplo de arquitectura de seguridad para un sistema SCADA*



Nota. Obtenido de *Guide to Operational Technology (OT) Security*, NIST, 2023

### 2.1.3 IIoT

El IoT, o Internet de las cosas, hace referencia a los objetos cotidianos que se conectan a una red e intercambian datos con otros dispositivos, mientras que el IIoT es una parte del IoT.

Por lo general, el IoT comprende cualquier equipo que aprovecha la conexión a Internet para enviar y recibir datos tal como menciona la empresa Red Hat (2021). Cuando estos equipos se utilizan con fines industriales, se los considera IIoT.

Los dispositivos del IoT de los usuarios incluyen productos como luces, cerraduras y termostatos que se encuentran conectados, mientras que los del IoT industrial abarcan una gran cantidad de elementos, como medidores de agua, maquinarias o sensores de tuberías.

El término "Internet Industrial de las Cosas" (IIoT) se emplea para describir la implementación de dispositivos interconectados en entornos como fábricas y empresas de energía. Su función primordial es facilitar un nivel más elevado de automatización y autocontrol en las maquinarias industriales, con el fin de mejorar la eficiencia operativa (Red Hat, 2021).

IIoT World (2018) indica que la industria manufacturera tiene una larga historia de máquinas y sistemas automatizados. La IIoT forma parte de los esfuerzos más amplios de la Industria 4.0 y la transformación digital para ayudar a conectar activos críticos, extraer datos y mejorar las operaciones de la fábrica.

El retorno de la inversión con IIoT aumenta una vez que las empresas aplican análisis avanzados, como el aprendizaje automático, para identificar correlaciones de datos en tiempo real, y la automatización de procesos como los tickets de reparación. Debido a que el uso de estas dos etapas va a la zaga de la conectividad de dispositivos y la supervisión en tiempo real, las empresas de fabricación tienen una oportunidad significativa de avanzar en sus capacidades de IIoT para lograr un mayor impacto futuro (IIoT World, 2018).

## **2.2 Ciberseguridad en Entornos Industriales**

### **2.2.1 Introducción**

La empresa Kaspersky (2021) define a la ciberseguridad como la práctica de defender computadoras, servidores, dispositivos móviles, sistemas electrónicos, redes y datos de ataques malintencionados. También se conoce como seguridad de las tecnologías de la información o seguridad de la información electrónica. El término se aplica en diversos contextos, desde la empresa a la informática móvil, y puede dividirse en las siguientes categorías:

- Seguridad de redes: es la práctica de proteger una red informática de intrusos, ya sean atacantes selectivos o programas maliciosos oportunistas.
- Seguridad de las aplicaciones: se centra en mantener el software y los dispositivos libres de amenazas. Una aplicación comprometida podría dar acceso a los datos que está diseñada para proteger. El éxito de la seguridad empieza en la fase de diseño, mucho antes de que se despliegue un programa o dispositivo.
- Seguridad de la información: protege la integridad y privacidad de los datos, tanto en almacenamiento como en tránsito.
- Seguridad operativa: incluye los procesos y decisiones para manejar y proteger los activos de datos. Los permisos que tienen los usuarios cuando acceden a una red y los procedimientos que determinan cómo y dónde pueden almacenarse o compartirse los datos entran dentro de este ámbito.
- Recuperación de catástrofes y continuidad del negocio: se trata de cómo responde una organización a un incidente de ciberseguridad o a cualquier otro suceso que provoque la pérdida de operaciones o datos. Las políticas de recuperación de desastres dictan cómo la

organización restaura sus operaciones e información para volver a la misma capacidad operativa que antes del suceso. La continuidad del negocio es el plan al que recurre la organización cuando intenta operar sin determinados recursos.

- Educación del usuario final: aborda el factor más imprevisible de la ciberseguridad: las personas. Cualquiera puede introducir accidentalmente un virus en un sistema por lo demás seguro si no sigue unas buenas prácticas de seguridad. Enseñar a los usuarios a eliminar archivos adjuntos de correo electrónico sospechosos, a no conectar unidades USB no identificadas y otras lecciones importantes es vital para la seguridad de cualquier organización (Kaspersky, 2021).

Por otro lado, según el estándar ISO 27001 de la Organización Internacional de Estandarización existen tres conceptos que forman parte del pilar de la seguridad de la información: confidencialidad, integridad y disponibilidad. Para que un programa de ciberseguridad se considere integral y completo, debe cumplir adecuadamente toda esta tríada (International Organization for Standardization, 2013). Primero, la confidencialidad protege la información de accesos no autorizados y usos indebidos, salvaguardando datos sensibles como información comercial o personal. Se utilizan contraseñas, listas de control de acceso y cifrado para evitar el robo de contraseñas y otros ataques.

En cuanto a la integridad, Heymsfeld (2018) indica que las medidas aseguran que la información no sea alterada de manera no autorizada, manteniendo la precisión de los datos tanto en almacenamiento como en transmisión. Esto incluye el control de acceso, autenticación rigurosa, y técnicas como verificaciones de hash y firmas digitales para evitar cambios no autorizados y asegurar que los datos sean auténticos.

Finalmente, la disponibilidad garantiza que los sistemas de información estén accesibles para los usuarios autorizados en todo momento. Esto abarca la protección contra fallos de hardware, paradas de software y problemas de red, así como ataques maliciosos que buscan interrumpir el acceso al sistema. La disponibilidad constante es crucial para evitar pérdidas económicas, insatisfacción de clientes y daños a la reputación (Heymsfeld, 2018).

### **2.2.2 Tipos de Ciberataques**

En el mundo de los ciberataques, uno de los métodos más comunes es el uso de malware, un tipo de software desarrollado por ciber-delincuentes con el propósito de alterar o dañar las computadoras de los usuarios. Este software malicioso suele distribuirse mediante archivos adjuntos en correos electrónicos no solicitados o descargas que parecen seguras. Los atacantes utilizan el malware para obtener beneficios económicos o para llevar a cabo ataques con intenciones políticas. Entre las variedades de malware se encuentran los virus, troyanos, spyware y adware. Sin embargo, el ransomware ha crecido significativamente en los últimos años debido a su destructividad. Este tipo de malware cifra archivos esenciales tanto en dispositivos locales como en redes, y demanda un pago para su liberación. Los atacantes lo emplean para extorsionar a las víctimas, ya que su encriptación es tan fuerte que no se puede romper fácilmente, lo que obliga a las personas a depender de copias de seguridad para recuperar su información. Sin copias de seguridad, la única opción es pagar el rescate, aunque incluso entonces no hay garantía de recibir la clave de descifrado. En la Figura 4 se muestra un ejemplo de este tipo de malware (Trend Micro, 2023):



**Figura 4**

*Mensaje del ransomware CriptoLoker solicitando el pago de un rescate*



Nota. Obtenido de *¿Qué es el Ransomware?*, Trend Micro, 2023

Otro método utilizado es la inyección SQL, que permite a los atacantes acceder y robar datos de una base de datos aprovechando vulnerabilidades en las aplicaciones. Insertan código malicioso a través de consultas SQL manipuladas, lo que les otorga acceso a información sensible almacenada (Kaspersky, 2021).

El phishing es otra táctica común en la que los ciberdelincuentes envían correos electrónicos que imitan comunicaciones de empresas legítimas para solicitar datos confidenciales. Esta técnica a menudo engaña a las víctimas para que proporcionen información personal y detalles de tarjetas de crédito.

También Kaspersky (2021) indica que los ataques de hombre en el medio implican interceptar comunicaciones entre dos partes para robar datos. Esto puede ocurrir en redes WiFi inseguras, donde un atacante intercepta el tráfico entre un dispositivo y la red.

Finalmente, los ataques de denegación de servicio (DoS) saturan redes y servidores con un volumen masivo de tráfico, impidiendo que los sistemas procesen solicitudes legítimas y paralizando las funciones esenciales de una organización (Kaspersky, 2021).

### **2.2.3 Vulnerabilidades Explotadas en Sistemas de Control Industrial**

Si bien los ICS introducen mucha eficiencia en los procesos operativos, también plantea nuevos problemas en materia de seguridad. Según describe la empresa Trend Micro (2022) en su sitio web, los actores de las amenazas tienen mucho que ganar cuando atacan a este tipo de empresas. Un ataque con éxito a ICS tiene graves efectos en cualquier organización. Algunos de estos efectos incluyen paradas operativas, equipos dañados, pérdidas financieras, robo de propiedad intelectual y riesgos sustanciales para la salud y la seguridad. A la hora de llevar a cabo los ataques, estos actores de amenazas suelen estar motivados por un beneficio económico, una causa política o incluso un objetivo militar. Los ataques pueden estar patrocinados por el Estado o también pueden provenir de competidores, personas con información privilegiada con un objetivo malicioso e incluso hacktivistas.

La primera fase de un ataque contra ICS suele consistir en un reconocimiento que permite al atacante inspeccionar el entorno. El siguiente paso sería emplear diferentes tácticas que ayuden a los atacantes a hacerse un hueco en la red objetivo. Las estrategias y tácticas en este punto son muy similares a las de un ataque dirigido. Para lanzar un malware, un atacante hará uso de todas las posibles vulnerabilidades y configuraciones específicas de un ICS. Una vez identificadas y

explotadas estas vulnerabilidades, los efectos de un ataque pueden provocar cambios en determinadas operaciones y funciones o ajustes en los controles y/o configuraciones existentes (Trend Micro, 2022).

Dado que todos los ICS tienen que ver tanto con la tecnología de la información (IT) como con la tecnología operativa (OT), agrupar las vulnerabilidades por categorías ayuda a determinar y aplicar estrategias de mitigación. La guía de seguridad para sistemas de control industrial (ICS) del Instituto Nacional de Estándares y Tecnología (NIST) clasifica las preocupaciones en torno a políticas y procedimientos, así como en las vulnerabilidades presentes en diferentes plataformas y redes. Estas vulnerabilidades pueden abarcar desde aspectos relacionados con políticas y procedimientos hasta problemas en la configuración de plataformas, incluyendo hardware y software. También se consideran cuestiones de protección contra malware, configuración de red, y seguridad del hardware y perímetro de red. Además, se incluyen aspectos relacionados con la comunicación, las conexiones inalámbricas y la supervisión y registro de redes (Trend Micro, 2022).

#### **2.2.4 Casos de ciberataques en ICS**

Los ataques contra sistemas ICS suelen ser ataques dirigidos que utilizan la vía de entrada de estos sistemas para hacerse un espacio que les permita realizar movimiento lateral dentro de la organización. Entre los casos más resonantes se encuentran el gusano Stuxnet, que se utilizó para manipular centrifugadoras dentro de instalaciones nucleares en Irán, y BlackEnergy que afectó a instalaciones de generación de energía en Ucrania. A pesar de que la mayoría de los ataques se centraron en el robo de datos y/o el espionaje industrial, los dos casos mencionados demostraron cómo el malware tenía un efecto cinético (Trend Micro, 2021).

Según indica McMillen (2016), en enero de 2016 GitHub publicó una solución de pruebas de penetración que contenía una herramienta de fuerza bruta que podía utilizarse contra el protocolo Modbus. La publicación y posterior uso de esta herramienta por parte de varios actores desconocidos probablemente provocó el aumento de la actividad maliciosa contra ICS en los últimos 12 meses. La mayoría de los ataques contra ICS en 2016 se produjeron en Estados Unidos. Esto no fue sorprendente, ya que Estados Unidos tiene la mayor presencia de sistemas ICS conectados a Internet en el mundo.

El malware SFG, descubierto en junio de 2016 en las redes de una empresa energética europea, creaba una puerta trasera en los sistemas de control industrial atacados. Según los investigadores de seguridad de SentinelOne Labs, la puerta trasera entregaba una carga útil que se utilizaba para extraer datos de la red energética o para desconectarla potencialmente. Dicho malware, estaba basado en Windows y fue diseñado para eludir en su momento el software antivirus y los firewalls tradicionales (McMillen, 2016).

A continuación, se describen otros casos emblemáticos de ciberataques a ICS de alto impacto mundial:

- Estonia (año 2007): en abril de ese año numerosos ataques cibernéticos causaron la inoperatividad de páginas web gubernamentales, medios de comunicación y universidades, principalmente mediante ataques de Denegación de Servicio Distribuido (DDoS). El 19 de mayo, todos los sitios recuperaron su funcionalidad, marcando así el fin de la primera ciberguerra. Estos ataques fueron desencadenados tras la decisión del gobierno de Estonia de retirar un monumento en el centro de Tallin, lo que generó la protesta por parte de Rusia (Vazquez, 2015).

- Arabia Saudita (año 2012): Aramco, la mayor petrolera del mundo, experimentó un extenso ataque que inutilizó alrededor de 35.000 terminales con sistema operativo Windows durante casi medio año. La infección tuvo origen cuando un empleado abrió un correo electrónico fraudulento en un ataque de phishing, ejecutando así el virus Shamoon/W32.distract. Su función principal consistió en la eliminación indiscriminada de archivos de los discos rígidos (Kubecka, 2015).

### **2.2.5 Impacto de la Pandemia COVID-19 en la Ciberseguridad**

Según describe Campillo (2022), el 11 de marzo de 2020 la Organización Mundial de la Salud (OMS) declaró formalmente que la enfermedad causada por el virus corona descubierto en diciembre de 2019 (COVID-19) comenzó a considerarse pandémica. A raíz de esto, muchos países declararon la emergencia sanitaria, obligando a sus ciudadanos a confinarse en sus domicilios y prohibir la libre circulación por los espacios públicos, incluyendo la asistencia presencial a sus lugares de trabajo. Las acciones tomadas en respuesta a la pandemia, han generado que las empresas que ya permitían el trabajo remoto lo continúen y amplíen, y aquellas que no lo tenían, lo introduzcan. El aumento en la modalidad de trabajo desde casa ha planteado nuevos desafíos en términos de ciber-seguridad que requerían respuestas inmediatas. En consecuencia, muchas empresas han implementado medidas más rigurosas de ciber-seguridad y han fomentado prácticas seguras en este ámbito, con el fin de permitir que sus empleados trabajen desde casa minimizando los riesgos cibernéticos. Un considerable número de organizaciones han acelerado la adopción de entornos multinube como una estrategia para obtener ventajas en costos y capacidad, permitiendo así respaldar fuerzas laborales distribuidas para hacer frente a los desafíos derivados de la

pandemia. Por lo tanto, una de las tendencias más notables en términos de ataques se está orientando hacia la nube.

En los primeros cuatro meses del año 2020, coincidiendo con el período de mayor propagación del COVID-19 a nivel mundial, Interpol registró 907.000 mensajes de spam, 737 incidentes vinculados a malware y 48.000 URLs maliciosas. Durante ese tiempo, Interpol distribuyó encuestas sobre el impacto de la crisis del COVID-19 a sus 194 países miembros, obteniendo respuestas de 48 de ellos. El análisis resultante de la información compartida por los países se complementó con datos proporcionados por el Interpol Cybercrime Threat Response (CTR) y el Cyber Fusion Centre (CFC). Algunas de las categorías de delitos que se vieron incrementados durante este período son las siguientes (Campillo, 2022):

- Estafas online y phishing: aprovechado la situación de preocupación entre la población por el virus, se utilizaron temas relacionados con la pandemia como señuelo para robar datos de sus víctimas, haciéndose pasar por gobiernos e instituciones.
- Malware disruptivo: principalmente ataques de tipo DDoS y ransomware.
- Malware recolector de datos: utilización de troyanos, spyware, etc.
- Dominios maliciosos: creación de sitios webs fraudulentos con palabras claves relacionadas a la pandemia.
- Desinformación (Campillo, 2022).

Teniendo en cuenta estos antecedentes, Lakshmanan (2020) menciona que también en el año 2020 se detectó una campaña de malware que utiliza señuelos relacionados con el COVID-19 para dirigirse a los sectores gubernamentales y de energía en Azerbaiyán. En estos ataques selectivos, se utilizaron documentos de Microsoft Word como vehículos para introducir un troyano de acceso remoto (RAT) hasta ese momento desconocido llamado "PoetRAT". Este malware

basado en Python tenía la capacidad de extraer información confidencial, como documentos, pulsaciones de teclas, contraseñas e incluso imágenes de la cámara web.

Los investigadores indicaron que el malware está específicamente diseñado para afectar a los sistemas de control de supervisión y adquisición de datos (SCADA) en la industria energética, dirigido a sistemas como las turbinas eólicas, cuyas identidades aún no se conocen.

Este desarrollo fue solo uno de los tantos intentos de ataques cibernéticos que aprovecharon los temores continuos asociados a la pandemia como anzuelo para instalar malware, robar información y obtener beneficios (Lakshmanan, 2020).

### **2.2.6 Mitigación de Riesgos en OT**

A fin de mitigar los efectos de un potencial ciberataque y proteger los tres pilares de la ciberseguridad (confidencialidad, integridad y disponibilidad), Kamlofsky et al. (2015) propone una solución integral que incluye la protección de la red con seguridad perimetral, una gestión eficiente de la seguridad informática, implementación de mecanismos de criptografía y demás consideraciones relacionadas al hardware y software de los equipos en red.

Se sugiere operar con redes segmentadas de manera lógica, empleando Firewalls que faciliten la filtración del tráfico, así como Routers con capacidad de gestionar VLANs para lograr una separación lógica de los distintos segmentos, acompañados de ACL. También se aconseja la implementación de sistemas IDS/IPDS para detectar ataques en el momento en que ocurren. Además, se considera esencial contar con un SOC (Centro de Operaciones de Seguridad) y un NOC (Centro de Operaciones de Red) desde los cuales se pueda realizar el monitoreo en tiempo real de los servidores y dispositivos de seguridad.

Respecto a las gestiones necesarias relacionadas a la seguridad informática, las pautas de la norma ISO 27001 ofrecen un conjunto de buenas prácticas para la administración de la seguridad de la información. De todos modos, el elemento más susceptible siempre es el factor humano. Es fundamental implementar un programa de formación continua y asignar permisos de acceso mínimos. Cada terminal y punto de acceso a la red debe contar con un antivirus actualizado. Se recomienda gestionar adecuadamente la seguridad física del entorno. Es imperativo adoptar medidas preventivas y correctivas basadas en procedimientos para la gestión y manejo de incidentes, así como realizar pruebas de penetración y análisis de vulnerabilidades tanto internos como externos. Esto permitirá establecer un sólido esquema de defensa en profundidad que impacte tanto a la empresa como a sus proveedores (Kamlofsky y otros, 2015).

Por otro lado, el autor también sugiere implementar algún tipo de algoritmo en las comunicaciones dentro de la red como criptografía asimétrica pos-cuántica empleando anillos no conmutativos ya que sería más apta para procesadores de bajo poder de cómputo como es el caso de los PLCs.

Finalmente, sería recomendable también que sólo se permita la instalación de equipos y dispositivos en la red que cumplan con las normas de seguridad y estabilidad en el tiempo (Kamlofsky y otros, 2015).

### **Marco de Ciberseguridad en sistemas industriales**

Según indica la NIST (2023), muchas organizaciones de los sectores público y privado han adoptado el Marco de Ciberseguridad del NIST (National Institute of Standards and Technology) para guiar las actividades de ciber-seguridad y considerar los riesgos de ciber-seguridad. El marco consta de cinco funciones concurrentes y continuas para presentar las normas, directrices y



prácticas de la industria de una manera que permita la comunicación de actividades y resultados de ciber-seguridad en toda la organización. Cuando se consideran conjuntamente, estas funciones proporcionan una visión estratégica de alto nivel para la gestión de riesgos de ciber-seguridad. El marco identifica además las categorías y subcategorías clave subyacentes para cada función y las asocia con ejemplos de información subyacentes para cada función y las relaciona con referencias informativas tales como directrices y prácticas existentes para cada subcategoría.

En términos generales, podemos mencionar las principales características de cada uno de estas funciones según lo descrito por la NIST (2023):

- Identificar (ID): Desarrollar un entendimiento organizativo para gestionar el riesgo de ciber-seguridad para sistemas, personas, activos, datos y capacidades.
- Proteger (PR) - Desarrollar e implementar métodos de resguardo adecuados para garantizar la prestación de servicios críticos.
- Detectar (DE) - Desarrollar e implementar actividades apropiadas para identificar un evento de ciber-seguridad.
- Responder (RS) - Desarrollar e implementar actividades apropiadas para tomar medidas ante un incidente de ciber-seguridad detectado.
- Recuperación (RC) - Desarrollar e implementar actividades apropiadas para mantener los planes de resiliencia y restaurar las capacidades o servicios que se hayan visto afectados por un incidente de ciber-seguridad.

En la Figura 5 se pueden observar las cinco funciones:

## Figura 5

### Cibersecurity Framework Version 1.1



Nota. Obtenido de *Guide to Operational Technology (OT) Security*, NIST, 2023

## Ciber-resiliencia

Según mencionan Kott y Linkov (2018), la sociedad demanda una creciente dependencia en sistemas cibernéticos interconectados, desde actividades cotidianas hasta defensa y tráfico aéreo. Aunque esta integración mejora la eficiencia, también conlleva amenazas de piratas informáticos, incluyendo ataques como DDoS, robo de datos y ransomware. Estas amenazas afectan a individuos, empresas e incluso gobiernos. La evaluación de riesgos en ciber-seguridad se ve limitada debido a la complejidad de sistemas interdependientes. Se destaca la necesidad de enfoques de gestión que aborden riesgos en todos los ámbitos de los ciber-sistemas. Dada la imprevisibilidad y evolución rápida de ciber-amenazas, endurecer los sistemas contra amenazas identificadas se muestra parcialmente eficaz. En este sentido, se propone el concepto de ciber-resiliencia, siendo la capacidad para prepararse, absorber, recuperar y adaptarse a los efectos adversos, asociados a los ciber-ataques. Aquí, según el contexto, utilizamos el término ciber-resiliencia para referirnos principalmente a la propiedad de resiliencia de un sistema o red; a

veces también utilizamos el término para referirnos a las características o componentes de la red que permiten la ciber-resiliencia.

Las infraestructuras críticas proporcionan servicios esenciales como agua, electricidad, comunicaciones y salud, y están interconectadas con sistemas cibernéticos. La interdependencia entre estos sistemas, contruidos y operados por diversas entidades, puede llevar a fallos sistémicos en cascada. Existen diversas amenazas, tanto naturales como humanas, que pueden afectar a las infraestructuras críticas, incluyendo ciber-amenazas. La resiliencia regional se evalúa considerando la interrelación entre sistemas cibernéticos y físicos, así como la dependencia mutua entre infraestructuras críticas y ciber-sistemas. Se introduce una metodología de Evaluación de Resiliencia Cibernética (ERC) para examinar y mejorar la resiliencia regional, identificando áreas de preocupación y ofreciendo opciones de mejora.

El ERC incorpora evaluaciones de vulnerabilidad, evaluaciones de capacidades y los esfuerzos de planificación de la protección de infraestructuras para elaborar un análisis de las infraestructuras críticas de una región y de las capacidades de preparación pertinentes. Los esfuerzos específicos asociados con cada proyecto ERC pueden incluir evaluaciones regionales y de seguridad física in situ, revisiones de la resistencia cibernética, ciber-evaluaciones, productos geoespaciales, talleres, debates facilitados con partes interesadas públicas y privadas, modelización y análisis, formación y concienciación sobre mitigación de riesgos y ejercicios prácticos (Kott & Linkov, 2018).

## 2.3 PKI

### 2.3.1 Características Principales

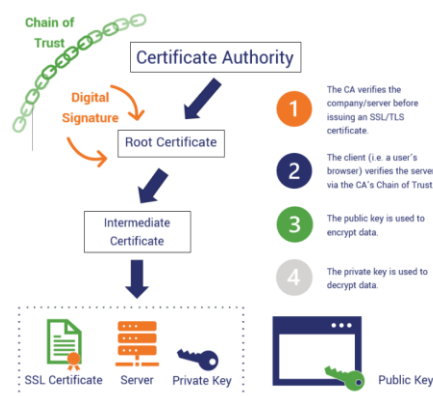
Alamilla Hernández et al. (2020) explica que la Infraestructura de Clave Pública (PKI, por sus siglas en inglés) establece una jerarquía o estructura de confianza entre una entidad que busca ser reconocida y requiere tener su firma en Internet, y un usuario. En esencia, el fundamento de todas las comunicaciones que utilizan PKI es la creación de una identidad, ya sea para la persona que accede a un sitio restringido o para el sitio que se presenta al público. La premisa principal siempre es la verificación y establecimiento de una identidad.

Se puede utilizar para certificar usuarios, computadoras y servidores, aunque también para solucionar problemas generando certificados en equipos específicos (verificando al cliente que sea quien dice ser y el equipo valide al servidor sea quien dice ser).

En la Figura 6 se puede observar un ejemplo típico de una arquitectura PKI:

**Figura 6**

*Ilustración de cómo funciona una Infraestructura de Clave Pública*



Nota. Obtenido de *Your Guide to How PKI Works & Secures Your Organization*, por Crane, 2020

Según la empresa Microsoft (2023), las funciones de una PKI son mantener, distribuir, validar y revocar certificados SSL/TLS. Dentro de esta infraestructura. Se destacan los siguientes conceptos:

- **Protocolo SSL/TLS:** la función principal del protocolo SSL es garantizar la privacidad y confiabilidad en la comunicación entre dos aplicaciones. Este protocolo consta de dos capas: el protocolo de registro SSL y el protocolo de Handshake SSL. El primero se encarga de encapsular otros protocolos de nivel superior, mientras que el segundo permite que tanto el cliente como el servidor se autenticuen e intercambien algoritmos de encriptación y claves criptográficas antes de que la aplicación comience a recibir o transmitir datos (Microsoft, 2023).
- **Certificado:** los certificados digitales funcionan como la versión digital del documento de identidad en cuanto a la autenticación de individuos se refiere. Estos certificados posibilitan que una persona demuestre su verdadera identidad al mostrar que posee la clave secreta asociada a su certificado. Un aspecto crucial de un certificado de clave pública es la conexión entre la clave pública de una entidad certificadora y sus atributos vinculados a su identidad. Este certificado respalda que una clave pública pertenece a una entidad certificadora reconocida y que dicha entidad está al tanto de la clave privada asociada. Para que los certificados digitales sean efectivos, es esencial contar con una entidad certificadora que los respalde. Aunque es posible autocertificar los certificados, carecerían de garantías sobre la veracidad de la identidad y, por lo tanto, es improbable que terceros los acepten al no reconocer la fuente del certificado (Microsoft, 2023).

Existe también otro concepto relacionado llamado Lista de Revocación de Certificados (CRL) la cual es una lista de certificados digitales revocados por la entidad de certificación

antes de su fecha de expiración programada. La comprobación de revocación de certificados puede impedir el acceso al cliente si la CRL de cualquier certificado de la cadena de certificados ha expirado o no está disponible (Microsoft, 2023).

- Certificados X.509: el estándar X.509 para certificados es una norma establecida por la UIT-T (Unión Internacional de Telecomunicaciones, Sector de Normalización de las Telecomunicaciones) y la ISO/IEC (Organización Internacional de Normalización / Comisión Electrotécnica Internacional). Este estándar fue inicialmente lanzado en 1988, y su versión 1 fue ampliada en 1993 para incorporar dos nuevos campos destinados a respaldar el control de acceso a directorios (Alamilla Hernández y otros, 2020).

La implementación generalizada de técnicas de clave pública demanda una infraestructura que establezca un conjunto de normas, autoridades de certificación, relaciones entre diversas CAs (entidades certificadoras), procedimientos para identificar y confirmar rutas de certificación, protocolos operativos, protocolos de gestión, herramientas interoperables y un marco legal (Alamilla Hernández y otros, 2020).

- Firma digital: es una firma electrónica que se usa para autenticar la identidad de quien envía un mensaje o quien firma un documento electrónico. Desde una perspectiva legal y práctica, una firma digital proporciona una solución efectiva para conferir validez jurídica a archivos o documentos electrónicos. Similar al método tradicional de firma con papel y tinta, la firma digital incorpora la identidad del firmante al documento digital. No obstante, a diferencia de la firma manuscrita, se considera prácticamente imposible falsificar una firma digital de la misma manera. Además, la firma digital garantiza que cualquier modificación realizada en los datos firmados no pueda pasar desapercibida.

Se puede implementar firma electrónica avanzada con el algoritmo RSA ya que se puede dar soporte para la generación del par de claves que se necesitan (Alamilla Hernández y otros, 2020).

Dentro de la infraestructura de una PKI, se identifican varios componentes esenciales. La arquitectura incluye a las entidades encargadas de emitir y verificar la validez de los certificados, conocidas como autoridades de certificación. También se encuentra la autoridad de registro, que actúa como intermediario entre los usuarios finales y la autoridad de certificación en el proceso de emisión y renovación de certificados. Además, la autoridad de validación desempeña un papel crucial al consolidar y gestionar el registro de todos los certificados digitales, incluyendo los que están activos, expirados o revocados, y asegurar que esta información sea accesible para los usuarios (DocuSign, 2020).

En los siguientes apartados se analizarán las alternativas más importantes de implementaciones de Autoridades Certificantes que existen en la actualidad.

### **Microsoft Active Directory Certificate Services**

De acuerdo con lo que menciona la empresa Microsoft (2023), Active Directory Certificate Services (ADCS) es una función de Windows Server para la emisión y gestión de certificados de infraestructura de clave pública (PKI) utilizados en protocolos seguros de comunicación y autenticación.

ADCS ofrece diversas funciones clave. En primer lugar, las autoridades de certificación, tanto raíz como subordinadas, se encargan de emitir certificados para usuarios, equipos y servicios, así como de gestionar su validez. Además, la inscripción web permite a los usuarios solicitar certificados y obtener listas de revocación de certificados a través de un navegador. El servicio

Online Responder se encarga de procesar las solicitudes de estado de revocación de certificados, evaluando su estatus y proporcionando respuestas firmadas con la información solicitada. También, el servicio de inscripción de dispositivos de red facilita que routers y otros equipos de red sin cuentas de dominio obtengan certificados. La atestación de clave TPM permite a la autoridad de certificación confirmar que la clave privada está protegida por un TPM basado en hardware y que este TPM es confiable, evitando la exportación del certificado a dispositivos no autorizados y asociando la identidad del usuario al dispositivo. Por último, el servicio web de política de inscripción de certificados proporciona información sobre las políticas de inscripción, mientras que el servicio web de inscripción de certificados permite a los usuarios y computadoras realizar la inscripción de certificados a través de un servicio web, incluso si el ordenador cliente no es parte del dominio o no está conectado al mismo.

Entre las aplicaciones que admite ADCS se incluyen Secure/Multipurpose Internet Mail Extensions (S/MIME), redes inalámbricas seguras, redes privadas virtuales (VPN), seguridad de protocolo de Internet (IPsec), Encrypting File System (EFS), inicio de sesión con tarjeta inteligente, Secure Socket Layer/Transport Layer Security (SSL/TLS) y firmas digitales (Microsoft, 2023).

## **OpenSSL CA**

Según Nguyen (2015), OpenSSL es una biblioteca criptográfica gratuita y de código abierto que proporciona varias herramientas de línea de comandos para manejar certificados digitales. Algunas de estas herramientas pueden utilizarse para actuar como autoridad de certificación.



Una autoridad de certificación (CA) es una entidad que firma certificados digitales. Muchos sitios web necesitan que sus clientes sepan que la conexión es segura, por lo que pagan a una CA de confianza internacional (por ejemplo, VeriSign, DigiCert) para que firme un certificado para su dominio.

En algunos casos puede tener más sentido actuar como su propia CA, en lugar de pagar a una CA como DigiCert. Los casos más comunes incluyen la seguridad de un sitio web de una intranet o la emisión de certificados a clientes para permitirles autenticarse en un servidor (por ej. Apache, OpenVPN) (Nguyen, 2015).

### **2.3.2 Dispositivos criptográficos**

Se ha visto en apartados anteriores el uso de certificados digitales y la generación de claves para operaciones de autenticación y garantizar la privacidad y confiabilidad en la comunicación entre dos aplicaciones. A fin de proteger las claves privadas que se encuentran en poder de los usuarios, DNp Corp (2023) recomienda el uso de dispositivos criptográficos para ofrecer un segundo factor de autenticación y poner a resguardo el almacenamiento de las claves privadas.

Existen en el mercado dos tipos de dispositivos portables para usuarios finales: el token criptográfico y la smartcard. Respecto al primero, la empresa mencionada explica que se trata de dispositivos USB basado en un microprocesador, ofreciendo autenticación en certificados digitales y solución de generación de firmas digitales con valor legal, es fácil de usar, compatible con distintos sistemas operativos, e incluye un software de firma que permite realizar firma en diferentes tipos de archivos (PDF, paquete office, etc.) (Dnp Corp, 2023).

Actualmente, se aconseja que los dispositivos cumplan con ciertos requisitos técnicos para asegurar un nivel básico de seguridad y protección contra vulnerabilidades conocidas. Estos

dispositivos deben contar con una carcasa de material resistente, una interfaz USB estándar tipo A de versión 2.0 o superior, y un indicador LED que muestre la actividad. Además, deben permitir la obtención del número de serie a través de la API PKCS#11 y tener certificación FIPS 140-2 Nivel 2 o superior. La memoria del dispositivo debería ser de al menos 32 Kbytes. También es importante que puedan generar, operar, almacenar y gestionar claves criptográficas asimétricas RSA de 2048 bits como mínimo, así como generar y operar claves simétricas con un nivel de robustez equivalente al algoritmo AES. Además, deben permitir el almacenamiento de certificados X509v3 y usar funciones de hash seguro, como SHA-2 (Ministerio de Modernización, 2016).

Por otro lado, la smartcard o tarjeta inteligente es un dispositivo criptográfico certificado que permite almacenar una cantidad considerable de certificados digitales, generar la clave RSA de hasta 2048 bits, y cumple con estándares ISO 7816-3 como también protocolos T=0 Y T=1 (Dnp Corp, 2023). En la Figura 7 se pueden observar diferentes modelos de dispositivos tokens. La mencionada empresa sugiere que los dispositivos deben cumplir con varias características esenciales. Deben ser capaces de manejar comunicaciones T=0, T=1 y USB, y permitir la generación de claves de 1024 o 2048 bits directamente en el dispositivo. Además, deben realizar operaciones criptográficas, autenticación y control de acceso de acuerdo con la norma ISO 7816, y contar con una interfaz USB conforme a la parte 12 de esa norma. También deben ser compatibles con algoritmos criptográficos como DES, 3DES, MD5, SHA-1, SHA-256, RSA 1024 y RSA 2048, y garantizar la seguridad en las comunicaciones entre la tarjeta y la aplicación. Es importante que el dispositivo soporte los estándares PKCS#11, MS-CAPI y PC/SC para facilitar su integración con el software correspondiente, así como el proveedor de servicios criptográficos de Microsoft para la inscripción y el inicio de sesión con tarjetas en Windows. Además, debe permitir la generación y verificación de firmas digitales, ofrecer 64KB de memoria para el usuario,

y proporcionar un identificador único de 64 bits. La capacidad para integrarse con navegadores web y correos electrónicos, cumplir con el estándar PKCS#15, y permitir la integración con OpenSC, así como el almacenamiento seguro de certificados digitales X.509 v3, también son aspectos recomendados (Macroseguridad, 2023).

### **Figura 7**

*Modelos de dispositivos token (a la izquierda) y smartcard (a la derecha)*



Nota. Obtenido de *Tokens USB*, Macroseguridad, 2023

Por último, un HSM (Módulo de Seguridad de Hardware)) es un dispositivo de seguridad basado en hardware que crea, guarda y resguarda claves y llaves criptográficas (PKI). Aunque existen diversos programas que generan módulos de certificación, un dispositivo hardware ofrece un nivel de seguridad superior (Macroseguridad, 2023).

Los HSM posibilitan la generación de claves y llaves para certificados digitales de clave pública. Estos dispositivos admiten rutinas con un alto grado de aleatoriedad y también tienen la capacidad de almacenar contraseñas de acceso a certificados específicos.

Cuando un sistema experimenta un uso intensivo de claves criptográficas, la elección más acertada es un HSM. Proporcionan seguridad basada en hardware para aplicaciones críticas, como

bases de datos y servidores web o de aplicaciones, ya que las llaves se generan dentro del límite FIPS del HSM. Estos dispositivos pueden generar y almacenar claves RSA de 1024, 2048 bits y más (4096 bits), al mismo tiempo que las mantiene fuera del servidor de la organización (Macroseguridad, 2023).

Este dispositivo resulta ideal para proyectos que requieren manejar una gran cantidad de transacciones encriptadas por segundo, garantizando un rendimiento óptimo. Un HSM puede ser compartido entre varios servidores y es compatible con el montaje en rack, lo que ayuda a optimizar el espacio si es necesario agregar diferentes dispositivos. Además, mejora el rendimiento SSL de los servidores, asegurando que mantengan la velocidad necesaria sin requerir la adición de aceleradores (Macroseguridad, 2023).

En la Figura 8 se muestra un ejemplo de un equipo HSM:

### **Figura 8**

*HSM de la empresa Thales*



Nota. Obtenido de *HSM*, Macroseguridad, 2023

### 3.1 Introducción

Los ICS son sistemas que administran los procesos industriales mediante la integración de autómatas interconectados entre sí y éstos hacia los sensores y actuadores, con el fin de supervisar y actuar en los procesos de fabricación en los diferentes tipos de industrias. Los sistemas SCADA se crearon para controlar las operatorias en los procesos industriales, integrando PC, servidores y redes de dispositivos automatizados. Luego, con el tiempo, surgió la necesidad de integrar la red corporativa e Internet a los ICS, exponiendo las amenazas y riesgos que ya existían también en éstos últimos. Al respecto, la criptografía puede ayudar a aplicar mecanismos de seguridad para la comunicación entre los PLCs y el sistema SCADA, encriptando la información que se transmitirá y mitigando las amenazas externas. (Kamlofsky y otros, 2015).

### 3.2 Evolución Histórica de los Sistemas IT/OT

Según lo especificado por la empresa Bigaidea (2022), históricamente las tecnologías enfocadas en la información (IT) y las orientadas a la operación (OT) han permanecido separadas, con sus respectivos equipos enfocados en tareas y objetivos distintos, e incluso con perfiles laborales diferentes. La comunicación y coordinación entre estas áreas ha sido limitada, y esta brecha se acentúa a medida que se descende en la estructura organizativa de la empresa.

No obstante, gracias a nuevos procesos y técnicas analíticas, se puede aprovechar la gran cantidad de datos generados en los sistemas productivos para obtener resultados novedosos y generar información detallada sobre el proceso de producción. Esto permite realizar correcciones,

optimizaciones y crear informes de valor para las capas de negocio, abriendo un conjunto de herramientas que facilitan la toma de decisiones más informadas desde el ámbito empresarial.

Bigaidea (2022) menciona que es relevante destacar la creciente adopción de tecnologías de red propias del ámbito de IT en la cadena productiva. Esto presenta una oportunidad para el intercambio de conocimientos entre los técnicos de red y comunicaciones.

Con una transformación cuidadosa, los beneficios derivados de una integración adecuada entre los sistemas y equipos de ambos mundos son cada vez más reconocidos y buscados en el entorno corporativo. Esto ha llevado a un aumento en el número de empresas que se embarcan en la tarea de integrar y conectar ambas partes de su operativa (Bidaidea, 2022).

### **3.3 Marco Demográfico y Revoluciones Industriales**

Antes de comenzar a abordar los conceptos fundamentales y detalles técnicos asociados a los sistemas SCADA, es necesario conocer el origen y las necesidades que comenzaron a surgir en el mundo relacionadas a la automatización de procesos industriales, así como también el control operativo y protección de dichos sistemas. Para ello, Contreras (2017) menciona que en Gran Bretaña se inició un proceso conocido como transición del régimen demográfico antiguo al moderno, marcando un cambio significativo en lugar de una revolución demográfica. Durante este periodo, se observó un incremento constante en el crecimiento de la población debido principalmente a una notable reducción en la tasa de mortalidad, lo que marcó una diferencia significativa con respecto al antiguo patrón demográfico caracterizado por altas tasas de mortalidad y crisis periódicas asociadas a la falta de alimentos. La población de Inglaterra y Gales aumentó de 5.8 millones en 1700 a alrededor de 9 millones en 1801.

Este crecimiento se atribuyó a mejoras significativas en la producción agrícola, lo que resultó en mejoras en la cantidad, calidad y variedad de alimentos. Además, los avances científicos del siglo XVIII marcaron el comienzo de cambios significativos en la medicina, tanto en la prevención como en el tratamiento de enfermedades, como el desarrollo de la vacuna contra la viruela. Los avances en higiene personal y general también contribuyeron a la reducción de la mortalidad, especialmente la infantil, que era alta en el antiguo régimen demográfico (Contreras, 2017).

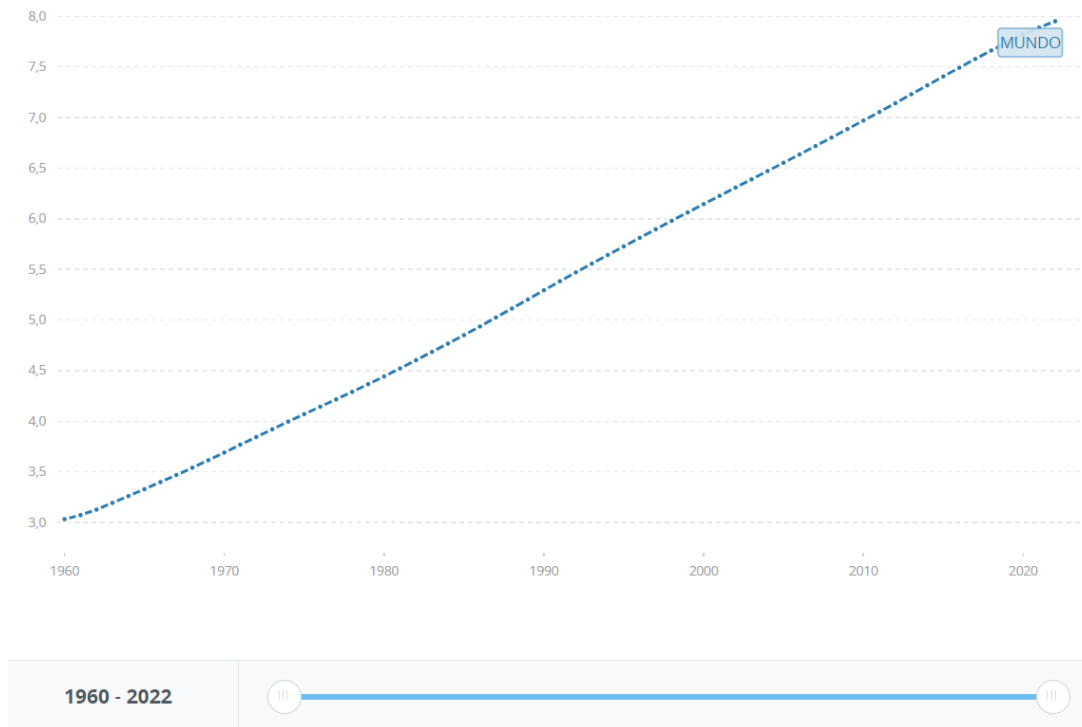
Este aumento demográfico tuvo importantes consecuencias, como el aumento de la fuerza laboral y de consumidores, fundamentales para el avance industrial y la creación de un sistema de producción masiva en las fábricas. Además, provocó cambios en la agricultura, impulsando las revoluciones agraria y agrícola, lo que también influyó en el crecimiento de la población.

Aunque el aumento en la población fue esencial para el cambio económico, como se observa en el caso de Inglaterra, es crucial reconocer que no basta por sí solo, ya que debe ir acompañado de otros cambios y procesos. Por ejemplo, en el caso de Irlanda, hubo un aumento en la población entre mediados del siglo XVIII y el XIX, pero no se tradujo en un progreso similar; en cambio, enfrentó graves crisis demográficas y una emigración masiva hacia los Estados Unidos (Self Bank, 2023).

En la Figura 9 se puede observar el crecimiento demográfico mundial desde el año 1960 hasta nuestros días:

**Figura 9**

*Población mundial en miles de millones de personas*



Nota. Obtenido de *Grupo Banco Mundial*, Banco Mundial, 2024

Ahora bien, este crecimiento demográfico demandó que el mundo evolucione y busque maneras de facilitar y automatizar las necesidades de la humanidad a través del uso de máquinas y herramientas sofisticadas para cada época.

Continuando con lo que indica Self Bank (2023), las revoluciones industriales se caracterizan por ser procesos de transformación profunda que afectan los ámbitos industrial, social y tecnológico. Estos cambios sustanciales implican una reconfiguración en la forma de producir y comercializar bienes y servicios, así como en la organización misma de la sociedad.

Aunque se mencionan distintas revoluciones industriales, la Primera Revolución Industrial, propiamente dicha, tuvo su origen en el siglo XVIII en Inglaterra, marcada por la invención de la



máquina de vapor y los enormes cambios que esta generó. Estos cambios fueron especialmente notables en la industria textil, así como en el ámbito del transporte, con la introducción del ferrocarril y los grandes barcos a vapor (Self Bank, 2023).

Estas transformaciones fueron el motor para cambiar una sociedad mayormente rural y local en una más urbana, mecanizada e interconectada, lo que a su vez permitió aumentar la producción y desvincularla del lugar de consumo.

Self Bank (2023) indica que el desarrollo de innovaciones como la electricidad y el motor de combustión representó un nuevo empuje a la fabricación de productos en grandes factorías y al transporte tanto de mercancías como de personas, desarrollándose además potentes industrias como la del petróleo y la del acero. A esta se la denominó Segunda Revolución Industrial (segunda mitad del siglo XIX-1914).

La Tercera Revolución Industrial (mediados del siglo XX) está basada en la difusión de la informática, que ha permitido potencialidades de cálculo y de manejo de equipos muy por encima de las del ser humano (Self Bank, 2023). Sin lugar a dudas la invención del primer PLC es lo que marcó esta revolución, el cual fue diseñado en el año 1968 por la empresa Bedford Associates, reemplazando los relés de un sistema de control por tarjetas electrónicas, lo que permitiría programar nuevas funciones sin necesidad de recablear o cambiar el hardware. Aquel modelo Modicon 84 (nombre que le asignaron sus creadores) ha ido creciendo en función de cómo evolucionaba la tecnología. Tal es así que de la conversión inicial con 500 instrucciones por segundo se ha pasado a las 50.000.000 de instrucciones por segundo en los últimos equipos desarrollados por Schneider Electric (InfoPLC++, 2019).

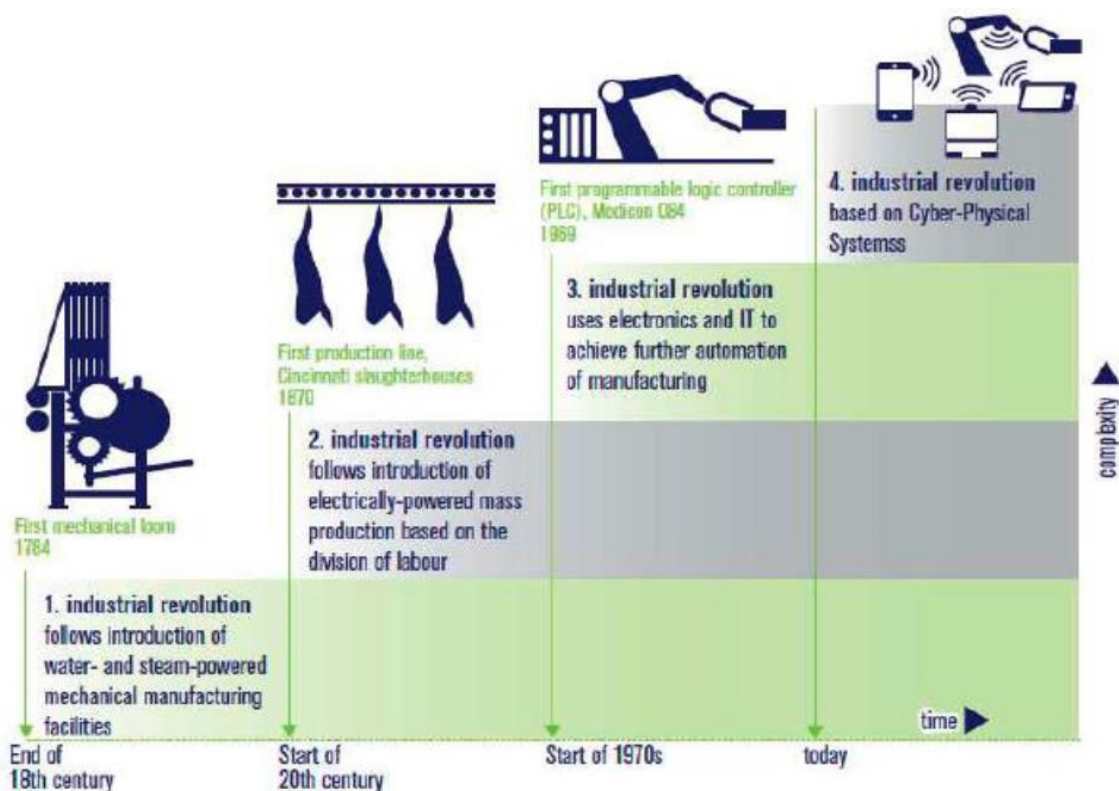
Respecto a la Cuarta Revolución Industrial (también llamada Industria 4.0), surge alrededor del año 2013 en Alemania. Al respecto, Lasi y Kemper (2014) destacan entre otras cosas

el uso de fábricas inteligentes, la interoperabilidad de sistemas físicos y digitales y la organización autónoma de los sistemas de fabricación de bienes de uso. Por otro lado, se crean nuevos sistemas de distribución y aprovisionamiento, adaptados a las necesidades humanas y no de forma inversa, de manera tal que el desarrollo de nuevos productos y servicios se realizan de forma individual.

En la Figura 10 se mencionan las características principales de las revoluciones industriales:

**Figura 10**

*Evolución cronológica de las revoluciones industriales*



Nota. Obtenido de *Recomendaciones para la aplicación de la iniciativa estratégica Industria 4.0*, por Kagermann, 2023

### 3.3.1 Industria 4.0

Tal como indican HERČKO et al. (2018), la primera mención del concepto de Industria 4.0 se presentó en 2011 en la Feria de Hannover. Posteriormente, en 2012, un grupo de trabajo liderado por Siegfried Dais (de Robert Bosch GmbH) y Henning Kagermann (de la Academia Alemana de Ciencia y Tecnología) desarrolló y finalizó este concepto en 2013. Mientras que la primera revolución industrial se basó en el uso de vapor y máquinas de vapor, la segunda en la electrificación, la tercera en computadoras y robots, la cuarta se fundamenta en el uso de los llamados sistemas ciberfísicos (CPS).

La idea principal del concepto es la interconectividad de maquinaria de producción, productos mecanizados y semielaborados, así como todos los demás sistemas y subsistemas de una empresa industrial (incluidos ERP, sistemas de ventas, etc.). Para crear una red distribuida e inteligente de diversas entidades a lo largo de la cadena de valor, estos sistemas operan relativamente de forma independiente y se comunican entre sí según sea necesario.

Los pilares fundamentales de la Industria 4.0 incluyen varios elementos clave. Los sistemas ciber-físicos (CPS) son cruciales en la integración del mundo físico y virtual. Estos sistemas combinan procesos físicos y computacionales, incorporando tanto gestión informática como procesos físicos que se complementan mutuamente. El desarrollo de los CPS se lleva a cabo en tres etapas: la primera generación emplea tecnologías de identificación como las etiquetas RFID para seguimiento y reconocimiento únicos; la segunda generación introduce sensores con capacidades limitadas; y la tercera generación mejora al incluir sensores avanzados capaces de almacenar y analizar datos mientras están conectados a la red (HERČKO y otros, 2015).

El Internet de las Cosas (IoT) es otro componente esencial, permitiendo que dispositivos como RFID, sensores y teléfonos móviles se conecten y colaboren para alcanzar objetivos

comunes. En este contexto, los CPS son considerados parte de esta red, y el IoT se define como un sistema en el que estos sistemas ciber-físicos trabajan juntos a través de conexiones únicas.

Además, HERČKO et al. (2018) indica que el Internet de los Servicios (IoS) facilita la oferta de servicios en línea. Incluye participantes, infraestructura, modelos de negocio y los servicios mismos, que son ofrecidos y combinados para crear servicios de mayor valor por diferentes proveedores, utilizando varias plataformas de comunicación.

Las fábricas inteligentes, por otro lado, representan instalaciones y maquinaria altamente avanzadas que no solo automatizan procesos, sino que también ofrecen soporte integral a las personas en sus tareas diarias. Estas fábricas se basan en la recopilación, procesamiento y análisis de información en tiempo real, lo que permite mantener un conocimiento continuo y preciso del estado y la ubicación de cada uno de los dispositivos y componentes que las conforman. Este enfoque reduce tiempos de inactividad, optimiza recursos y permite una toma de decisiones más informada y ágil. En el núcleo de estas fábricas, los sistemas integrados trabajan con una combinación de datos físicos y virtuales. Los datos físicos incluyen parámetros como la posición, estado operativo, rendimiento y posibles fallos de la maquinaria. Por otro lado, la información virtual abarca elementos como documentos electrónicos, planos digitales, algoritmos predictivos y modelos de simulación que contribuyen al diseño, monitoreo y mantenimiento de los procesos productivos. La integración de estos datos crea un entorno holístico que mejora la sincronización entre las operaciones humanas y las automatizadas.

En este contexto, los Sistemas Ciberfísicos (CPS) y el Internet de las Cosas (IoT) juegan un papel fundamental. Los CPS, a través de su capacidad para conectar y controlar sistemas físicos mediante redes de información, trabajan en conjunto con el IoT, que facilita la comunicación y el intercambio de datos entre dispositivos interconectados. Esta combinación permite que las

máquinas y sistemas colaboren entre sí de manera autónoma y eficiente, ajustándose dinámicamente a las condiciones del entorno y maximizando el rendimiento. Por lo tanto, las fábricas inteligentes representan un paso crucial hacia la transformación digital de la industria, al aprovechar tecnologías avanzadas para crear ecosistemas productivos más sostenibles, adaptativos y competitivos. (HERČKO y otros, 2015).

En la Tabla 1 se ilustran las relaciones entre principios y componentes:

**Tabla 1**

*Relaciones entre principios y componentes*

<b>Principios</b>	<b>CPS</b>	<b>IoT</b>	<b>IoS</b>	<b>Smart Factory</b>
Interoperabilidad	X	X	X	X
Virtualización	X	-	-	X
Descentralización	X	-	-	X
Capacidades en tiempo real	-	-	-	X
Orientación al servicio	-	-	X	-
Modularidad y reconfigurabilidad	-	-	X	-

Nota. Obtenido de *Design Principles for Industrie 4.0 Scenarios: A Literature Review*, por Hermann, 2015

### **Niveles de Automatización en la Industria**

Creado en la década de 1990, el modelo de referencia de Purdue es un modelo de flujo de datos de referencia para la fabricación integrada, lo que implica el uso de computadoras para gestionar todo el proceso de producción. Ofrece un marco para que las empresas permitan la

colaboración entre usuarios finales, integradores y proveedores en la integración de aplicaciones dentro de las capas clave de la red empresarial y la infraestructura de procesos (Checkpoint, 2022).

Fue adoptado por ISA-99 y empleado como modelo conceptual para la segmentación de redes en sistemas de control industrial (ICS). Este modelo ilustra las interconexiones e interdependencias de todos los componentes principales de un ICS típico, dividiendo la arquitectura en dos zonas: Tecnología de la Información (TI) y Tecnología Operativa (OT).

En la base del modelo de Purdue se encuentra la Tecnología Operativa (OT), que incluye los sistemas utilizados en infraestructuras críticas y manufactura para monitorear y controlar el equipo físico y los procesos operativos. En el modelo de Purdue, esta zona está separada de la zona de Tecnología de la Información (TI), que se encuentra en la parte superior del modelo. Entre ambas zonas, encontramos una DMZ que sirve para separar y controlar el acceso entre las zonas de TI y OT (Checkpoint, 2022).

Por otra parte, Madias (2018) indica que la automatización de unidades industriales de proceso se organiza usualmente en cinco niveles:

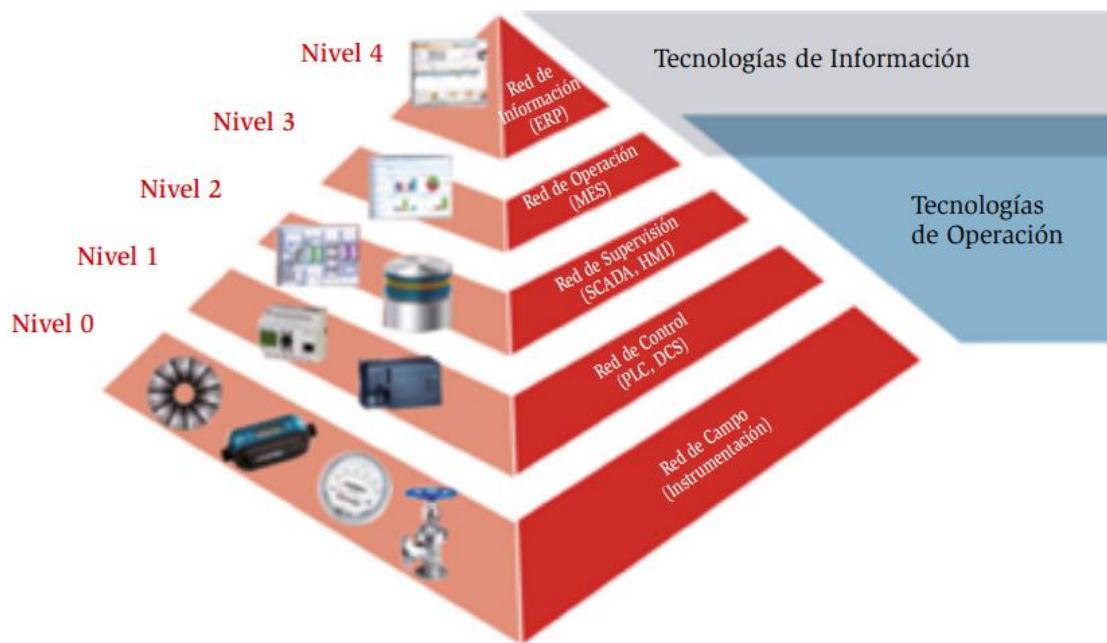
- Nivel 0: se trata de la adquisición de datos de campo, mediante instrumentos y sensores, para controlar los equipos.
- Nivel 1: es el nivel básico, que suele incluir sistemas de control con controladores básicos programables (PLC), e interfaces hombre-máquina (HMI, por sus iniciales en inglés), para la operación y monitoreo, en topologías de redes locales o generales, como las redes Ethernet. Los equipos de este nivel utilizan datos del proceso suministrados por los instrumentos del nivel 0.
- Nivel 2: incluye el control de seguimiento avanzado de productos, evaluación de calidad, optimización de la producción, etc.

- Nivel 3: se gestionan los flujos de trabajo para poder optimizar los procesos y productos.
- Nivel 4: se desarrollan todas las actividades relacionadas con el negocio, necesarias en una organización industrial, comunicando distintas unidades de producción y manteniendo relaciones con proveedores y clientes.

En la Figura 11 se puede apreciar la distribución de los niveles mencionados y ejemplos de los elementos más comunes para cada uno de ellos:

**Figura 11**

*Los cinco niveles de automatización y las tecnologías que suele utilizar*



Nota. Obtenido de *Sistemas de control de procesos en la acería*, Madias, 2018

## **3.4 Sistemas SCADA**

### **3.4.1 Introducción**

Los sistemas SCADA en su nivel fundamental son Sistemas de Control Industrial basados en computadoras que supervisan y controlan procesos industriales que existen en el mundo físico. Pueden encontrarse en instalaciones de fabricación, producción y procesamiento de petróleo, productos farmacéuticos, energía, tratamiento y distribución de agua, etc. Son el mejor método de control para procesos con grandes cantidades de datos que deben recopilarse y analizarse, que se extienden a grandes distancias y que requieren un control crítico en procesos veloces (Adams, 2014).

Para ello se deben utilizar diversos periféricos, software de aplicación, unidades remotas, sistemas de comunicación, etc., que le permiten al operador tener acceso completo al proceso mediante su visualización en una computadora tal como menciona Pérez-López (2015).

El primer tipo de SCADA se utilizó en aplicaciones tales como tuberías de gas y líquidos, la transmisión y distribución de energía eléctrica y en los sistemas de distribución de agua, para su control y monitoreo automático.

Hoy en día existen varios sistemas que permiten controlar y supervisar, tales como PLC, DCS y ahora SCADA, que se pueden integrar y comunicar entre sí mediante una red ethernet con el fin de que el operador pueda mejorar la interfaz en tiempo real. Esto permite no solo supervisar el proceso sino tener acceso al historial de las alarmas y variables de control con mayor claridad, combinar bases de datos relacionadas, presentar en una computadora, por ej. una plantilla Excel,



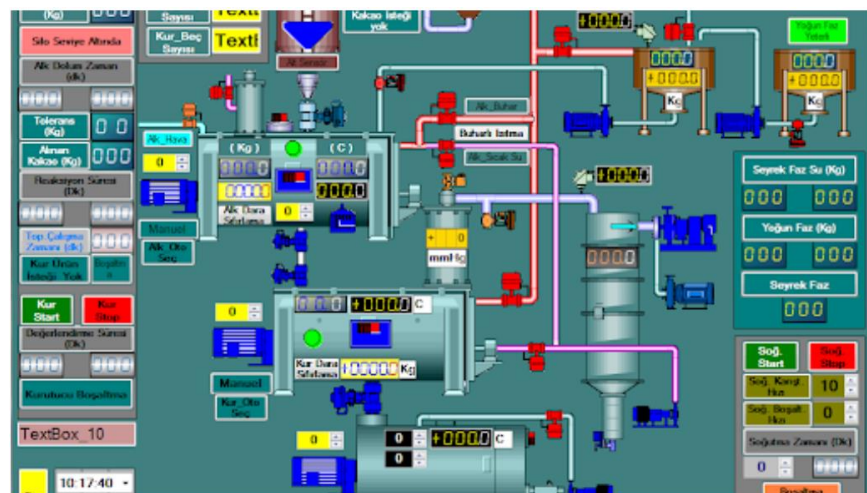
un documento Word, todo en ambiente Windows, con lo que todo el sistema resulta más amigable (Pérez-López, 2015).

Un sistema SCADA es un conjunto de aplicaciones diseñadas para operar en computadoras de control de producción, conectadas a la planta mediante comunicación digital con instrumentos y actuadores, y una interfaz gráfica para el operador. Originalmente destinado a la supervisión y adquisición de datos, ahora incluye hardware y buses especializados. Su interconexión se realiza a través de una interfaz PC-planta centralizada, permitiendo la comunicación con dispositivos de campo como controladores autónomos y autómatas programables. Esto facilita el control automático del proceso desde una computadora configurable y modificable, además de proporcionar información del proceso a diversos usuarios (Pérez-López, 2015).

La Figura 12 muestra un ejemplo de un sistema SCADA típico:

**Figura 12**

*Representación de un sistema SCADA*



Nota. Obtenido de *Explicación de los sistemas SCADA / Mantenimiento*, UpKeep, 2022

### 3.4.2 Arquitectura y Componentes de Hardware

#### HMI

La función de monitoreo de estos sistemas se realiza sobre una computadora industrial, ofreciendo una visión de los parámetros de control sobre la pantalla, lo que se denomina un HMI (iniciales de: Human Machine Interface), como en SCADA, pero sólo ofrecen una función complementaria de monitorización: observar mediante aparatos especiales el curso de uno o varios parámetros fisiológicos o de otra naturaleza para detectar posibles anomalías. Es decir, los sistemas de automatización de interfaz gráfica tipo HMI básicos ofrecen una gestión de alarmas básica, mediante las cuales la única opción que le queda al operario es realizar una parada de emergencia, reparar o compensar la anomalía y hacer un reset. Los sistemas SCADA utilizan un HMI interactivo que permite detectar alarmas y a través de la pantalla solucionar el problema mediante las acciones adecuadas en tiempo real. Esto les otorga una gran flexibilidad. En definitiva, el modo supervisor del HMI de un SCADA no solo señala los problemas, sino que, orienta en cuanto a los procedimientos para solucionarlos. A menudo, las palabras SCADA y HMI inducen a cierta confusión. Ciertamente es que todos los sistemas SCADA ofrecen una interfaz gráfica PC-Operario tipo HMI, pero no todos los sistemas de automatización que tienen HMI son SCADA. La diferencia radica en la función de supervisión que pueden realizar estos últimos a través del HMI (Pérez-López, 2015).

## **MTU (Master Terminal Unit)**

Se trata de la computadora principal del sistema, el cual supervisa y recoge la información del resto de las subestaciones, ya sean otros ordenadores conectados (en sistemas complejos) a los instrumentos de campo o directamente sobre dichos instrumentos. Este ordenador suele ser una PC que soporta el HMI. De esto se deriva que el sistema SCADA más sencillo es el compuesto por un único ordenador, que es el MTU que supervisa toda la estación.

El MTU tiene varias funciones clave. Una de sus tareas es interrogar periódicamente a las Unidades Terminales Remotas (RTU) y enviarles instrucciones, generalmente siguiendo un esquema de comunicación maestro-esclavo. Además, el MTU sirve como interfaz para los operadores, proporcionando la visualización de variables en tiempo real, gestionando alarmas y recopilando datos históricos para su presentación. También es capaz de ejecutar software especializado que lleva a cabo funciones específicas relacionadas con el proceso supervisado por el sistema SCADA, como la detección de fugas en un oleoducto (Pérez-López, 2015).

## **RTU (Remote Terminal Unit)**

Estas computadoras están situadas en los nodos estratégicos del sistema gestionando y controlando las subestaciones. Reciben las señales de los sensores de campo y comandan los elementos finales de control ejecutando el software de la aplicación SCADA. Se encuentran en el nivel intermedio o de automatización, estando a un nivel superior el MTU y a un nivel inferior los distintos instrumentos de campo que son los que ejercen la automatización física del sistema, control y adquisición de datos. Estos ordenadores no tienen que ser PC, ya que la necesidad de soportar un HMI no es tan grande a este nivel, por lo tanto, suelen ser computadoras industriales

tipo armarios de control, aunque en sistemas muy complejos puede haber subestaciones intermedias en formato HMI.

Una tendencia actual es dotar a los controladores lógicos programables (PLC) con la capacidad de funcionar como RTU gracias a un nivel de integración mayor y CPU con mayor potencia de cálculo. Esta solución minimiza costos en sistemas en los que las subestaciones no sean muy complejas, sustituyendo el ordenador industrial mucho más costoso (Pérez-López, 2015).

## **Red de Comunicación**

Pérez-López (2015) menciona que es el nivel que gestiona la información que los instrumentos de campo envían a la red desde el sistema. El tipo de BUS utilizado en las comunicaciones puede ser muy variado según las necesidades del sistema y del software escogido para implementar el sistema SCADA, ya que no todos los softwares (ni los instrumentos de campo como PLC) pueden trabajar con todos los tipos de BUS.

Hoy en día, gracias a la estandarización de las comunicaciones con los dispositivos de campo, se puede implementar un sistema SCADA sobre prácticamente cualquier tipo de BUS. Se encuentran SCADA sobre formatos estándares como los RS-232, RS-422 y RS-485 a partir de los cuales, y mediante un protocolo TCP/IP, se puede conectar el sistema sobre un bus en configuración DMS ya existente, pasando por todo tipo de buses de campo industriales hasta formas más modernas de comunicación como Bluetooth (Bus de Radio), microondas, satélite, cable, etc.

A parte del tipo de BUS, existen interfaces de comunicación especiales para la comunicación en un sistema SCADA, como pueden ser módems para estos sistemas que soportan

los protocolos de comunicación SCADA y facilitan la implementación de la aplicación. Otra característica de SCADA es que la mayoría se implementa sobre sistemas WAN de comunicaciones, es decir, los distintos terminales RTU pueden estar deslocalizados geográficamente (Pérez-López, 2015).

### **Instrumentos de Campo**

Son todos aquellos que permiten realizar tanto la automatización o control del sistema (PLC, controladores de procesos industriales y actuadores en general) como los que se encargan de la captación de información del sistema (sensores y alarmas). Una característica de los SCADA es que sus componentes son diseñados por distintos proveedores, sin coordinación entre sí. De manera que se tienen diferentes proveedores para las RTU (incluso es posible que un sistema utilice RTU de más de un proveedor), módems, radios, software de supervisión e interfaz con el operador, de detección de pérdidas, etc. (Pérez-López, 2015).

### **PLC**

Según explica Vallejo (2019), de una manera general podemos definir al controlador lógico programable como toda máquina electrónica diseñada para controlar en tiempo real y en medio industrial procesos secuenciales de control. Su programación y manejo pueden ser realizados por personal con conocimientos eléctricos o electrónicos, sin previos conocimientos sobre informática.

Los controladores lógicos programables surgieron a finales de los años 60 y principios de los 70, con sus orígenes en la industria automotriz. Estas industrias dependían de sistemas industriales basados en relés para impulsar sus procesos de fabricación.

En el año 1968, General Motors tuvo la idea de crear algo llamado "Controlador Lógico Programable" para ahorrar dinero en sistemas de control. Expusieron cuidadosamente las especificaciones para este controlador, que describían un sistema de control por relé que podría usarse no sólo en la industria automotriz, sino también en cualquier industria manufacturera. Estas especificaciones llamaron la atención de empresas como GEFanuc, Reliance Electric, MODICON y Digital Equipment Co. Sus esfuerzos finalmente llevaron a la creación de lo que ahora conocemos como el controlador lógico programable (Vallejo, 2019).

Con el avance de la electrónica y la tecnología de microprocesadores en la década de 1970, los PLC experimentaron un importante avance. Esto trajo mejoras notables en su capacidad para interactuar con el operador, ampliar las capacidades de datos, utilizar términos de video y desarrollar programas. El Control Lógico Programable es ideal para ser operado en condiciones críticas industriales, ya que fue diseñado y concebido para su uso en el medio ambiente industrial. En un entorno industrial, un controlador lógico programable (PLC) es cualquier máquina electrónica que controla procesos secuenciales en tiempo real.

Los procesos industriales suelen requerir de un PLC cuando tienen necesidades específicas como espacio reducido, procesos de producción variables, procesos de producción secuenciales, instalaciones de procesos complejos y necesidades de chequeo de programación centralizada de las partes del proceso (Vallejo, 2019).

De esta manera, son ampliamente utilizados en el control de maniobras de máquinas, maniobra de instalaciones y en aplicaciones de señalización y control.

Dependiendo del tipo de PLC que se esté utilizando, tanto las entradas como las salidas se mantienen separadas del CPU. En la mayoría de los casos, se emplean optoacopladores para las entradas, mientras que se utilizan relés u optoacopladores para las salidas.

Un componente esencial del "corazón" de la CPU es el microprocesador. La tarea vital de procesar el programa de usuario que estamos a punto de presentar se asigna a la unidad central de procesamiento (CPU). Para lograr esto, tenemos una serie de áreas de memoria, registros e instrucciones de programa ubicadas en la parte superior del diagrama de bloques. En modelos más avanzados, como los que tienen reguladores PID y control de posición, las funciones ya se pueden integrar en la CPU.

Respecto a la memoria, Vallejo (2019) indica que ésta posee varias secciones encargadas de distintas funciones. Así tenemos:

- Memoria del programa de usuario: aquí introduciremos el programa que el PLC va a ejecutar cíclicamente.
- Memoria de la tabla de datos: es la zona encargada de atribuir las funciones específicas del programa. Se suele subdividir en zonas según el tipo de datos (como marcas de memoria, temporizadores, contadores, etc.).
- Memoria del sistema: aquí se encuentra el programa en código de máquina que monitoriza el sistema (programa del sistema o firmware). Este programa es ejecutado directamente por el microprocesador/microcontrolador que posea el PLC.
- Memoria de almacenamiento: se trata de una memoria externa que empleamos para almacenar el programa de usuario, y en ciertos casos parte de la memoria de la tabla de datos. Suele ser de uno de los siguientes tipos: EPROM, EEPROM, o FLASH.

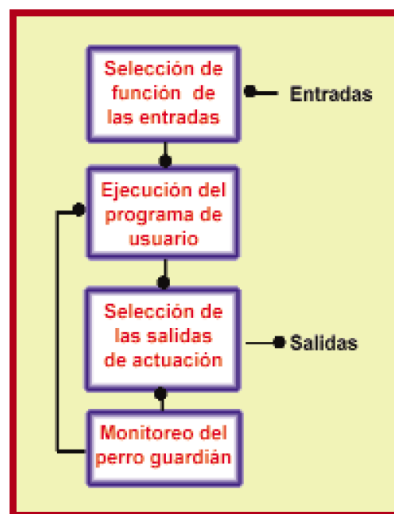
Respecto a la Unidad de proceso Central (CPU) podemos decir que es la encargada de ejecutar el programa de usuario mediante el programa del sistema (es decir, el programa de usuario es interpretado por el programa del sistema). Sus funciones son vigilar que el tiempo de ejecución del programa de usuario no exceda un determinado tiempo máximo (tiempo de ciclo máximo). A

esta función se la suele denominar Watchdog (perro guardián). También se encarga de ejecutar el programa de usuario, crear una imagen de las entradas, ya que el programa de usuario no debe acceder directamente a dichas entradas. Otra función es la de renovar el estado de las salidas en función de la imagen de las mismas obtenida al final del ciclo de ejecución del programa de usuario. Por último, también se encarga de realizar el chequeo del sistema (Vallejo, 2019).

Los PLCs poseen un ciclo de trabajo que ejecutarán de forma continua el diagrama de flujo, tal como se muestra en la Figura 13:

### Figura 13

Diagrama de flujo en el ciclo de trabajo de un PLC



Nota. Obtenido de *Los Controladores Lógicos Programables*, por Vallejo, 2019

Vallejo (2019) indica que se desprenden los siguientes componentes principales:

- Unidades de E/S: generalmente se dispone de dos tipos digitales y analógicas. Mientras que las primeras se basan en el principio de todo o nada, es decir no conducen señal alguna o poseen un nivel mínimo de tensión. Estas E/S se manejan nivel de bit dentro del programa de usuario. Respecto a las analógicas, pueden poseer cualquier valor dentro de un rango



determinado especificado por el fabricante. Se basan en conversores A/D y D/A aislados de la CPU (ópticamente o por etapa de potencia). Estas señales se manejan a nivel de byte o palabra (8/16 bits) dentro del programa de usuario.

- Interfaces: todo PLC posee la virtud de poder comunicarse con otros dispositivos (como una PC). Lo normal es que posea una interfase serie del tipo RS-232 / RS422. A través de esta línea se pueden manejar todas las características internas del controlador, incluida la programación del mismo, y suele emplearse para monitorización del proceso en otro lugar separado.
- Unidades de Programación: el modo más empleado para programar un PLC es mediante una computadora tipo PC. Permite programar desde un ordenador personal estándar, con todo lo que ello supone: herramientas más potentes, posibilidad de almacenamiento en soporte magnético, impresión, transferencia de datos, monitorización mediante software SCADA, etc. Para cada caso el fabricante proporciona lo necesario, bien el equipo o el software/cables adecuados. Cada equipo, dependiendo del modelo y fabricante, puede poseer una conexión a uno o varios de los elementos anteriores.
- Dispositivos Periféricos: el PLC, en la mayoría de los casos, puede ser ampliable. Las ampliaciones abarcan un gran abanico de posibilidades, que van desde las redes internas (LAN, etc.), módulos auxiliares de E/S, memoria adicional, etc. hasta la conexión con otros autómatas del mismo modelo. Cada fabricante facilita las posibilidades de ampliación de sus modelos, los cuales pueden variar incluso entre modelos de la misma serie (Vallejo, 2019).

En la Figura 14 se puede apreciar a modo de ejemplo un PLC de la marca Schneider Electric donde se pueden observar varios de los elementos descriptos en los apartados anteriores:

**Figura 14**

*PLC marca Schneider Electric modelo M221*



Nota. Obtenido de *M221 PLC 16 ES Rele ETH Compact*, Schenider Electric, 2024

### 3.4.3 OpenScada

En la actualidad existen diversas versiones licenciadas del software SCADA en el mercado que ofrecen empresas al público e industrias en general. Pero también existen versiones gratuitas que pueden utilizarse para desarrollar soluciones a medida adaptables según las necesidades del usuario final.

OpenScada (2018) representa un sistema SCADA o HMI abierto construido sobre los principios de modularidad, multiplataforma y escalabilidad. Está genéricamente destinado a: adquisición, archivo (historial de conducta), visualización de la información, emisión de acciones

de control, y también para otras operaciones relacionadas, que son características de los sistemas SCADA o HMI con todas las funciones.

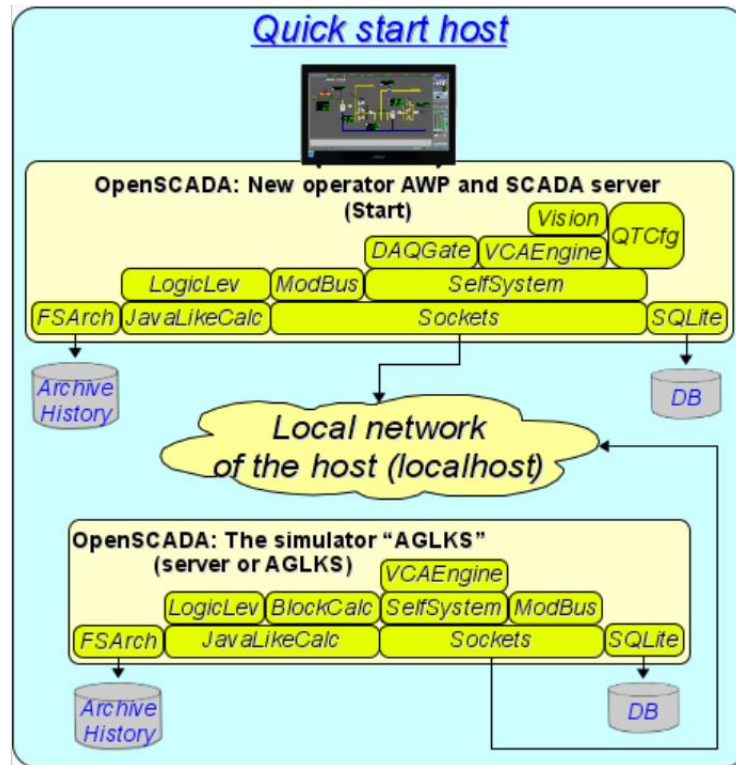
Las empresas que se dedican a la implantación de ACS-TP (Sistemas de Control de Automatización de Procesos Tecnológicos), están interesadas en el control total del sistema SCADA, que implantan en los objetos del cliente. El Cliente es el último eslabón de la cadena de creación del programa. La calidad de la interacción del Cliente con el desarrollador es directamente proporcional a la satisfacción del Cliente, así como a la velocidad de mejora del programa. La adaptación de un sistema SCADA comercial terminado suele conducir al deterioro o a la falta total de interacción entre el Cliente y el desarrollador (OpenScada, 2018).

Hay varias soluciones posibles para abordar este problema. Una opción es formar vínculos cercanos con el fabricante del sistema SCADA, lo que implica una integración directa o indirecta con su unidad de ejecución, aunque esto puede significar perder parcial o totalmente la independencia. Otra alternativa es desarrollar un sistema SCADA propio y comercial, lo que ofrece control total. Sin embargo, este enfoque requiere un equipo amplio de especialistas altamente cualificados, algo que las pequeñas empresas dedicadas a implementar ASC-TP suelen no tener. Además, el resultado puede ser un sistema SCADA que no alcance el nivel de los productos comerciales más básicos, con código de baja calidad y funciones mediocres. La tercera posibilidad es optar por sistemas SCADA de código abierto o de desarrollo conjunto. Esto combina los beneficios de las otras opciones al ofrecer control completo sobre el sistema sin necesidad de un gran equipo de expertos altamente cualificados. También mejora la calidad del sistema al aprovechar la experiencia de numerosos especialistas externos y la variedad de plataformas soportadas, permitiendo seleccionar una plataforma por sus ventajas específicas y no solo por su

compatibilidad con el sistema SCADA (OpenScada, 2018). En la Figura 15 se muestra un ejemplo de una integración típica de un sistema SCADA:

**Figura 15**

*Conexión simple de la estación SCADA y el servidor con una base de datos demo*



Nota. Obtenido de *OpenScada*, 2018

### 3.5 Principales Protocolos Industriales de Comunicación

#### 3.5.1 Introducción

Según menciona SDI (2022), los protocolos de comunicación son estándares que están formados por procedimientos, restricciones y formatos, que permiten el intercambio de un

conjunto de información, lo cual puede lograr la correcta comunicación entre servidores o dispositivos a través de una red. Para todo ello, los protocolos de comunicación incluyen ciertos mecanismos que permiten que los dispositivos se identifiquen y establezcan conexiones entre sí. También se incluyen normas que especifican cómo son los paquetes y los datos en cada mensaje enviado y recibido.

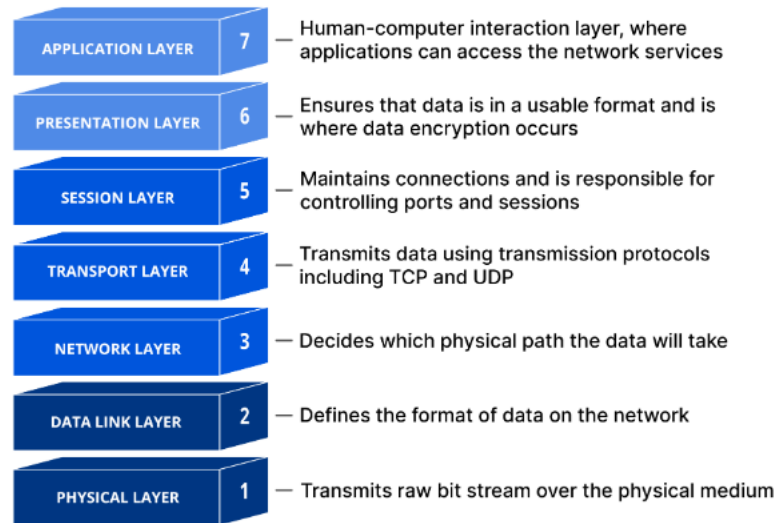
Los sistemas de automatización industrial generalmente se despliegan mediante una arquitectura distribuida y de código abierto, utilizando comunicaciones basadas en redes digitales. A medida que estos sistemas se expanden, aumentando el número de dispositivos conectados entre sí, se ha vuelto cada vez más evidente la necesidad de establecer un estándar de comunicación que facilite la integración de cada componente de manera uniforme, sin importar su tipo, propósito o fabricante. Un ejemplo de esta normalización es el modelo OSI (Open Systems Interconnection) que posibilita una comunicación fiable entre dispositivos, independientemente de su origen (SDI, 2022).

## **Modelo OSI**

El modelo OSI se puede ver como un lenguaje universal para la conexión de las redes de equipos. Se basa en el concepto de dividir un sistema de comunicación en siete capas abstractas, cada una apilada sobre la anterior, teniendo una función específica y comunicándose con las capas superiores e inferiores (CloudFlare, 2024). En la Figura 16 se muestran las diferentes capas de este modelo:

**Figura 16**

*Modelo OSI*



Nota. Obtenido de *¿Qué es el modelo OSI?*, CloudFlare, 2024

La empresa CloudFlare (2024) describe las siete capas de abstracción del modelo OSI de la siguiente manera:

- **Capa de Aplicación (7):** es la única capa que tiene un contacto directo con la información del usuario. Las aplicaciones de software, como navegadores web y clientes de correo electrónico, utilizan la capa de aplicación para iniciar comunicaciones. Es importante destacar que las aplicaciones de software cliente no están incluidas en la capa de aplicación. En cambio, esta capa se encarga de los protocolos y del procesamiento de datos necesarios para que el software presente información relevante al usuario.
- **Capa de presentación (6):** la responsabilidad principal de esta capa es preparar los datos para su utilización por parte de la capa de aplicación, es decir, facilita que los datos estén listos para ser consumidos por las aplicaciones. La capa de presentación se encarga de

tareas como la traducción, cifrado y compresión de los datos. Cuando dos dispositivos de comunicación se conectan, es posible que utilicen métodos de codificación diferentes, por lo que esta capa tiene la tarea de convertir los datos entrantes a una sintaxis comprensible para la capa de aplicación del dispositivo receptor. En el caso de una comunicación cifrada, la capa 6 se encarga de agregar el cifrado en el extremo del emisor y descifrarlo en el extremo del receptor, asegurándose de presentar datos legibles a la capa de aplicación. Adicionalmente, la capa de presentación comprime los datos recibidos de la capa de aplicación antes de enviarlos a la capa 5. Este proceso contribuye a mejorar la velocidad y eficiencia de la comunicación al reducir la cantidad de datos transferidos.

- Capa de Sesión (5): se encarga de abrir y cerrar comunicaciones entre dispositivos, denominando "sesión" al tiempo entre inicio y cese de la comunicación. Asegura que la sesión permanezca abierta el tiempo necesario para la transferencia de datos, cerrándola rápidamente para evitar desperdicio de recursos. Además, coordina la transferencia usando puntos de control. En caso de interrupción, la sesión se reinicia desde el último punto de control, reduciendo la cantidad de datos pendientes de transmisión. Sin puntos de control, la transferencia completa debería reiniciarse desde cero.
- Capa de Transporte (4): se encarga de las comunicaciones de extremo a extremo entre dos dispositivos. Antes de enviar los datos a la capa 3, esta capa toma la información de la capa de sesión y la segmenta. En el dispositivo receptor, la capa de transporte es responsable de reensamblar estos segmentos para construir datos que la capa de sesión pueda utilizar. Además, la capa de transporte asume la responsabilidad del control de flujo y de errores. El control de flujo determina la velocidad óptima de transmisión para evitar que un emisor con una conexión rápida sobrecargue a un receptor con una conexión lenta. En el extremo

receptor, la capa de transporte realiza un control de errores asegurándose de que los datos recibidos estén completos y solicitando una retransmisión en caso contrario. Los protocolos de la capa de transporte incluyen el Protocolo de Control de Transmisión (TCP) y el Protocolo de Datagramas de Usuario (UDP).

- Capa de Red (3): tiene la responsabilidad de facilitar la transferencia de datos entre dos redes distintas. Cuando los dispositivos de comunicación están en la misma red, la capa de red no desempeña un papel esencial. En el dispositivo emisor, esta capa divide los segmentos provenientes de la capa de transporte en unidades más pequeñas denominadas paquetes y luego los vuelve a ensamblar en el dispositivo receptor. Además, la capa de red se encarga de determinar la mejor ruta física para que los datos alcancen su destino, un proceso conocido como enrutamiento. Los protocolos asociados con la capa de red incluyen la dirección IP, el Protocolo de mensajes de control de Internet (ICMP), el Protocolo de mensajes de grupo de Internet (IGMP) y el paquete IPsec.
- Capa de Enlace de Datos (2): La capa de enlace de datos guarda similitudes con la capa de red, con la diferencia de que se encarga de facilitar la transferencia de datos entre dos dispositivos dentro de la misma red. Su función principal consiste en tomar los paquetes provenientes de la capa de red y dividirlos en fragmentos más pequeños conocidos como tramas. Similar a la capa de red, esta capa asume la responsabilidad del control de flujo y la gestión de errores en las comunicaciones internas de la red, mientras que la capa de transporte se ocupa exclusivamente del control de flujo y errores en las comunicaciones dentro de la red.
- Capa Física (1): en esta capa se encuentran los elementos físicos que participan en la transmisión de datos, como los cables y los interruptores de red. Además, es en este nivel



donde la información se transforma en una sucesión de bits, es decir, en una secuencia de unos y ceros. Para que los dispositivos puedan distinguir entre unos y ceros, es esencial que la capa física de ambos esté configurada con una convención de señal acordada (CloudFlare, 2024).

### **3.5.2 Modbus**

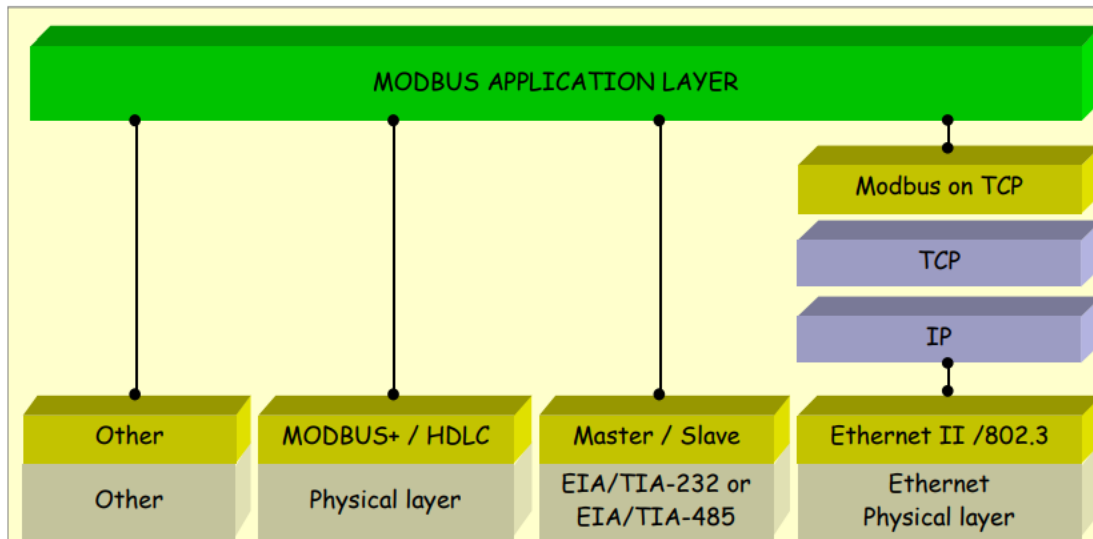
Según explica la empresa Modbus (2012) en su artículo, se trata de un protocolo de mensajería de capa de aplicación, situado en el nivel 7 del modelo OSI, que proporciona comunicación cliente/servidor entre dispositivos conectados en diferentes tipos de buses o redes. Diseñado por la empresa Modicon, es un estándar de facto en serie del sector desde 1979 que sigue permitiendo la comunicación entre millones de dispositivos de automatización. Ofrece servicios especificados por códigos de función. Los códigos de función Modbus son elementos de las PDU de solicitud/respuesta Modbus.

Hay varias implementaciones del protocolo Modbus, entre las más destacadas se encuentran: Modbus RTU, que utiliza transmisión serie asíncrona por diversos medios como cables (EIA/TIA-232-E, EIA-422, EIA/TIA-485-A), fibra óptica, o radio. Modbus ASCII se emplea en comunicaciones serie y utiliza caracteres ASCII para el protocolo de comunicación, incorporando un control de redundancia longitudinal (LRC) como checksum. También está Modbus TCP/IP, y finalmente, Modbus Plus, que es un protocolo de alta velocidad que opera mediante un sistema de token a través de la red (Modbus, 2012).

En la Figura 17 se muestra un diagrama de este protocolo:

**Figura 17**

*Pila de Comunicación Modbus*



Nota. Obtenido de *Modbus Application Protocol Specification V1.1b3*, Modbus, 2012

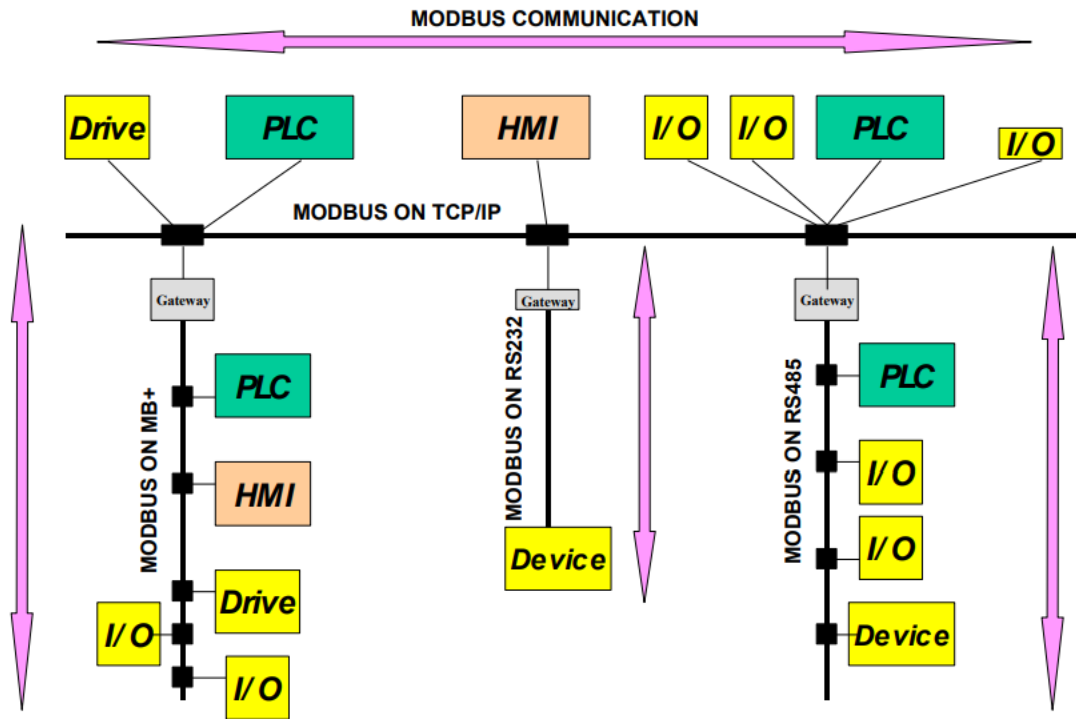
El protocolo Modbus permite una comunicación sencilla en todo tipo de arquitecturas de red.

Cualquier tipo de dispositivo (PLC, HMI, panel de control, controlador, control de movimiento, dispositivo de E/S, etc.) puede utilizar el protocolo Modbus para iniciar una operación remota (Modbus, 2012).

La misma comunicación puede realizarse tanto en una línea serie como en una red Ethernet TCP/IP Ethernet. Las pasarelas permiten una comunicación entre varios tipos de buses o redes utilizando el protocolo Modbus. En la Figura 18 se puede apreciar un ejemplo de una arquitectura Modbus:

**Figura 18**

*Ejemplo de arquitectura de red MODBUS*



Nota. Obtenido de *Modbus Application Protocol Specification V1.1b3*, Modbus, 2012

## Modbus RTU y ASCII

Según el artículo de la empresa Modbus (2006), se trata de la implementación más común del protocolo Modbus y se estandariza sobre línea serie para intercambiar peticiones entre un maestro y uno o varios esclavos, por lo que tiene lugar en los niveles 1 y 2 del modelo OSI.

Un sistema de tipo maestro-esclavo tiene un nodo maestro que emite comandos explícitos a uno de los nodos "esclavos" y procesa respuestas. Los nodos esclavos no suelen transmitir datos sin una petición del nodo maestro y no se comunican con otros nodos esclavos.

A nivel físico, los sistemas MODBUS sobre línea serie pueden utilizar diferentes interfaces físicas (RS485, RS232), aunque la interfaz TIA/EIA-485 (RS485) es la más común. Pero la

interfaz serie TIA/EIA-232-E (RS232) también puede utilizarse cuando sólo se requiere una comunicación punto a punto corta (Modbus, 2006).

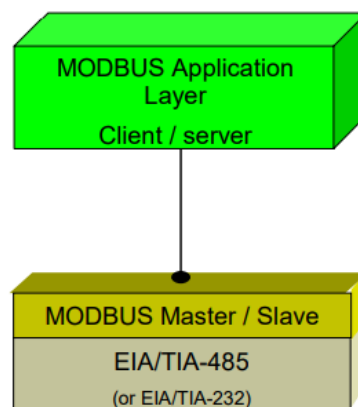
La capa de enlace de datos se divide en dos subcapas distintas. Una de ellas es el protocolo maestro/esclavo, y la otra se refiere al modo de transmisión, que puede ser RTU o ASCII.

La Figura 19 ofrece una representación general de la pila de comunicaciones serie Modbus comparada con las 7 capas del modelo OSI:

**Figura 19**

*Protocolo Modbus serie comparado con el modelo OSI*

Layer	ISO/OSI Model	
7	Application	MODBUS Application Protocol
6	Presentation	Empty
5	Session	Empty
4	Transport	Empty
3	Network	Empty
2	Data Link	MODBUS Serial Line Protocol
1	Physical	EIA/TIA-485 (or EIA/TIA-232)



Nota. Obtenido de *Modbus over Serial Line Specification and Implementation Guide V1.02*, Modbus, 2006

El modo Modbus RTU es la implementación más común, ya que utiliza codificación binaria y comprobación de errores CRC. Los mensajes Modbus ASCII (aunque algo más legibles porque utilizan caracteres ASCII) son menos eficientes y utilizan una comprobación de errores CRC menos eficaz. El modo ASCII utiliza caracteres ASCII para comenzar y terminar los mensajes, mientras que RTU utiliza espacios de tiempo (3,5 veces el carácter) de silencio para el encuadre. Los dos modos son incompatibles, por lo que un dispositivo configurado para el modo

ASCII no puede comunicarse con uno que utilice RTU. Los mensajes Modbus ASCII requieren el doble de bytes para transmitir el mismo contenido que un mensaje Modbus RTU (ProSoft Technology, 2019).

## **Modbus TCP/IP**

Según la empresa Modbus (2018), se trata del protocolo Modbus RTU con una interfaz TCP que se ejecuta en Ethernet. La estructura de mensajería Modbus es el protocolo de aplicación que define las reglas para organizar e interpretar los datos independientemente del medio de transmisión.

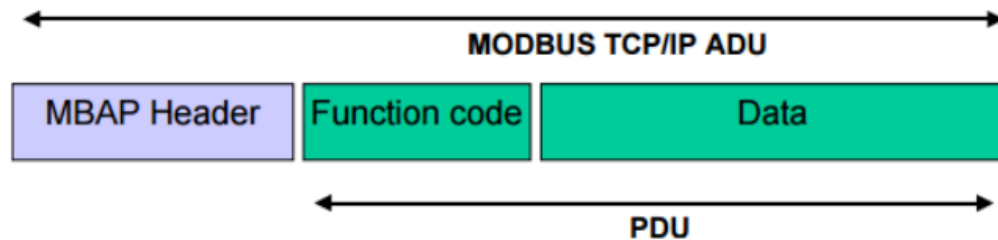
La función principal de TCP es que todos los paquetes de datos se reciban correctamente, mientras que IP garantiza que los mensajes se dirijan y enruten correctamente.

Así que, en resumen, Modbus TCP/IP utiliza TCP/IP y Ethernet para transportar los datos de la estructura de mensajes Modbus entre dispositivos compatibles. Es decir, Modbus TCP/IP combina una red física (Ethernet), con un estándar de red de red (TCP/IP), y un método estándar de representación de datos (Modbus como el protocolo de aplicación). En la práctica, Modbus TCP incrusta una trama de datos Modbus estándar en una trama TCP sin la suma de comprobación Modbus (Modbus, 2018).

Ahora bien, la especificación Modbus/TCP define una Unidad de Datos de Aplicación (ADU). Esta ADU se define como se muestra en la Figura 20:

**Figura 20**

*Modbus/TCP ADU*



Nota. Obtenido de *MODBUS/TCP Security Protocol Specification*, Modbus, 2018

La diferencia entre una Unidad de Datos de Protocolo Modbus (PDU) tradicional y la ADU es la adición de la cabecera Modbus Application Protocol (mbap) en la parte delantera de la trama (Modbus, 2018).

En 1996, el protocolo Modbus/TCP se registró en IANA (Internet Assigned Number Authority) y se le asignó el número de puerto de sistema 502. Durante este proceso de registro, el protocolo Modbus/TCP pasó a denominarse protocolo mbap debido a la cabecera mbap en el ADU Modbus/TCP.

El protocolo Modbus/TCP Security es una variante centrada en la seguridad del protocolo Modbus/TCP que utiliza Transport Layer Security (TLS).

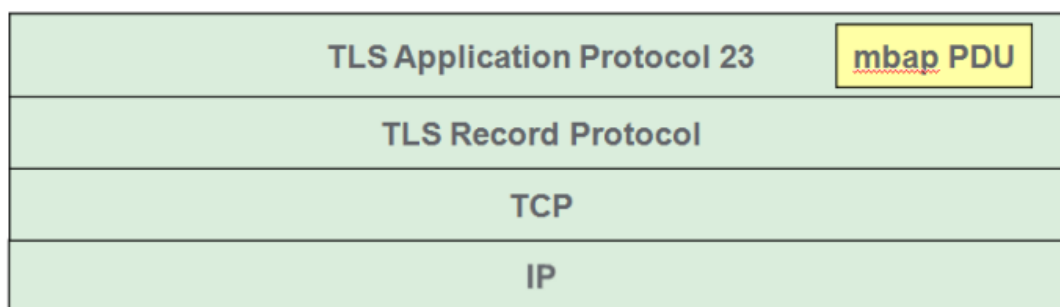
Como se puede observar en la Figura 21, PDU mbap se encuentra encapsulada en TLS proporcionando un protocolo centrado en la seguridad alternativo a mbap y añadiendo transporte confidencial de los datos, integridad de los datos, protección anti-repetición, autenticación del punto final a través de certificados y la autorización a través de la información incrustada en el certificado, tales como usuario y funciones del dispositivo (Modbus, 2018).

En mbaps, el protocolo mbap se transporta a través de TLS ofreciendo una capacidad de autenticación mediante certificados x.509v3. Los clientes y servidores mbaps deben estar provistos de estos certificados para participar en la función de autenticación TLS.

TLS permite el uso de claves precompartidas para establecer una conexión segura, pero su uso no se tiene en cuenta en esta especificación ya que no permite la transferencia de información de rol para proporcionar una función de autorización (Modbus, 2018).

**Figura 21**

*Mbap PDU encapsulado in TLS*



Nota. Obtenido de *MODBUS/TCP Security Protocol Specification*, Modbus, 2018

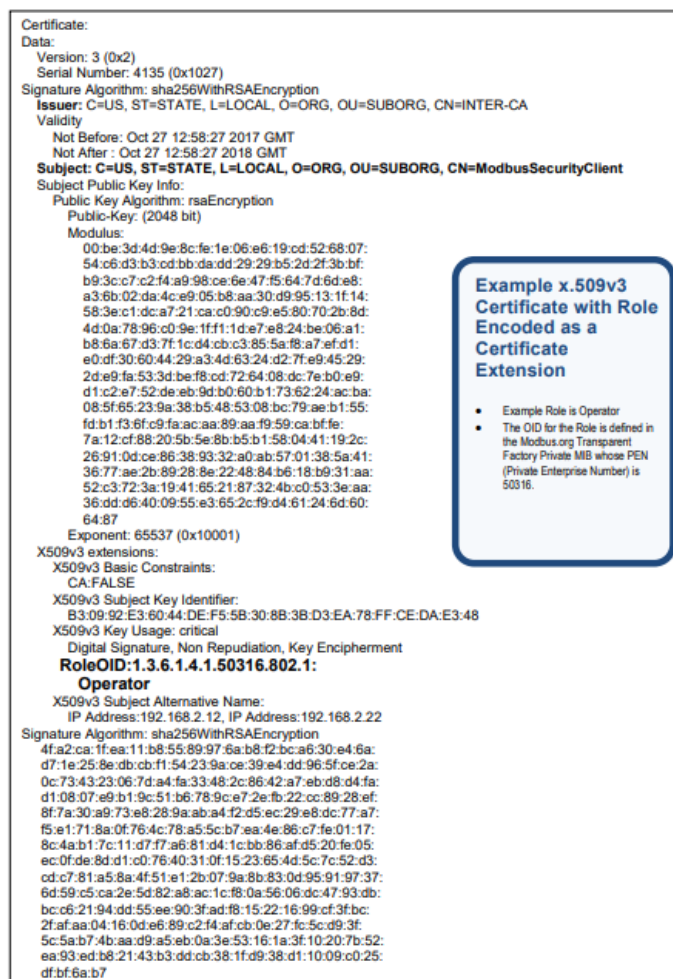
TLS proporciona seguridad de capa de transporte entre dos puntos finales. Para ello, los puntos finales TLS ejecutan el protocolo TLS Handshake para negociar los parámetros de seguridad y crear una sesión TLS.

Para que dos dispositivos mbaps se comuniquen de forma segura utilizando TLS, debe establecerse un contexto de seguridad entre los puntos finales de la conexión TLS. El protocolo TLS Handshake establece el contexto seguro, es decir, la sesión TLS. Ésta tiene un identificador de sesión y el contexto de seguridad se describe mediante un conjunto de parámetros de seguridad. La autenticación mutua requiere que cada punto extremo envíe su cadena de certificados de

dominio al punto extremo remoto. Una vez recibida la cadena de certificados del punto remoto, el punto extremo TLS verificará la firma de cada certificado utilizando el siguiente certificado CA de la cadena hasta que pueda verificar la raíz de la cadena (Modbus, 2018). En la Figura 22 se muestra un ejemplo de un certificado digital:

**Figura 22**

*Ejemplo de certificado x.509 v3 con extensión de función*



Nota. Obtenido de *MODBUS/TCP Security Protocol Specification*, Modbus, 2018



## **Modbus Plus**

Bello et al. (2013) explica que Modbus Plus es una variante del protocolo Modbus, que fue desarrollado originalmente por Modicon (ahora parte de Schneider Electric) en la década de 1970. Utiliza una arquitectura de red en anillo, lo que significa que los dispositivos se conectan en un bucle cerrado, formando un anillo de comunicación. Esto proporciona redundancia y asegura que la comunicación pueda continuar incluso si hay un fallo en un segmento de la red.

El protocolo utiliza una topología de maestro/esclavo, donde un dispositivo maestro inicia las comunicaciones y los dispositivos esclavos responden a las solicitudes del maestro. Esto permite la coordinación y el control eficiente de los dispositivos conectados.

Entre sus principales características se incluyen una topología en anillo, que mejora la fiabilidad de la red al ofrecer rutas redundantes para la comunicación. También soporta velocidades de transmisión de hasta 1 Mbit/s, lo que asegura una comunicación rápida y eficiente entre los dispositivos. La arquitectura de maestro/esclavo permite una adecuada coordinación y control de los dispositivos en la red. Además, ofrece un alto nivel de determinismo, garantizando tiempos de respuesta predecibles y consistentes (Bello y otros, 2013).

Modbus Plus opera principalmente en las capas física y de enlace del modelo OSI. Utiliza el estándar RS-485 para la capa física y define un protocolo de enlace de datos específico.

Es importante tener en cuenta que, aunque Modbus Plus sigue siendo utilizado en algunos entornos industriales, también existen otros protocolos más modernos, como Modbus TCP/IP, que ofrecen características avanzadas y compatibilidad con redes Ethernet industriales. La elección del protocolo dependerá de los requisitos específicos del sistema y la infraestructura existente (Bello y otros, 2013).

### 3.5.3 DNP3

Según indica la empresa Copadata (2022) en su sitio web, DNP3 es un estándar de control remoto establecido utilizado por las empresas de servicios eléctricos en los Estados Unidos y muchos otros países del mundo.

Se creó en 1993 y define específicamente la interacción entre sistemas informáticos públicos teniendo en cuenta las comunicaciones remotas. Con este fin, DNP3 se enfoca en proporcionar una forma liviana de transmitir valores de datos simples con un alto grado de integridad.

DNP3 establece dos tipos de puntos finales que interactúan entre sí: uno es el maestro y el otro es la unidad remota. El maestro, que corresponde a la estación central del centro de control, es una computadora o red con suficiente capacidad para almacenar y procesar todos los datos provenientes de las unidades remotas, facilitando su visualización. Por otro lado, la unidad remota se encuentra en el campo y se encarga de recolectar información de diversos dispositivos en distintas ubicaciones, transmitiéndola a la estación principal. Alternativamente, una unidad remota DNP3 puede ser un dispositivo que se comunica directamente con la estación maestra, como una RTU, un medidor de flujo de agua o energía, un inversor fotovoltaico o cualquier otro tipo de estación controlada (Copadata, 2022).

Si bien DNP3 ha demostrado ser eficaz para transferir datos de un punto a otro, la protección de datos es otra cuestión. La ciberseguridad requiere un conjunto de medidas organizativas, arquitectónicas y técnicas. El uso de DNP3 en un sistema aumenta específicamente la necesidad de protección de datos en todos los puntos de la ruta de transmisión. Además, el sistema debe estar protegido contra intervenciones no autorizadas. Para hacer esto, las aplicaciones

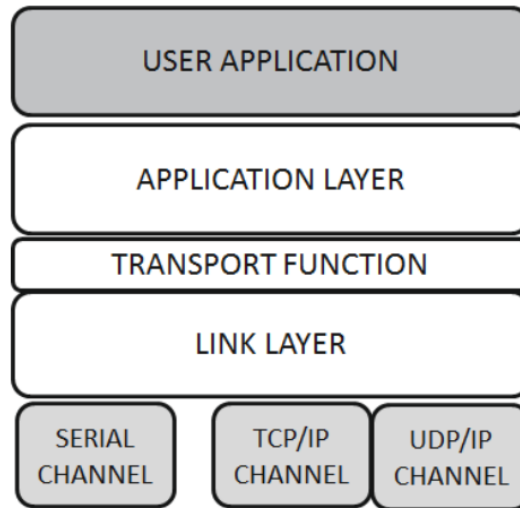
basadas en DNP3 generalmente usan cifrado TLS junto con el proceso de autenticación segura que se define a continuación (Copadata, 2022):

- Cifrado TLS: protege los sistemas conectados a través de un canal TCP/IP cifrando los datos para que solo los sistemas internos puedan leerlos. El cifrado TLS está claramente definido en el estándar DNP3, por lo que a menudo se utiliza como medida de seguridad básica para evitar la divulgación innecesaria de información, el acceso no autorizado y la manipulación de mensajes.
- Autenticación segura: este mecanismo opcional requiere de autenticación cuando ciertas solicitudes provienen del maestro o de la unidad remota. Estas funciones protegidas de autenticación son a menudo funciones críticas que afectan la operatividad del sistema, como la configuración de los resultados de los comandos, la lectura de mensajes de confirmación y similares. La autenticación es bidireccional y funciona utilizando el principio de desafío-respuesta, de manera que, si se solicita una función, se desafía al maestro a que proporcione la respuesta adecuada a un mensaje de la unidad remota, basada en una clave previamente compartida. De esta manera, se evitan operaciones no autorizadas o involuntarias. Mientras que la autenticación no cifra los datos ni garantiza la confidencialidad, proporciona una capa adicional de seguridad como protección frente a funciones potencialmente nocivas y alteraciones del sistema.

Por último, cabe mencionar que es un protocolo de tres capas según el modelo OSI, tal como se muestra en la Figura 23 (Copadata, 2022):

**Figura 23**

*Estructura modular del protocolo DNP3*



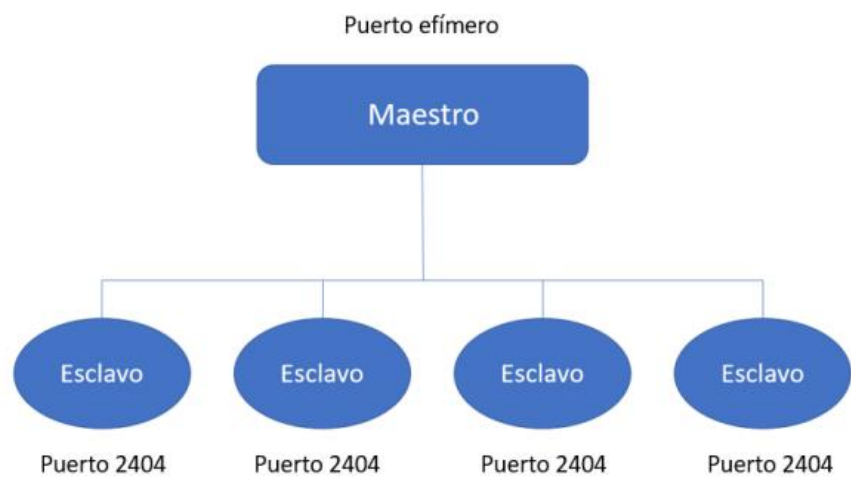
Nota. Obtenido de *DNP3 (Distributed Network Protocol) e IEC 61850*, Copadata, 2022

### **3.5.4 IEC 60870-5-104**

La empresa ABB Inc. (2017) indica que el estándar internacional IEC 60870-5-104, desarrollado por la IEC4 y lanzado en el año 2000, se basa en el estándar IEC 60870-5-101, compartiendo la misma estructura en la capa de aplicación. Su función principal consiste en establecer comunicación a través de TCP/IP para garantizar una transmisión segura de datos entre el centro de control del sistema SCADA y los diferentes controladores mencionados anteriormente. También especifica que el puerto comúnmente utilizado para las transmisiones TCP es el 2404. Este puerto está asignado a los paquetes designados como esclavos, quienes tienen la capacidad exclusiva de enviar respuestas o información en respuesta a consultas formuladas por un maestro, quien se encargará de emitir órdenes o recopilar la información proporcionada por los esclavos. En la Figura 24 de puede observar una arquitectura típica:

**Figura 24**

*Arquitectura Maestro-Esclavo IEC 60870-5-104*



Nota. Obtenido de *Desarrollo de un Sistema Eficiente de Análisis del Protocolo IEC 60870-5-104 para la Detección de Anomalías en Redes Scada*, por Sanches Gómez, 2019

La pila de protocolos IEC 60870-5 se basa en el modelo de referencia reducido denominado Arquitectura de Rendimiento Mejorado (EPA). La EPA incluye tres capas del modelo OSI. En la Tabla 2 se muestran las capas de OSI usadas en EPA:

**Tabla 2**

*Disposición estándar seleccionada de la norma complementaria de telecontrol definida*

<b>Selected application functions of IEC 60870-5-5</b>	<b>User process</b>
Selected application information elements of IEC 60870-5-4	Application layer (7)
Selected application service data units of IEC 60870-5-3	
Selected link transmission procedures of IEC 60870-5-2	Link layer (2)
Selected transmission frame formats of IEC 60870-5-1	
Selected ITU-T recomendations	Physical layer (1)

Nota. Obtenido de *IEC 60870-5-101/104 Communication Protocol Manual*, ABB Inc., 2017

La empresa ABB Inc (2017) también indica que la capa de aplicación define los elementos de información para estructurar los datos de aplicación y las funciones de los servicios de comunicación. El proceso de usuario describe una serie de funciones básicas de aplicación.

La capa de enlace define los formatos de trama y los procedimientos de transmisión de la comunicación IEC.

La capa física define las especificaciones dependientes del hardware de las interfaces de comunicación IEC 60870-5-104 (ABB Inc., 2017).

### **3.5.5 Profibus**

La empresa Profibus (2023) indica en su sitio web que se trata de un protocolo de comunicación industrial diseñado para la interconexión de dispositivos y sistemas de automatización. Se originó con la finalidad de mejorar la eficiencia en los procesos industriales.

Esta tecnología surgió a finales de la década de 1980 como resultado de una colaboración entre el gobierno alemán y diversas empresas, destacándose rápidamente por sus prestaciones y su estructura estandarizada y abierta.

Al principio, el Profibus se utilizaba en el estándar RS-485, que era muy conocido en ese momento proporcionando el perfil FMS (Especificación de Mensajes de Fieldbus), que permitía la comunicación entre sistemas de automatización con una estructura estándar y centrada en objetos, manejando grandes cantidades de datos, aunque no necesariamente en tiempo real o de manera determinista. Sin embargo, con el avance de la tecnología, este perfil dejó de utilizarse gradualmente. La adopción inicial de esta tecnología se motivó por la necesidad de reducir la longitud de los cables requeridos en instalaciones industriales, acercando la medición o control de

variables al lugar donde se generaban. Esto resultó en la disminución de costos de materiales, tiempos de instalación y errores asociados (Profibus, 2023).

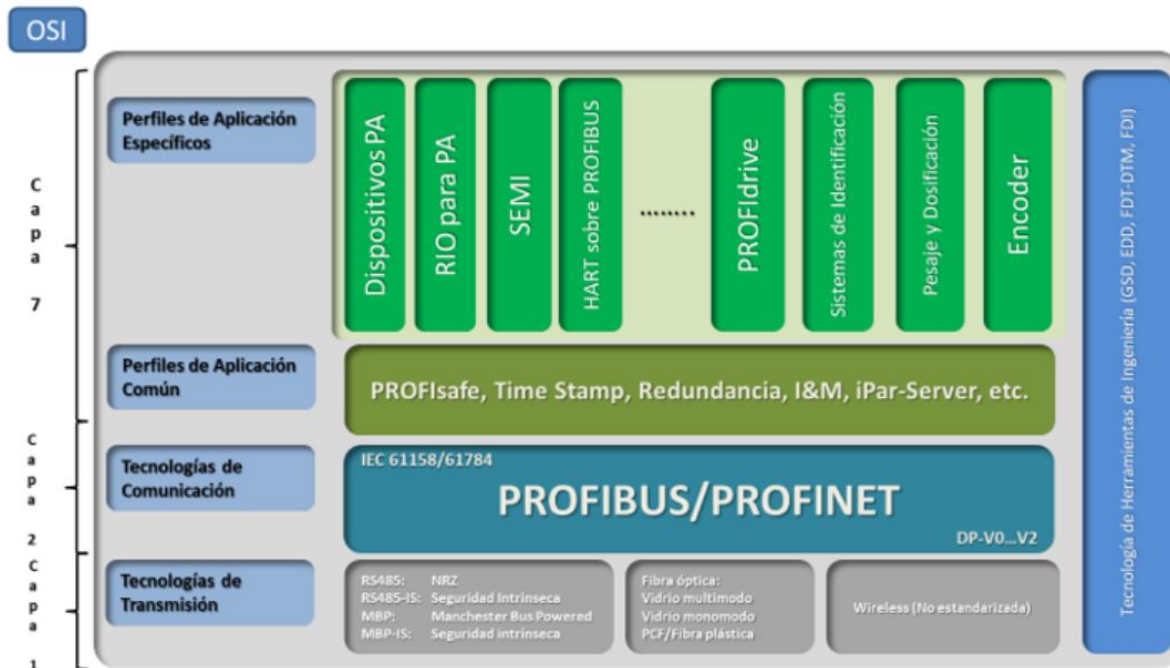
Finalmente, en 1998, se presentó el perfil DP-V1, habilitando la adopción del Profibus en la automatización de procesos. El Profibus PA (Process Automation) es un perfil específicamente diseñado para conectar sensores y actuadores utilizados en industrias de procesos, como químicas y petroquímicas. Este perfil cuenta con características que facilitan su implementación en áreas con riesgos de explosión, permitiendo la reconfiguración de parámetros operativos o el intercambio de dispositivos sin detener el proceso en curso, gracias a la capa física MBP (Manchester Bus Powered), que permite la transmisión de comunicación y alimentación a través de los mismos hilos.

Si bien en la actualidad, con el enfoque predominante en las redes basadas en Ethernet industrial, cabe mencionar que Profibus posee una implementación ágil y sencilla en plantas industriales existentes o nuevas y es posible gracias a sus características flexibles. Su arquitectura abierta facilita la conexión de diversos dispositivos, sin importar la marca o el modelo, proporcionando una mayor libertad para configuraciones personalizadas adaptadas a las necesidades específicas de cada instalación (Profibus, 2023).

En cuanto a la velocidad de transferencia, Profibus puede alcanzar hasta 12 Mbps (megabits por segundo), una capacidad que en su momento se consideró suficientemente aceptable para los requisitos de la industria. Además, el protocolo permite una expansión fácil mediante actualizaciones simples en caso de que sea necesario aumentar su rendimiento. En la Figura 25 se muestra cómo se integra el modelo OSI con el protocolo:

**Figura 25**

*Utilización de las capas del modelo OSI en el protocolo Profibus*



Nota. Obtenido de *PROFIBUS: Qué es y cómo funciona*, Profibus, 2023

## 3.6 Criptografía y Dispositivos de Seguridad

### 3.6.1 Introducción a la Criptografía

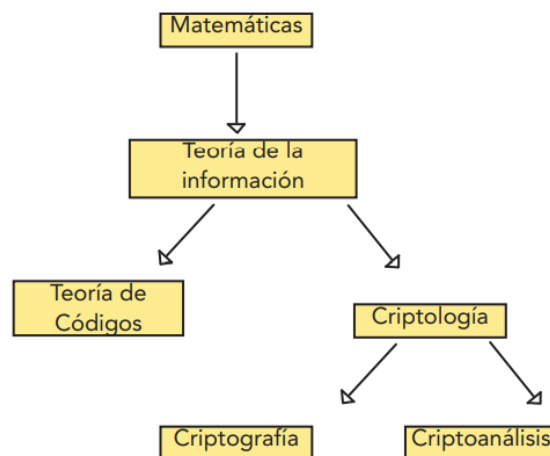
Según el autor Granados Paredes (2006), el término criptografía tiene su origen etimológico en las palabras griegas Kriptos=ocultar y Graphos=escritura, lo que implica esconder la escritura o, en un sentido más amplio, aplicar técnicas para volver un mensaje ininteligible. En su categorización dentro de las disciplinas académicas, la criptografía proviene de una rama de las matemáticas que fue iniciada por el matemático Claude Elwood Shannon en 1948, conocida como "Teoría de la Información". Esta rama se desglosa en dos ramas principales: "Teoría de Códigos"



y "Criptología". A su vez, la Criptología se subdivide en Criptoanálisis y Criptografía, tal como se ilustra en la Figura 26:

**Figura 26**

*Origen de la Criptografía*



Nota. Obtenido de *Introducción a la Criptografía*, por Granados Paredes, 2006

En un sentido más amplio, Granados Paredes (2006) también menciona que la criptografía se ocupa de concebir funciones o dispositivos capaces de convertir mensajes legibles o en texto claro en mensajes cifrados de tal manera que tanto la transformación (cifrado) como su inversa (descifrado) solo sean viables con el conocimiento de una o más llaves. En contraste, el criptoanálisis es la disciplina que examina los métodos utilizados para recuperar mensajes en claro a partir de uno o varios mensajes cifrados, sin la necesidad de conocer la o las llaves, y/o para hallar la llave o llaves con las que esos mensajes fueron cifrados.

Por otro lado, desde el punto de vista histórico, la criptografía se divide en dos categorías: la criptografía clásica y la criptografía moderna. La criptografía clásica abarcó desde períodos anteriores a la era actual hasta la mitad del siglo XX, caracterizándose por ser no computarizada

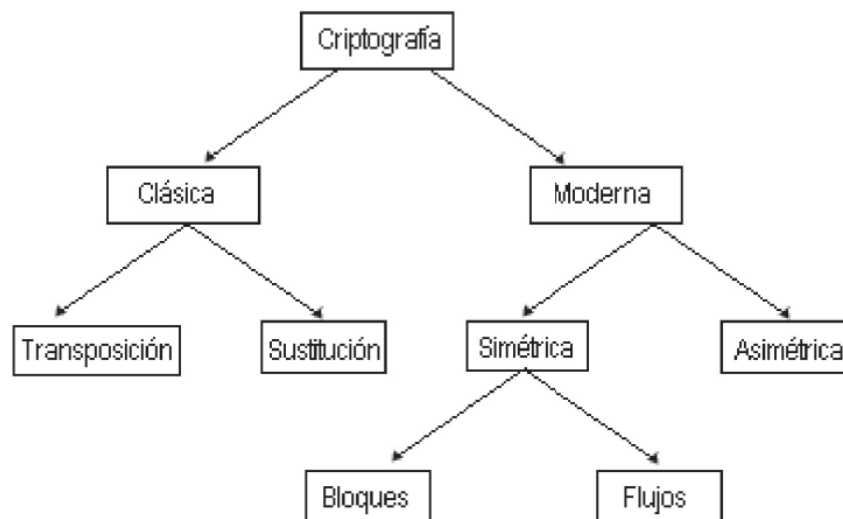
o, más precisamente, no digitalizada. Los métodos empleados eran diversos, algunos bastante simples y otros extremadamente complicados para la época en términos de criptoanálisis.

La criptografía moderna, en cambio, tuvo su inicio después de tres eventos clave. Primero, con la publicación de la "Teoría de la Información" por Shannon; segundo, con la introducción del estándar de cifrado DES (Data Encryption Standard) en 1974; y finalmente, con el estudio de Whitfield Diffie y Martin Hellman sobre la aplicación de funciones matemáticas unidireccionales a un modelo de cifrado, conocido como cifrado de llave pública, en 1976 (Granados Paredes, 2006).

Tanto la criptografía clásica como la moderna se clasifican según las técnicas o métodos empleados para cifrar los mensajes, como se ilustra en la Figura 27:

**Figura 27**

*Clasificación de la Criptografía*



Nota. Obtenido de *Introducción a la Criptografía*, por Granados Paredes, 2006

### 3.6.2 Algoritmos de Cifrado

#### Simétricos

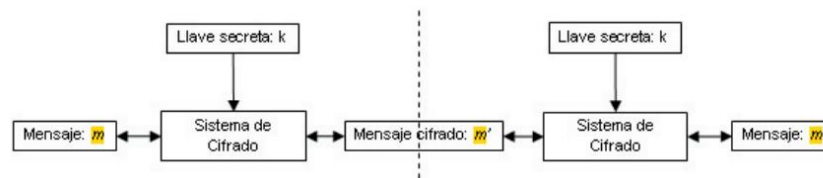
Mendoza T. (2008) indica que la criptografía simétrica emplea una única clave tanto para cifrar como para descifrar el mensaje de datos, lo que implica la utilización de un secreto compartido. En consecuencia, la seguridad de este procedimiento está vinculada a la premisa de que una persona no autorizada no logre obtener la clave de sesión o clave secreta.

Existen dos variantes de algoritmos criptográficos simétricos, a saber, el cifrador en bloque y el cifrador en flujo. La nomenclatura "cifra" se utiliza para describir un algoritmo de cifrado. Los cifradores en bloque operan codificando datos en segmentos de tamaño fijo, comúnmente de 64 bits de longitud. Entre los cifradores en bloque más conocidos se encuentran DES, 3-DES, RC2, RC5, RC6 y Rijndael, también conocido como AES (Mendoza T., 2008).

En la Figura 28 se puede observar cómo funciona este tipo de criptografía:

**Figura 28**

#### *Criptografía Simétrica*



Nota. Obtenido de *Introducción a la Criptografía*, por Granados Paredes, 2006

Mediante este tipo de criptografía, podemos asegurar la confidencialidad, ya que solo la persona que posea la llave secreta tendrá la capacidad de visualizar el mensaje. No obstante, la criptografía simétrica presenta desafíos al compartir secretos con múltiples personas, ya que sería

necesario generar una nueva llave secreta para cada individuo, lo que podría resultar en una gestión complicada de todas las llaves. Además, surge la dificultad de compartir de manera confidencial e íntegra la llave secreta con otra persona. Estos problemas encuentran solución, en cierta medida, mediante el uso de criptografía asimétrica (Granados Paredes, 2006).

Entre los algoritmos de cifrado simétrico más seguros en la actualidad se encuentra el AES-256, que fue desarrollado en respuesta a la creciente vulnerabilidad de los métodos de cifrado de la época. En 1997, el Instituto Nacional de Estándares y Tecnología de los Estados Unidos (NIST) encargó a Vincent Rijmen y Joan Daemen la creación de un nuevo estándar de cifrado, que resultó en la tecnología AES adoptada oficialmente en 1998. Desde su implementación general en 2002, AES se ha establecido como el estándar de cifrado del NIST. A diferencia de otros métodos, AES realiza múltiples rondas de transposición, sustitución y mezcla utilizando una clave de 256 bits, generando 14 rondas de cifrado y ofreciendo un número extremadamente alto de combinaciones posibles (Panda Security, 2023).

Otro algoritmo significativo es el Triple DES, oficialmente conocido como Algoritmo de Cifrado de Datos Triple (3DEA). Este método utiliza el estándar DES en tres fases consecutivas para cifrar los datos, abordando así las limitaciones de seguridad de DES, que emplea una clave de 56 bits. Aunque 3DES mejora la seguridad mediante la aplicación de tres claves diferentes, su eficacia depende de que se utilicen tres claves separadas para mantener su seguridad (Ciberseguridad, 2021).

## **Asimétricos**

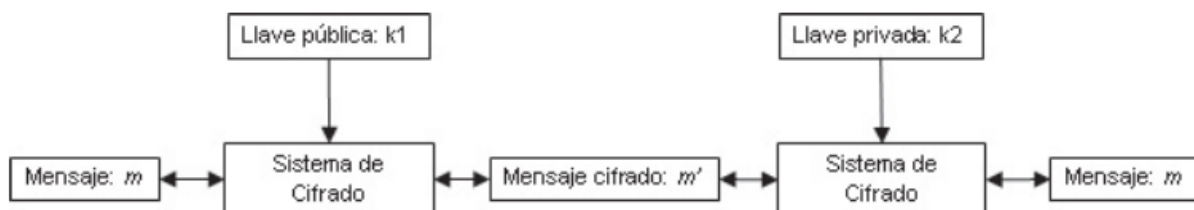
Los algoritmos asimétricos difieren significativamente de los simétricos en un aspecto crucial. Mientras que en la generación de una clave simétrica simplemente se elige un número

aleatorio con la longitud adecuada, el proceso para generar claves asimétricas es más complejo. Estos algoritmos se denominan asimétricos porque, en lugar de utilizar una única clave para llevar a cabo tanto la codificación como la decodificación, emplean dos claves distintas: una para el cifrado y otra para el descifrado. Estas dos claves están relacionadas matemáticamente, con la característica fundamental de que una clave no puede descifrar lo que cifra. Al completar la generación de una clave asimétrica, se establece una clave de cifrado (clave pública) y una clave de descifrado (clave privada). La primera puede ser conocida por cualquier persona, pero es esencial ocultar cuidadosamente la clave privada. Las claves asimétricas poseen la notable propiedad de que lo que se cifra con una clave solo puede descifrarse con la otra (Mendoza T., 2008).

Al examinar la Figura 29, que representa el concepto de criptografía de clave pública, se evidencia de manera clara la ausencia de simetría. En un lado de la figura se lleva a cabo el cifrado o descifrado mediante una llave pública, mientras que en el otro lado se utiliza una llave privada. La falta de simetría en esta representación es precisamente la característica que da origen al nombre de criptografía asimétrica.

**Figura 29**

*Criptografía Asimétrica*



Nota. Obtenido de *Introducción a la Criptografía*, por Granados Paredes, 2006

En el artículo de la empresa Ciberseguridad (2021), se menciona que entre los algoritmos asimétricos considerados más seguros hoy en día podemos citar a RSA, el cual fue creado en 1978 por Rivest, Shamir y Adlman, y es el sistema criptográfico asimétrico más conocido y usado. Frecuentemente, se emplea el cifrado RSA en conjunción con otros esquemas de cifrado o para firmar digitalmente mensajes, validando así la autenticidad e integridad de un mensaje. Usualmente, no se utiliza para cifrar mensajes o archivos completos debido a su menor eficiencia y mayor consumo de recursos en comparación con el cifrado de clave simétrica. Para mejorar la eficiencia, generalmente se cifra un archivo con un algoritmo de clave simétrica, y luego se encripta la clave simétrica utilizando RSA. Bajo este proceso, solo una entidad con acceso a la clave privada RSA puede descifrar la clave simétrica. Sin acceso a la clave simétrica, el archivo original no puede descifrarse. Este enfoque se utiliza para mantener la seguridad de mensajes y archivos sin comprometer la eficiencia o utilizar excesivos recursos computacionales.

El cifrado RSA puede implementarse en diversas plataformas, como OpenSSL, wolfCrypt, cryptlib y otras bibliotecas criptográficas. Siendo uno de los primeros esquemas de cifrado de clave pública ampliamente adoptados, RSA ha establecido las bases para gran parte de nuestras comunicaciones seguras. Tradicionalmente utilizado en TLS y como el algoritmo original en el cifrado PGP, RSA sigue siendo visible en diversos navegadores web, correos electrónicos, VPN, chats y otros canales de comunicación (Ciberseguridad, 2021).

### **3.6.3 Funciones hash criptográficas**

Tal como menciona la empresa SSL.com (2023), una función hash criptográfica pertenece a un conjunto de funciones hash diseñadas para aplicaciones criptográficas como SSL/TLS. Similar a otras funciones hash, estas funciones son algoritmos matemáticos unidireccionales que

asignan datos de cualquier tamaño a una cadena de bits de tamaño fijo. Su uso es común en prácticas de seguridad de la información, como firmas digitales, códigos de autenticación de mensajes y otras formas de autenticación.

Las funciones hash criptográficas deben cumplir con ciertas características clave. Primero, deben garantizar que el valor hash generado para un mensaje sea siempre el mismo, asegurando así determinismo. Además, el proceso de cálculo del valor hash debe ser rápido. Otra propiedad crucial es que debe ser extremadamente difícil encontrar dos mensajes que produzcan el mismo valor hash, lo que se conoce como resistencia a colisiones. También debe ser prácticamente imposible crear un mensaje diseñado para obtener un valor hash específico. Finalmente, cualquier modificación mínima en el mensaje original debería provocar cambios notables en el valor hash, sin que estos cambios guarden una relación obvia con el hash inicial (SSL.com, 2023).

La unicidad de cada hash es crucial para la integridad de estas funciones, distinguiéndolas al garantizar que un mensaje específico sea identificado de manera única e imposible de duplicar. En esquemas de firma digital, como en la firma de documentos o correos electrónicos S/MIME, se requiere calcular un hash criptográfico del mensaje y agregarlo a la firma. El destinatario, mediante su software, calcula independientemente el hash para verificar la integridad del mensaje. Sitios web a menudo publican valores hash para archivos descargables. Al descargar un archivo, un usuario puede usar su propio software para calcular el hash, verificando así la integridad del archivo.

La seguridad de contraseñas también depende de hashes criptográficos. Las contraseñas de los usuarios se cifran y luego se comparan con el hash almacenado para autenticación (SSL.com, 2023).

Estas funciones se emplean extensamente en protocolos de seguridad como SSL/TLS y SSH, así como en otras aplicaciones que requieren la integridad de los datos (SSL.com, 2023).

## **MD5**

La empresa Avast (2024) indica que el MD5, que corresponde a "Message Digest Algorithm" o algoritmo de resumen de mensajes, es un protocolo criptográfico empleado para autenticar mensajes y verificar tanto el contenido como las firmas digitales. Este se apoya en una función hash que asegura que un archivo enviado coincide con el recibido por la destinataria. Aunque en el pasado se utilizaba el MD5 para el cifrado de datos, su aplicación principal en la actualidad se centra en tareas de autenticación. El algoritmo transforma los datos en una cadena compuesta por 32 caracteres. Por ejemplo, la palabra "frog" siempre produce este hash: 938c2cc0dcc05f2b68c4287040cfcf71. De manera similar, un archivo de 1,2 GB también genera un hash con la misma longitud de caracteres. Al enviar ese archivo a otra persona, la computadora verifica su hash para garantizar que coincida con el que usted envió.

En el pasado, MD5 se empleaba con fines de seguridad y cifrado de datos, aunque en la actualidad su principal aplicación es la autenticación. Debido a la posibilidad de que un hacker genere un archivo con el mismo hash que otro archivo completamente diferente, el MD5 no se considera seguro en situaciones donde alguien podría manipular un archivo. No obstante, si simplemente está copiando un archivo de un lugar a otro, el MD5 resulta útil (Avast, 2024).



## **Familia SHA**

Según explica Alamilla Hernández (2020), la familia SHA (Secure Hash Algorithm, Algoritmo de Hash Seguro) se describe como un conjunto de funciones criptográficas hash respaldadas por la Agencia Nacional de Seguridad de Estados Unidos y publicadas por el Instituto Nacional de Estándares y Tecnología (NIST).

Dentro de la familia SHA, el primer integrante fue introducido en 1993 y oficialmente se denomina SHA. No obstante, de manera no oficial, se le reconoce como SHA-0 actualmente para evitar confusiones con sus sucesores. Dos años después, en 1995, se lanzó SHA-1. Desde entonces, se han publicado cuatro versiones adicionales, cada una con modificaciones en el diseño y un aumento en la cantidad de bits de salida formando parte de la familia SHA-2: SHA-224, SHA-256, SHA-384 y SHA-512.

En agosto de 2015, se publicó el nuevo estándar de funciones criptográficas hash SHA-3 mediante el Federal Information Processing Standards Publication, FIPS 202 (Alamilla Hernández y otros, 2020).

A pesar de pertenecer aparentemente a la familia de estándares SHA, SHA-3 difiere internamente en filosofía de los algoritmos anteriores, como SHA-1, SHA-2 y MD5. La familia de funciones hash SHA-3 consta de seis funciones, cuatro de las cuales son funciones criptográficas hash denominadas SHA3-224, SHA3256, SHA3-384 y SHA3-512. Las otras dos funciones son de salida variable, conocidas como XOFs por sus siglas en inglés, llamadas SHAKE128 y SHAKE256, respectivamente. Aunque las funciones de salida variable difieren de las funciones hash, se pueden utilizar de manera similar y adaptarse a las necesidades criptográficas individuales.

En resumen, SHA-256 con una longitud de 256 bits es actualmente muy robusto. Sin embargo, a medida que la capacidad computacional continúe avanzando, el algoritmo podría ser

vulnerado mediante colisiones o ataques de pre-imagen al igual que ocurrió con su antecesor, SHA-1.

La filosofía subyacente en SHA-3 difiere significativamente de sus versiones precedentes, lo que complica considerablemente la tarea de vulnerar el algoritmo. La capacidad computacional actual no permite llevar a cabo tantas operaciones en un período corto, dificultando la posibilidad de romperlo (Alamilla Hernández y otros, 2020).

Considerando esto, se puede afirmar con seguridad que, cuando se identifiquen debilidades en el algoritmo de hash SHA-2, el nuevo algoritmo SHA estará disponible para su implementación. Sin embargo, superar sus medidas de seguridad requerirá recursos financieros significativos, limitando esta tarea a naciones con capacidades económicas considerables.

Por último, cabe mencionar que en SHA-3 las operaciones y procesos que realiza para crear un hash o resumen demandan una capacidad computacional eficiente. En este sentido, las operaciones de SHA-3 aún son computacionalmente lentas, a diferencia de su versión anterior, que ofrece una mayor eficiencia en la realización de operaciones criptográficas, permitiendo que las aplicaciones que lo emplean sean lo suficientemente rápidas. Por este motivo, no puede aún dejar de utilizarse SHA-2 en algunas implementaciones (Alamilla Hernández y otros, 2020).

### 4.1 Introducción

Los Sistemas de Control y Adquisición de Datos (SCADA) posibilitan la gestión, supervisión y control de procesos automatizados mediante la captura y análisis de datos en tiempo real. Inicialmente concebidos fuera del ámbito empresarial, los componentes SCADA se vieron incapaces de hacer frente a diferentes tipos de amenazas como hemos descripto en el capítulo anterior (malware, DDoS, etc.), presentes en la red empresarial actual (Kamlofsky y otros, 2015).

La seguridad de estos sistemas ha emergido como un desafío, dada la convergencia IT/OT y el creciente riesgo de ciber-ataques provenientes de Internet. La conectividad expone esta tecnología a posibles ataques, poniendo en peligro infraestructuras críticas como redes eléctricas, plantas de gas y petróleo, así como sistemas de gestión del agua. Proteger los sistemas SCADA conectados a Internet y a la red interna de la empresa contra intrusos representa un nuevo reto, requiriendo la aplicación de principios y procesos de seguridad de la información (Bonnetto y otros, 2016).

El sistema SCADA se compone de una interfaz hombre-máquina (HMI), un sistema de supervisión (controlador o MTU), unidades terminales remotas (RTU), controladores lógicos programables (PLC) y una infraestructura de comunicación que vincula el sistema de supervisión con las RTU (Pérez-López, 2015).

A medida que la industria SCADA evolucionó, los proveedores adoptaron estándares abiertos, reduciendo el número total de protocolos SCADA a unos pocos populares, como Modbus, Ethernet/IP, Profibus, Distributed Network Protocol 3 (DNP3), etc. Aunque en un principio la ciberseguridad no era un problema debido al aislamiento del sistema SCADA, la interconexión creciente con el exterior ha destacado la necesidad de protección (SDI, 2022).

Las técnicas criptográficas son fundamentales para brindar seguridad, fiabilidad y disponibilidad a los sistemas SCADA. La distribución segura de claves y los desafíos de gestión son discutidos, presentando un enfoque basado en PKI para asegurar eficientemente el sistema SCADA con énfasis en la disponibilidad e integridad (Microsoft, 2023).

Por otro lado, la integración de la red OT con los sistemas ERP a fin de obtener datos que permitan mejorar los procesos, optimizar insumos y relevar información estadística de los sistemas SCADA, generó una brecha de seguridad que puede ser utilizada por ciber-atacantes para acceder a información sensible o interrumpir el normal funcionamiento de una planta industrial (Bonnetto y otros, 2016).

Tal como menciona Heymsfeld (2018), las amenazas en las redes SCADA se dividen de la siguiente manera:

- Pérdida de Disponibilidad: se refiere a la interrupción del acceso confiable y oportuno a sistemas o datos, lo cual puede obstaculizar la identificación y el aislamiento de fallas, así como la restauración de la energía en situaciones anormales, como un apagón. También puede afectar la eficiencia de la cadena de suministro eléctrico. Dado que soluciones de seguridad ineficientes pueden perturbar procesos y operaciones críticas en las redes SCADA, la solución de seguridad debe ser eficaz para preservar la disponibilidad.
- Pérdida de Integridad: este tipo de amenaza implica la alteración o destrucción no autorizada de información, lo cual puede causar graves daños a las infraestructuras. Para protegerse contra estas amenazas, se pueden implementar esquemas de firma digital y autenticación de fuentes.
- Pérdida de Confidencialidad: Consiste en la divulgación no autorizada de información a través de medios externos. En sistemas SCADA, un ejemplo podría ser la vulneración de

la privacidad mediante el espionaje del consumo de energía transmitido desde las RTU. Para protegerse, al igual que con la integridad, un método común es cifrar las comunicaciones SCADA mediante el uso de claves seguras y eficientes esquemas de gestión de claves (Heymsfeld, 2018).

## **4.2 Propuesta de implementación PKI en la red SCADA**

### **4.2.1 Arquitectura de servidores**

Según lo descrito en el capítulo anterior, los sistemas SCADA pueden implementarse de diferentes maneras en una organización. Esta propuesta incluye la utilización del software OpenScada en conjunto con un servidor web Apache.

Por otro lado, para implementar la infraestructura PKI se requiere el siguiente esquema de servidores básicos:

- Servidores Microsoft Windows Server 2022 para ser utilizados con el servicio Microsoft Active Directory Domain Services (ADDS).
- Servidores Microsoft Windows Server 2022 para ser utilizados con el servicio Active Directory Certificate Services (ADCA).

Se requieren dos servidores para cada servicio de modo de contar con un esquema de alta disponibilidad en caso que alguno de ellos falle. En este sentido, es recomendable utilizar un servidor físico y otro virtual para cada uno de los servicios, o bien dos servidores virtuales del mismo modo, pero montados en plataformas de virtualización con la redundancia suficiente para garantizar alta disponibilidad en caso que uno de ellos falle.

Dichos servidores deberán estar instalados en una red DMZ, protegidos a través de un Firewall y separados de la red OT, aunque garantizando la conectividad para poder hacer uso de sus servicios. Se deben habilitar a través de dicho firewall sólo los puertos y protocolos necesarios para el correcto funcionamiento de los servicios antes mencionados.

Por otro lado, se debe generar un certificado SSL/TLS para cifrar las comunicaciones entre el servidor OpenScada y la página web alojada en el servidor web Apache. Para ello, desde el servidor de la CA se deberá realizar la petición de un nuevo certificado, completando la información pertinente del sitio web OpenScada y demás campos requeridos, tal como se mencionó en el apartado 2.5.4.1 con los certificados que utilizan el estándar X.509. Luego, dicho certificado deberá ser configurado en el servidor web Apache. De esta manera, cuando un operador desde una terminal SCADA intente acceder al sitio web, la comunicación estará cifrada y el tráfico no podrá ser manipulado ni los datos robados por un ciberatacante.

Otro punto a tener en cuenta es que se deberá generar una tarea programada en los servidores AD CA para copiar de forma periódica el archivo CRL a los puntos de distribución definidos, los cuales deberán estar disponibles en una URL publicada por el servidor Apache. Como bien se mencionó en el capítulo anterior, en el archivo CRL se publicarán todos los certificados que hayan sido revocados manualmente antes de sus fechas de vencimiento, en caso que se detecte algunos de ellos con la clave privada comprometida o bien si algún usuario ya no pertenece a la organización o cambia de funciones internamente. De esta manera, se revocarían las credenciales de acceso a las terminales SCADA.

#### **4.2.2 Seguridad en las terminales SCADA**

Se requiere que las PCs utilizadas como terminales SCADA tengan instalado en sus almacenes locales el certificado de CA raíz, el cual posee información del servidor que emitió el certificado para el sitio web. De esta manera, se establece una cadena de certificación de confianza para el normal funcionamiento del esquema de seguridad propuesto. Para realizar esto, se recomienda distribuir este certificado raíz a través de los servicios de políticas de dominio del servidor AD DS, logrando los siguientes beneficios:

- Individualización de todas las PCs que son utilizadas como terminales SCADA y que son debidamente autorizadas para operar como tales.
- Automatizar la distribución del certificado raíz a todas las terminales, evitando la tarea de forma manual disminuyendo costos operativos y el margen de error.
- Distribuir a todos los equipos la revocación de dicho certificado de forma inmediata en caso que se detecte que el mismo se haya comprometido. Por otro lado, también distribuir un nuevo certificado renovado por vencimiento.

Por último, las mismas deben estar unidas al dominio de los servidores ADDS y se les deberá aplicar por política de dominio las restricciones y requisitos de seguridad alineadas a las buenas prácticas, según lo recomendado por las normas internacionales.

#### **4.2.3 Dispositivos Criptográficos Tokens**

Se propone la adquisición de dispositivos criptográficos tokens que posean los requisitos mínimos de seguridad mencionados en el capítulo anterior. Los mismos deberán ser entregados a todas las personas que cumplan el rol de operadores de terminales SCADA.

La finalidad de los mismos será la de autenticación para el inicio de sesión de Windows en las terminales y para el login en la aplicación OpenScada, implementando de esta manera un segundo factor de autenticación basado en un certificado digital personal para cada usuario. Dicho certificado será emitido por el servidor CA y almacenado en el interior de estos dispositivos, protegiendo la clave privada del usuario con los más altos estándares de seguridad. De esta manera, se agrega una capa adicional de seguridad en las terminales SCADA reemplazando el inicio de sesión tradicional de usuario y contraseña, minimizando el riesgo que un potencial usuario malintencionado o ciber-atacante con acceso a la contraseña pueda comprometer una terminal con todo el riesgo operativo que ello implica. Con este nuevo esquema, un atacante no sólo deberá poseer en su poder un dispositivo token físico y conectarlo al puerto USB de la terminal, sino que también deberá conocer el PIN del mismo, cumpliendo con los requisitos de complejidad de clave preestablecidos, de acuerdo a la política que defina la organización en materia de ciber-seguridad.

#### **4.2.4 Gestión Administrativa de Certificados Digitales**

Hemos visto en el capítulo anterior el rol que cumplen las personas designadas con Autoridades de Registro (AR), el cual era básicamente ser el “intermediario entre el usuario final de los certificados y la autoridad de certificación en la tarea de expedir y/o renovar los certificados”. Ahora bien, a continuación, se detallará cuáles son los pasos recomendados para realizar una gestión ordenada y segura de certificados digitales para usuarios finales operadores de terminales SCADA, incluyendo la emisión, renovación y revocación de los certificados.

Como primera medida, se deberá definir quiénes serán las personas designadas como tales. Se recomienda nombrar como mínimo a dos personas por cada área usuaria. De este modo, ante la ausencia de una de ellas la otra podrá realizar las gestiones pertinentes.



Los casos de uso son los siguientes:

- Emisión de nuevo certificado digital para usuario final: el usuario deberá ingresar a la URL publicada en el servidor de ADCA, la cual le permitirá autogestionar sus solicitudes de certificados digitales. Se deberá completar los datos personales y conectar el dispositivo token para que comience el proceso de generación de claves pública y privada.

La solicitud quedará en estado “Pendiente” hasta tanto un AR autorice la emisión del certificado digital requerido. Realizada dicha autorización, la solicitud pasará a estado “Aprobado”. En dicho estado, el usuario final accederá nuevamente a la URL para la descarga del certificado digital en su token, junto con su clave privada.

Nota: cabe mencionar que cada usuario sólo podrá tener vigente un solo certificado digital, por lo que para solicitar uno nuevo, primero deberá solicitar su autorevocación en la misma URL.

- Revocación de certificado digital: cuando se aproxima la fecha de vencimiento del certificado digital, el usuario final deberá proceder a la revocación de su certificado en dicha URL, tal como se mencionó en el inciso anterior.

Cabe mencionar que también las AR tienen la facultad de revocar certificados digitales de usuario finales, sea como un procedimiento excepcional ante problemas técnicos como también en casos donde se deba revocar un certificado porque el usuario haya extraviado o le hayan robado el dispositivo token. Las AR también deberán revocar certificados si el usuario ya no pertenece a la empresa o si el mismo cambió de funciones dentro de la organización.

### **4.3 Utilización del Protocolo Modbus TCP/IP con TLS**

Por último, tal como se ha descripto en el capítulo anterior, los dispositivos PLCs no poseen ningún mecanismo de cifrado en sus comunicaciones exponiendo esta vulnerabilidad a la potencial explotación por parte de ciberatacantes, utilizando la misma para provocar una interrupción en el normal funcionamiento de las infraestructuras críticas, acceder a datos operativos sensibles o bien vender los mismos en el mercado negro.

Aprovechando que el protocolo Modbus TCP/IP ya implementa TLS como algoritmo de cifrado, se propone esta metodología como un nuevo modelo teórico para encriptar las comunicaciones de los PLCs y mitigar dicha vulnerabilidad.

Ahora bien, ya es sabido que este tipo de dispositivos tienen recursos de hardware limitados en lo que respecta a procesamiento y memoria. Implementar este nivel de cifrado excedería la capacidad de procesamiento provocando una saturación en los recursos de los PLCs, o bien se experimentaría extrema lentitud en el normal funcionamiento de los mismos, ocasionando interrupciones no deseadas en las tareas operativas normales dentro de sus tareas.

Si bien desde el punto de vista teórico sería recomendable esta propuesta, se deberían tomar contramedidas para que los PLCs puedan soportar la sobrecarga en el uso del CPU (Unidad Central de Procesamiento) para las tareas de cifrado y descifrado, sin afectar el normal funcionamiento operativo de los equipos. Uno de estas medidas, podría ser la implementación de un protocolo de seguridad TLS liviano, pero utilizando algoritmos que hoy en día se consideran aún seguros, como por ejemplo SHA-256. Otra contramedida podría ser el rediseño de PLCs con mayor capacidad de procesamiento, o bien recursos de hardware adicionales exclusivos para las estas tareas de cifrado.

#### 4.4 Protección de las Terminales SCADA

Adicionalmente a lo antedicho en el presente capítulo, se recomiendan tomar medidas adicionales para reforzar cuestiones relacionadas a la protección de las terminales SCADA. Las más importantes son las siguientes:

- **Protección antivirus:** todas las PCs de los operadores deben contar con un antivirus instalado en su última versión estable y actualizado de forma permanente a través de un servidor centralizado de actualizaciones. Dicho software deberá ser capaz de proteger las terminales no solo ante cualquier tipo de malware conocido sino también las llamadas amenazas de día cero, las cuales no son detectables por las firmas tradicionales de los antivirus, pero sí por módulos específicos que detectan comportamiento anómalo sospechoso, como por ejemplo los intentos de cifrado por parte de ransomwares. Otros módulos importantes hoy en día que deberá tener el software antivirus es la capacidad de detección a través de Machine Learning, reputación de urls e indicadores de compromiso. Por último, a fin de garantizar que todas estas características se encuentren operativas en las PCs, se recomienda realizar escaneos remotos periódicos a todas las terminales SCADA y diseñar controles periódicos que permitan detectar cuándo un equipo no posee el antivirus instalado o bien el mismo por alguna cuestión técnica no se encuentre operativo.
- **Parches de seguridad del sistema operativo:** se recomienda mantener el sistema operativo de los equipos actualizado en su última versión estable, para mitigar el riesgo de explotación de vulnerabilidades conocidas de seguridad. Esto puede llevarse a cabo mediante un software centralizado de terceros y se recomienda también diseñar controles periódicos para que hacer cumplir la instalación de dichos parches.

- Principio del mínimo privilegio (PoLP): se refiere a un concepto en seguridad de la información que implica otorgar a un usuario los niveles mínimos de acceso necesarios para llevar a cabo sus funciones laborales. En términos generales, se considera que este principio es una práctica óptima en ciberseguridad y constituye un paso fundamental para salvaguardar el acceso con privilegios a datos y activos de alto valor. Este principio se recomienda aplicarlo tanto a nivel de sistema operativo (por ejemplo, restringiendo el acceso de los usuarios como administradores locales) como así también a nivel del software SCADA.
- Escaneo de puertos y uso de algoritmos inseguros: se recomienda diseñar controles para realizar escaneos periódicos de los equipos en búsqueda de puertos abiertos que no son estándares ni tampoco necesarios por ninguna aplicación homologada, así como también detectar si alguna aplicación instalada en los equipos utiliza algún protocolo de comunicación vulnerable.
- Bloqueo de unidades extraíbles: por último, se recomienda bloquear la utilización de medios extraíbles (como por ejemplo pen drive) a fin de mitigar el riesgo de una infección por malware provenientes de dichos dispositivos, permitiendo únicamente el uso de los dispositivos criptográficos recomendados en este capítulo. Esta tarea puede realizarse por ejemplo mediante una política de dominio utilizando los servicios de AD DS, o bien con el propio software antivirus desde su consola centralizada.

## 4.5 Concientización al usuario final

Si bien es importante adoptar medidas técnicas como las ya descriptas en este y el anterior capítulo, no se debe subestimar el accionar del usuario final en lo que respecta a la operatoria diaria y prevención de incidentes de ciber-seguridad.

Para ello, son importantes las campañas de concientización para usuarios finales con cierta frecuencia para que el usuario esté capacitado en actuar ante ciertos eventos sospechosos que puedan poner en riesgo la ciber-seguridad de las infraestructuras críticas.

Los temas más relevantes que no deberían faltar en una buena campaña de concientización son los siguientes:

- ataques de phishing
- contraseñas y autenticación
- ingeniería social
- medios extraíbles
- seguridad de los dispositivos móviles
- seguridad en el hogar
- seguridad en la nube
- seguridad física
- trabajar a distancia
- uso de Internet y del correo electrónico
- uso de las redes sociales
- wi-fi público

4.6 Recursos a utilizar

Para implementar la propuesta, se requiere la adquisición de al menos dos servidores. En uno de ellos, se instalará un sistema operativo Microsoft Windows Server 2022 donde funcionarán los servicios de Microsoft Active Directory Domain Services (ADDS) y Active Directory Certificate Services (ADCA). En el segundo servidor, funcionará un sistema operativo Linux donde se instalarán los aplicativos OpenScada y el servicio web de Apache.

Por último y de manera opcional pero recomendable, será necesaria la compra de dispositivos criptográficos tokens. La cantidad dependerá de las necesidades de cada organización y de los usuarios operadores a los cuales se les asignarán los mismos.

4.7 Cronograma de Tareas

En la Tabla 3 se especifican las tareas relacionadas a la implementación de esta propuesta de intervención y los tiempos estimados de cada una de ellas:

**Tabla 3**  
*Planificación de actividades*

Tareas a ejecutar		Meses								
ID	Descripción	1	2	3	4	5	6	7	8	9
1	Relevamiento de infraestructura SCADA existente									
2	Planificación y diseño de la implementación									
3	Implementación de la infraestructura PKI									
4	Implementación de medidas de ciberseguridad en SCADA									
5	Pruebas y validación de la seguridad implementada									
6	Evaluación y ajustes									
7	Documentación final y conclusiones									

A continuación, se describen las acciones a seguir en cada una de las tareas especificadas:

1. Relevar la tecnología existente en la organización.
2. Analizar los requerimientos de seguridad, definir la arquitectura PKI y seleccionar las herramientas y tecnologías.
3. Configurar la CA, generar los certificados digitales e implementar la autenticación basada en certificados y políticas de revocación de certificados.
4. Segmentar la red, configurar el tipo de cifrado y controlar el acceso basado en roles.
5. Realizar pruebas de funcionalidad PKI, evaluar la autenticación y cifrado, probar el sistema de intrusión y simular ataques comunes.
6. Analizar de resultados, optimizar las configuraciones y documentar los errores detectados.
7. Redactar el capítulo de implementación, las conclusiones y recomendaciones.

#### **4.8 Factores Externos Condicionantes**

Existen factores externos que podrían condicionar la implementación de este trabajo y que deben ser tenidos en cuenta en el entorno donde operan los sistemas SCADA, diseñando una estrategia de ciberseguridad efectiva que integre PKI y tomando en cuenta las limitaciones y oportunidades que cada uno de estos factores aporta. Los mismos son los siguientes:

- Marco regulatorio y legal: las normativas que regulan los sistemas SCADA y las infraestructuras críticas establecen requisitos de seguridad que influyen en la implementación de medidas de ciberseguridad.

- Evolución de las amenazas y riesgos: los sistemas SCADA enfrentan constantemente riesgos de ciberataques avanzados, como ransomware y ataques de denegación de servicio (DDoS). La creciente sofisticación de estas amenazas genera la necesidad de actualizar las medidas de seguridad e implementar soluciones PKI robustas para gestionar la autenticación y el cifrado en tiempo real.
- Innovación tecnológica en sistemas de control industrial: la introducción de tecnologías emergentes como IIoT, 5G y la computación en la nube en la automatización industrial está transformando las arquitecturas SCADA. Aunque estas innovaciones optimizan la eficiencia operativa, también plantean desafíos de seguridad, ya que amplían el perímetro de ataque y exigen una mayor compatibilidad e integración con soluciones PKI.
- Disponibilidad de recursos y presupuesto: implementar medidas avanzadas de ciberseguridad en SCADA y PKI requiere una inversión considerable en infraestructura, capacitación y mantenimiento. Las limitaciones presupuestarias pueden reducir el alcance y la efectividad de las estrategias de seguridad, en especial para organizaciones que operan infraestructuras críticas.
- Interoperabilidad y estándares de comunicación: los sistemas SCADA suelen emplear distintos protocolos industriales (como Modbus, DNP3, OPC, IEC 60870) que no fueron diseñados inicialmente con ciberseguridad. Esto representa un desafío para la implementación de medidas de seguridad, ya que las herramientas deben ser compatibles y eficaces en entornos con múltiples protocolos y fabricantes.
- Dependencia de proveedores y cadena de suministro: los sistemas SCADA dependen en gran medida de proveedores externos para el software y hardware. Los riesgos de ciberseguridad en la cadena de suministro, tales como el uso de software no seguro o



vulnerabilidades en el firmware, pueden comprometer la integridad del sistema y aumentar la vulnerabilidad de las infraestructuras críticas a ataques.

## **4.9 Evaluación del Proyecto**

En este apartado se llevará a cabo una evaluación del proyecto descrito en la propuesta de intervención. Para ello, se elaborará una matriz FODA, la cual permitirá identificar y analizar las características principales de la propuesta de intervención. Luego, se desarrollará una evaluación detallada de los costos asociados, considerando tanto los recursos de hardware como así también el personal necesario y los roles que desempeñarán.

### **4.9.1 Matriz FODA de la Propuesta de Intervención**

Con el objetivo de detallar y comprender las características fundamentales de la propuesta de intervención, se llevará a cabo un análisis utilizando la matriz FODA. Esta herramienta estratégica permitirá identificar y clasificar de manera estructurada las fortalezas, debilidades, oportunidades y amenazas que pueden influir en la implementación y el desarrollo del proyecto. Las fortalezas y debilidades se enfocarán en los aspectos internos del proyecto, mientras que las oportunidades y amenazas se centrarán en factores externos que podrían incidir positiva o negativamente en su progreso. Este análisis no solo facilitará la visualización de los elementos clave que afectan el desempeño del proyecto, sino que también proporcionará una base sólida para la toma de decisiones estratégicas y la mitigación de riesgos. En la Tabla 4 se presentan estos elementos organizados de manera clara y detallada, con el propósito de ofrecer una perspectiva integral que permita identificar posibles áreas de mejora y aprovechar al máximo los recursos disponibles.

**Tabla 4**

*Matriz FODA de la propuesta de intervención*



<b>FORTALEZAS</b>	<b>OPORTUNIDADES</b>
<p>El tema es relevante y de interés creciente en la industria debido al aumento de ataques cibernéticos en infraestructuras críticas.</p> <p>La combinación de SCADA y PKI aborda dos áreas esenciales para la seguridad en sistemas de control y autenticación.</p> <p>La infraestructura PKI es ampliamente usada y probada, con tecnologías y estándares que ya existen para su implementación en SCADA.</p>	<p>La tendencia hacia la automatización y digitalización de industrias presenta una demanda creciente de medidas de ciberseguridad.</p> <p>Los estándares de seguridad y regulaciones están evolucionando, lo que crea oportunidades para el desarrollo de nuevas estrategias y soluciones.</p> <p>Posibilidad de contribuir con investigaciones pioneras en un campo en crecimiento, aportando soluciones para la seguridad de infraestructuras críticas.</p>
<b>DEBILIDADES</b>	<b>AMENAZAS</b>
<p>Dificultad para acceder a ciertos casos de estudio o ejemplos reales, ya que las organizaciones son reacias a compartir detalles de su infraestructura de ciberseguridad.</p> <p>Las complejidades técnicas y legales de la implementación de PKI en sistemas SCADA pueden hacer que la investigación sea extensa.</p>	<p>La rápida evolución de las amenazas cibernéticas puede hacer que los enfoques y soluciones de seguridad se vuelvan obsoletos rápidamente.</p> <p>Las ciberamenazas específicas a los sistemas SCADA (como el ransomware y los ataques DDoS) son cada vez más sofisticadas.</p> <p>Los costos de implementación y mantenimiento de infraestructuras PKI seguras pueden ser una barrera para muchas empresas.</p>

#### **4.9.2 Análisis de Costos**

A continuación, se mostrará un presupuesto simplificado necesario para llevar a cabo la implementación de este trabajo de intervención, según las especificaciones funcionales indicadas en los apartados anteriores. Para ello, se utilizó la cotización que ofrece Amazon Web Services (AWS Pricing Calculator, 2024), informando los precios en dólares americanos tal como se muestra en la Figura 30:

Figura 30

Cálculo del costo de dos servidores para la implementación de esta propuesta

<b>Instancias EC2 (9)</b> Based on your inputs, this is the lowest-cost EC2 instance: <b>r5.xlarge</b> Instancia elegida: <b>m5.2xlarge</b>   Family: <b>m5</b>   <b>8vCPU</b>   <b>32 GiB Memoria</b>				
<b>Instancias EC2 (9)</b> Based on your inputs, this is the lowest-cost EC2 instance: <b>r5.xlarge</b> Instancia elegida: <b>r5.4xlarge</b>   Family: <b>r5</b>   <b>16vCPU</b>   <b>128 GiB Memoria</b>				
Nombre del servicio ▾	Estado ▾	Costo inicial ▾	Costo mensual ▾	
Amazon EC2 	-	0,00 USD	1758,19 USD	
Amazon EC2 	-	0,00 USD	524,63 USD	

Nota. Cotización generada utilizando la calculadora de Amazon Web Services (AWS Pricing Calculator), 2024

Según esta estimación, el costo total de mantenimiento y puesta en marcha de estos servidores necesarios asciende a un total de usd2.282,82 mensuales.

Por último, se requiere personal específico para llevar a cabo todas las tareas descriptas en los apartados anteriores. En la Tabla 5 se detallarán los costos asociados:

**Tabla 5**

*Cálculo del costo para el personal a contratar*

<b>Cantidad</b>	<b>Rol</b>	<b>Costo Mensual (en usd)</b>
1	Lider de Proyecto	1500
1	Administrador de IT	1100
2	Analista Funcional Sr.	2400

En base a estos costos, podemos concluir que la contratación del personal necesario representa un costo total mensual de usd5000.

---

## Conclusiones

Los sistemas SCADA han evolucionado hasta convertirse en una pieza fundamental en la automatización y supervisión de procesos industriales, desempeñando un papel crítico en industrias y gobiernos de todo el mundo. Su aplicación en la gestión de infraestructuras críticas nacionales destaca su relevancia estratégica. Sin embargo, la transición hacia la Industria 4.0 y la Internet Industrial de las Cosas (IIoT) ha transformado el panorama de estos sistemas, obligando a las organizaciones a extender sus redes corporativas a procesos industriales y a exponer las redes de tecnología operativa (OT) a Internet. Este cambio ha introducido vulnerabilidades significativas, no previstas cuando los sistemas SCADA fueron diseñados originalmente en el siglo XX.

En este sentido, la convergencia de redes IT y OT, impulsadas por la necesidad de integrar sistemas ERP con procesos industriales, ha incrementado la exposición de los sistemas SCADA a amenazas cibernéticas. Este aumento de conectividad exige una revisión exhaustiva de las medidas de seguridad para proteger tanto los datos críticos como la infraestructura subyacente.

Por otro lado, la implementación de una infraestructura de clave pública (PKI) robusta ha demostrado ser una solución eficaz para abordar las vulnerabilidades existentes. Los certificados digitales y la gestión de claves garantizan autenticación, integridad y confidencialidad en las comunicaciones SCADA, fortaleciendo la seguridad del sistema frente a accesos no autorizados y ataques maliciosos. Además, la PKI facilita la gestión centralizada y automatizada de credenciales, lo que permite una respuesta rápida y eficiente ante incidentes de seguridad.

En lo que respecta al uso del protocolo de seguridad TLS, podemos afirmar que resulta conveniente para cifrar las comunicaciones entre los Controladores Lógicos Programables (PLC) y otros componentes del sistema SCADA, añadiendo una capa crítica de protección. Este enfoque

previene la interceptación y manipulación de datos, asegurando que las operaciones industriales se desarrollen de manera segura y confiable. Asimismo, la implementación de TLS refuerza la confianza de operadores y usuarios al garantizar la privacidad y seguridad de las transacciones de datos.

Por último, las medidas dirigidas a proteger las terminales SCADA y a los usuarios operadores son fundamentales para reforzar la postura de seguridad general del sistema. Entre estas acciones destacan la segmentación de redes, la implementación de políticas de acceso basado en roles y el uso de firewalls para limitar el tráfico no autorizado. Además, la formación y concienciación de los operadores en prácticas de ciberseguridad son esenciales para mitigar el riesgo humano, considerado una de las vulnerabilidades más críticas en cualquier sistema.

Las implicaciones de estos hallazgos subrayan la necesidad de una estrategia de ciberseguridad integral y adaptativa en los sistemas SCADA. La combinación de PKI y TLS ofrece una defensa efectiva contra las amenazas cibernéticas, pero no debe considerarse una solución aislada. La seguridad en sistemas SCADA requiere un enfoque holístico que integre tecnología, procesos y personas.

Desde el punto de vista industrial, mantener los sistemas actualizados es crucial para protegerlos de las amenazas emergentes, y las organizaciones deben establecer programas de monitoreo continuo y respuesta a incidentes para abordar rápidamente cualquier vulnerabilidad. La colaboración entre industrias, proveedores de tecnología y agencias gubernamentales es vital para desarrollar estándares de seguridad comunes y compartir mejores prácticas. Adoptar estándares de seguridad reconocidos a nivel internacional permite a las organizaciones alinear sus estrategias de ciberseguridad con las mejores prácticas de la industria. Además, invertir en tecnologías de seguridad avanzadas y en la formación continua del personal es esencial para

fortalecer la defensa contra amenazas cibernéticas, y las organizaciones deben dar prioridad a la capacitación de sus empleados en prácticas de seguridad y gestión de incidentes para mejorar la resiliencia organizacional.

Finalmente y a modo de conclusión general, podemos afirmar que la implementación de una infraestructura PKI en sistemas SCADA, junto con el cifrado de comunicaciones mediante TLS y medidas de seguridad complementarias, proporciona una solución integral y efectiva para proteger entornos industriales. Este enfoque no solo mejora la seguridad y resiliencia de los sistemas SCADA, sino que también sienta las bases para una integración segura de nuevas tecnologías en la era de la Industria 4.0 y la IIoT. Las organizaciones deben continuar adaptando y evolucionando sus estrategias de ciberseguridad para enfrentar los desafíos dinámicos del entorno digital moderno, asegurando así la protección de sus activos más críticos.

---

### **Trabajos Futuros por Realizar**

Es posible continuar estudiando el protocolo Modbus con TLS con un mayor nivel de profundidad técnico a fin de poder implementar una capa de seguridad aún mejor para cifrar las comunicaciones en los PLC. O bien desarrollar nuevas versiones de estos dispositivos que posean mayor capacidad de procesamiento para poder implementar el protocolo en toda su expresión.

Por otro lado, en caso que el sistema SCADA requiera ser publicado en Internet es posible utilizar un certificado digital de terceros en lugar de un servidor CA interno. Para ello, se deberá adquirir dicho certificado en algún proveedor que ofrezca el mercado.



---

## **Acrónimos**

ACS-TP	Sistemas de Control de Automatización de Procesos Tecnológicos
ADCS	Active Directory Certificate Services
ADDS	Active Directory Domain Services
ADU	Automatic Duplex Unit
AES	Advanced Encryption Standard
API	Application Programming Interface
AR	Autoridad de Registro
ASCII	American Standard Code for Information Interchange
CA	Certification Authority
CFC	Cyber Fusion Centre
CPS	Cyber Physical Systems
CPU	Central Processing Unit
CRC	Cyclic Redundancy Check
CRL	Certificate Revocation List
CSP	Content Security Policy
CTR	Cybercrime Threat Response
DCS	Distributed Control System
DDoS	Distributed Denial of Service
DES	Data Encryption Standard
DMS	Document Management System
DMZ	Demilitarized Zone

DNP	Distributed Network Protocol
DoS	Denial of Service
DSA	Digital Signature Algorithm
E/S	Entrada/Salida
EFS	Encrypting File System
EPA	Arquitectura de Rendimiento Mejorado
ERC	Evaluación de Resiliencia Cibernética
ERP	Enterprise Resources Planning
FIPS	Federal Information Processing Standards
FMS	Fieldbus Message Specification
GMAO	Gestión de Mantenimiento Asistido por Ordenador
HMI	Human Machine Interface
HSM	Hardware Security Module
IANA	Internet Assigned Number Authority
ICMP	Internet Control Message Protocol
ICS	Industry Control System
IDS	Intrusion Detection System
IEC	International Electrotechnical Commission
IEC	International Electrotechnical Commission
IGMP	Internet Group Management Protocol
IIoT	Internet Industrial of Things
IoS	Internet of Services
IoT	Internet of Things

IP	Internet Protocol
IPDS	Intrusion, Prevention and Detection System
IPsec	Internet Protocol Security
ISO	Internacional Organization for Standardization
IT	Information Technology
LAN	Local Area Network
LRC	Longitudinal Redundancy Check
MD5	Message Digest Algorithm
MTU	Master Terminal Unit
NIST	National Institute of Standards and Technology
NOC	Centro de Operaciones de Red
OMS	Organización Mundial de la Salud
OSI	Open Systems Interconnection
OT	Operative Technology
PA	Process Automation
PAC	Programmable Automation Controller
PC	Personal Computer
PDU	Protocol Data Unit
PGP	Pretty Good Privacy
PID	Process ID
PIN	Personal Identification Number
PKCS	Public-Key Cryptography Standards
PKI	Public Key Infrastructure

PLC	Programmable Logic Controller
PoLP	Principio del mínimo privilegio
RFID	Radio-Frequency Identification
RSA	Rivest, Shamir y Adelman
RTU	Remote Terminal Unit
S/MIME	Secure/Multipurpose Internet Mail Extensions
SCADA	Supervisory, Control and Data Acquisition
SHA	Secure Hash Algorithm
SOC	Centro de Operaciones de Seguridad
SSH	Secure Shell
SSL	Secure Socket Layer
TCP	Transmission Control Protocol
TLS	Transport Layer Security
TPM	Trusted Platform Module
URL	Uniform Resource Locator
USB	Universal Serial Bus
VPN	Virtual Private Network
WAN	Wide Area Network

---

## Referencias

- ABB Inc. (20 de 7 de 2017). *IEC 60870-5-101/104 Communication Protocol Manual*. Obtenido de <https://library.e.abb.com/public/68021e6c8f654aca98c5b10d1a02134e/1MAC306892-MB%20C%20IEC%20104%20Comm%20Protocol.pdf>
- Adams, T. (2014). *Ced Engineering*. Obtenido de <https://www.cedengineering.com/userfiles/SCADA%20System%20Fundamentals-R1.pdf>
- Alamilla Hernández, L., Hernández Cadena, A., Garrido Vázquez, J., Magaña, J., & Gómez Zea, J. (2020). La seguridad de la firma electrónica con el estándar criptográfico algoritmo de hash seguro 3 (SHA-3). *Innovación y Desarrollo Tecnológico Revista Digital*. Obtenido de [https://iydt.files.wordpress.com/2020/05/2\\_1\\_la-seguridad-de-la-firma-electrc3b3nica-con-el-estc3a1ndar-criptogr3a1fico-algoritmo-de-hash-seguro-3-sha-3.pdf](https://iydt.files.wordpress.com/2020/05/2_1_la-seguridad-de-la-firma-electrc3b3nica-con-el-estc3a1ndar-criptogr3a1fico-algoritmo-de-hash-seguro-3-sha-3.pdf)
- Avast. (2024). *¿Qué es el algoritmo de hashing MD5 y cómo funciona?* Recuperado el 5 de 2 de 2024, de <https://www.avast.com/es-es/c-md5-hashing-algorithm>
- AWS Pricing Calculator. (2024). *Estimate the cost for your architecture solution*. Recuperado el 25 de 10 de 2024, de <https://calculator.aws/>
- Banco Mundial. (2024). *Grupo Banco Mundial*. Recuperado el 5 de 2 de 2024, de <https://datos.bancomundial.org/indicador/SP.POP.TOTL>
- Bello, E., Yair Morales, O., & Espada, G. (2013). *Modbus y Modbus Plus*. Obtenido de <https://es.scribd.com/presentation/165317028/Modbus-y-Modbus-Plus>
- Bidaidea. (25 de 2 de 2022). *Convergencia entre IT y OT*. Recuperado el 5 de 2 de 2024, de [https://ciberseguridadbidaidea.com/convergencia-entre-it-y-ot/#Objetivos\\_de\\_seguridad\\_de\\_la\\_convergencia\\_IT\\_OT](https://ciberseguridadbidaidea.com/convergencia-entre-it-y-ot/#Objetivos_de_seguridad_de_la_convergencia_IT_OT)
- Bonnetto, E., Yannou, B., Yannou-Le Bris, G., Boly, V., & Alvarez, J. (2016). A Categorization of Customer Concerns for an OT Front-End of Innovation Process in IT/OT Convergence Context. Obtenido de [https://www.researchgate.net/publication/318768503\\_A\\_CATEGORIZATION\\_OF\\_CUSTOMER\\_CONCERNS\\_FOR\\_AN\\_OT\\_FRONT-END\\_OF\\_INNOVATION\\_PROCESS\\_IN\\_ITOT\\_CONVERGENCE\\_CONTEXT](https://www.researchgate.net/publication/318768503_A_CATEGORIZATION_OF_CUSTOMER_CONCERNS_FOR_AN_OT_FRONT-END_OF_INNOVATION_PROCESS_IN_ITOT_CONVERGENCE_CONTEXT)
- Campillo, A. (10 de 2022). *Ciberseguridad en tiempos post - Covid*. Obtenido de [https://www.threepoints.com/sites/default/files/2022-10/Informe\\_Ciberseguridad%20en%20tiempos%20post%20covid.pdf](https://www.threepoints.com/sites/default/files/2022-10/Informe_Ciberseguridad%20en%20tiempos%20post%20covid.pdf)
- Checkpoint. (2022). *Purdue Model for ICS Security*. Recuperado el 2024 de 2 de 5, de <https://www.checkpoint.com/es/cyber-hub/network-security/what-is-industrial-control-systems-ics-security/purdue-model-for-ics-security/#PurdueModelforICSSecurity>

- Ciberseguridad. (2021). *¿Qué es el cifrado 3DES y cómo funciona?* Recuperado el 5 de 2 de 2024, de <https://ciberseguridad.com/guias/prevencion-proteccion/criptografia/cifrado-3des/>
- Ciberseguridad. (2021). *¿Qué es el cifrado RSA y cómo funciona?* Recuperado el 5 de 2 de 2024, de <https://ciberseguridad.com/guias/prevencion-proteccion/criptografia/cifrado-rsa/>
- CloudFlare. (2024). *¿Qué es el modelo OSI?* Recuperado el 5 de 2 de 2024, de <https://www.cloudflare.com/es-es/learning/ddos/glossary/open-systems-interconnection-model-osi/>
- Contreras, E. M. (2017). La transición demográfica en la Revolución Industria. *Los ojos de hipatía*(ISSN: 2341-0612).
- Copadata. (2022). *DNP3 (Distributed Network Protocol) e IEC 61850*. Recuperado el 5 de 2 de 2024, de <https://www.copadata.com/es/industrias/energia-infraestructura/energy-insights/dnp3-protocolo-de-red-distribuida/#:~:text=El%20protocolo%20DNP3%2C%20o%20Distributed,pa%C3%ADs%20en%20todo%20el%20mundo>
- Crane, C. (15 de 7 de 2020). *Your Guide to How PKI Works & Secures Your Organization*. Recuperado el 5 de 2 de 2024, de <https://securityboulevard.com/2020/07/your-guide-to-how-pki-works-secures-your-organization>
- Dnp Corp. (2023). *Token Criptográficos*. Recuperado el 5 de 2 de 2024, de <https://certificados-digitales.pe/token-criptografico#:~:text=Un%20dispositivo%20criptogr%C3%A1fico%20es%20un,aceleraci%C3%B3n%20hardware%20para%20operaciones%20criptogr%C3%A1ficas>
- DocuSign. (30 de 10 de 2020). *¿Qué es la infraestructura de clave pública o PKI cuál es su relación con la firma electrónica?* Recuperado el 5 de 2 de 2024, de <https://www.docusign.com/es-mx/blog/pki#:~:text=Autoridad%20de%20certificaci%C3%B3n,est%C3%A9n%20incluidos%20en%20su%20estructura>
- Granados Paredes, G. (10 de 7 de 2006). Introducción a la Criptografía. *Revista Digital Universitaria*, 7. Obtenido de [https://www.revista.unam.mx/vol.7/num7/art55/jul\\_art55.pdf](https://www.revista.unam.mx/vol.7/num7/art55/jul_art55.pdf)
- HERČKO, J., SLAMKOVÁ, E., & HNÁT, J. (2015). *Industry 4.0 – new era of manufacturing*.
- Hermann, M. (2015). *Design Principles for Industrie 4.0 Scenarios: A Literature Review*. Dortmund.
- Heymsfeld, R. (4 de 6 de 2018). *Confidentiality, Integrity and Availability - The CIA Triad*. Obtenido de <https://www.certmike.com/confidentiality-integrity-and-availability-the-cia-triad/>

- IIoT World. (18 de 5 de 2018). *Report on State of IIoT Adoption and Maturity in Three*.  
Obtenido de <https://iiot-world.com/connected-industry/report-on-state-of-iiot-adoption-and-maturity-in-three-industries>
- InfoPLC++. (7 de 2 de 2019). *50 años del PLC: de la 3ª a la 4ª revolución industrial*.  
Recuperado el 2 de 4 de 2024, de <https://www.infoplcn.net/plus-plus/tecnologia/item/106209-50-aniversario-plc>
- International Organization for Standardization. (2013). *ISO/IEC 27001 - Information*. Obtenido de <https://www.iso.org/isoiec-27001-information-security.html>
- Kagermann, H. (2013). *Recomendaciones para la aplicación de la iniciativa estratégica Industria 4.0*. Fráncfort del Meno.
- Kamlofsky, J., Colombo, H., Sliafertas, M., & Pedernera, J. (2015). Un Enfoque para Disminuir los Efectos de los Ciber-ataques a las Infraestructuras Críticas. *CAETI - Universidad Abierta Interamericana*, 1-4.
- Kaspersky. (23 de 8 de 2021). *What is Cyber Security?* Obtenido de <https://www.kaspersky.com/resource-center/definitions/what-is-cyber-security>
- Kott, A., & Linkov, I. (2018). *Cyber Resilience of Systems and Networks* (1ra ed.). Nueva York.
- Kubecka, C. (2015). How to Implement IT Security after a Cyber Meltdown Black Hat USA 2015.
- Lakshmanan, R. (20 de 4 de 2020). *COVID-Themed Lures Target SCADA Sectors With Data Stealing Malware*. Obtenido de <https://thehackernews.com/2020/04/coronavirus-scada-malware.html>
- Lasi, H., & Kemper, H.-G. (19 de 6 de 2014). *Industry 4.0*. (U. o. Stuttgart, Ed.)
- Macroseguridad. (2023). *HSM*. Recuperado el 5 de 2 de 2024, de <https://www.macroseguridad.net/productos/identidad/hsm/concepto.php>
- Macroseguridad. (2023). *PKI Card*. Recuperado el 5 de 2 de 2024, de [https://www.macroseguridad.net/productos/smartcards/pki\\_card/caracteristicas.php](https://www.macroseguridad.net/productos/smartcards/pki_card/caracteristicas.php)
- Macroseguridad. (2023). *Tokens USB*. Recuperado el 5 de 2 de 2024, de [https://www.macroseguridad.net/productos/tokens\\_usb/](https://www.macroseguridad.net/productos/tokens_usb/)
- Madias, J. (2018). *Sistemas de control de procesos en la acería*. Obtenido de [https://www.researchgate.net/publication/323538057\\_Sistemas\\_de\\_control\\_de\\_procesos\\_en\\_la\\_aceria](https://www.researchgate.net/publication/323538057_Sistemas_de_control_de_procesos_en_la_aceria)
- McMillen, D. (27 de 12 de 2016). *Attacks Targeting Industrial Control Systems (ICS) Up 110 Percent*. Obtenido de <https://securityintelligence.com/attacks-targeting-industrial-control-systems-ics-up-110-percent>

- Mendoza T., J. (2008). Demostración de Cifrado Simétrico y Asimétrico. *Revista de Ciencia y Tecnología*. Obtenido de <https://www.redalyc.org/pdf/5055/505554806007.pdf>
- Microsoft. (30 de 11 de 2023). *Introducción a la lista de revocación de certificados del servidor de directivas de red*. Recuperado el 5 de 2 de 2024, de <https://learn.microsoft.com/es-es/windows-server/networking/technologies/nps/network-policy-server-certificate-revocation-list-overview>
- Microsoft. (20 de 3 de 2023). *What is Active Directory Certificate Services?* Recuperado el 5 de 2 de 2024, de <https://learn.microsoft.com/en-us/windows-server/identity/ad-cs/active-directory-certificate-services-overview>
- Ministerio de Modernización. (15 de 12 de 2016). *Dispositivos criptográficos para firma digital (token)*. Obtenido de <https://www.argentina.gob.ar/onti/estandares-tecnologicos/dispositivos-criptograficos-para-firma-digital-token>
- Modbus. (20 de 12 de 2006). *Modbus over Serial Line Specification and Implementation Guide V1.02*. Obtenido de [https://modbus.org/docs/Modbus\\_over\\_serial\\_line\\_V1\\_02.pdf](https://modbus.org/docs/Modbus_over_serial_line_V1_02.pdf)
- Modbus. (26 de 4 de 2012). *Modbus Application Protocol Specification V1.1b3*. Obtenido de [https://www.modbus.org/docs/Modbus\\_Application\\_Protocol\\_V1\\_1b3.pdf](https://www.modbus.org/docs/Modbus_Application_Protocol_V1_1b3.pdf)
- Modbus. (24 de 7 de 2018). *MODBUS/TCP Security Protocol Specification*. Obtenido de [https://modbus.org/docs/MB-TCP-Security-v21\\_2018-07-24.pdf](https://modbus.org/docs/MB-TCP-Security-v21_2018-07-24.pdf)
- Nguyen, J. (9 de 12 de 2015). *Open SSL CA*. Recuperado el 5 de 2 de 2024, de <https://openssl-ca.readthedocs.io/en/latest/introduction.html>
- NIST. (9 de 2023). *Guide to Operational Technology (OT) Security*. Obtenido de <https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-82r3.pdf>
- OpenScada. (2018). *OpenScada*. Recuperado el 5 de 2 de 2024, de [http://oscada.org/wiki/Documents/Quick\\_start](http://oscada.org/wiki/Documents/Quick_start)
- Panda Security. (2023). *¿Qué es el cifrado AES? Una guía sobre el Advanced Encryption Standard*. Recuperado el 5 de 2 de 2024, de <https://www.pandasecurity.com/es/mediacenter/cifrado-aes-guia/>
- Pérez-López, E. (2015). *Los sistemas SCADA en la automatización industrial*. Tecnología en Marcha.
- Profibus. (17 de 2 de 2023). Recuperado el 5 de 2 de 2024, de [https://profibus.com.ar/profibus\\_que\\_es\\_y\\_como\\_funciona](https://profibus.com.ar/profibus_que_es_y_como_funciona)
- ProSoft Technology. (4 de 4 de 2019). Recuperado el 5 de 2 de 2024, de <https://www.prosoft-technology.com/knowledge-base/Protocols/Modbus/Whats-the-difference-between-Modbus-ASCII-and-Modbus-RTU>
- Red Hat. (7 de 5 de 2021). *¿Qué es el Internet industrial de las cosas?* Recuperado el 5 de 2 de 2024, de <https://www.redhat.com/es/topics/internet-of-things/what-is-iiot>



- Sampieri, R. H., Fernandez-Collado, C., & Baptista-Lucio, P. (2006). *Metodología de la Investigación*. México: McGraw-Hill.
- Sanches Gómez, D. (2019). *Desarrollo de un sistema eficiente de análisis del protocolo IEC 60870-5-104 para la detección de anomalías en redes Scada*. España. Obtenido de [https://repositorio.uam.es/bitstream/handle/10486/689052/sanches\\_gomez\\_david\\_tfg.pdf?sequence=1](https://repositorio.uam.es/bitstream/handle/10486/689052/sanches_gomez_david_tfg.pdf?sequence=1)
- Schenider Electric. (2024). *M221 PLC 16 ES Rele ETH Compact*. Recuperado el 5 de 2 de 2024, de <https://www.se.com/ar/es/product/TM221CE16R/m221-plc-16-es-rele-eth-compact/>
- SDI. (2022). *¿Qué es un protocolo de comunicación y cuál es el más utilizado?* Recuperado el 5 de 2 de 2024, de <https://sdindustrial.com.mx/blog/protocolos-de-comunicacion-que-son/>
- Self Bank. (9 de 5 de 2023). Recuperado el 2 de 5 de 2024, de <https://blog.selfbank.es/como-han-cambiado-el-mundo-las-revoluciones-industriales>
- SSL.com. (10 de 10 de 2023). *¿Qué es una función criptográfica de hash?* Obtenido de <https://www.ssl.com/es/preguntas-frecuentes/%C2%BFQu%C3%A9-es-una-funci%C3%B3n-hash-criptogr%C3%A1fica%3F/>
- Thales. (2023). *Luna Network HSM 7 Required Items*. Obtenido de [https://thalesdocs.com/gphsm/luna/7/docs/network/Content/install/network\\_hw\\_install/received\\_items\\_sa.htm](https://thalesdocs.com/gphsm/luna/7/docs/network/Content/install/network_hw_install/received_items_sa.htm)
- Trend Micro. (2021). *Industrial Control System*. Recuperado el 5 de 2 de 2024, de <https://www.trendmicro.com/vinfo/us/security/definition/industrial-control-system>
- Trend Micro. (2022). *Why Do Attackers Target Industrial Control Systems?* Recuperado el 5 de 2 de 2024, de <https://www.trendmicro.com/vinfo/us/security/news/cyber-attacks/why-do-attackers-target-industrial-control-systems>
- Trend Micro. (2023). *¿Qué es el Ransomware?* Recuperado el 5 de 2 de 2024, de [https://www.trendmicro.com/es\\_mx/what-is/ransomware.html#:~:text=El%20ransomware%20es%20un%20tipo,trav%C3%A9s%20de%20la%20extorsi%C3%B3n%20digital](https://www.trendmicro.com/es_mx/what-is/ransomware.html#:~:text=El%20ransomware%20es%20un%20tipo,trav%C3%A9s%20de%20la%20extorsi%C3%B3n%20digital)
- UpKeep. (2022). *Explicación de los sistemas SCADA / Mantenimiento*. Recuperado el 5 de 2 de 2024, de <https://upkeep.com/es/learning/scada-systems-explained/#c%C3%B3mo-funciona-scada>
- Vallejo, H. (2019). Los Controladores Lógicos Programables. *Saber Electrónica, 166*. Obtenido de <https://es.scribd.com/document/441002034/Saber-Electronica-N%C2%BA-166-Edicion-Argentina>
- Vazquez, S. (2015). Ciberseguridad en Paraguay. III Conferencia Internacional y Taller de Ciberseguridad e Infraestructuras Críticas de Información. Buenos Aires.