Universidad Abierta Interamericana

Seguridad de entornos SCADA basada en infraestructura de clave pública PKI

Tutoría Técnica: Mg. Jorge Alejandro Kamlofsky

Profesora de Trabajo Final: Dra. Marcela Rosalba Samela

Alumno: Facundo Albano Bernardi

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

julio, 2025

Resumen

Los Sistemas de Supervisión, Control y Adquisición de Datos, comúnmente conocidos como *SCADA* "Supervisory Control and Data Acquisition", automatizan y gestionan procesos industriales complejos sin intervención humana. Debido a su finalidad específica de control, este tipo de solución fue concebida para operar en redes independientes, completamente aisladas del entorno empresarial. La integración de tecnologías impulsada por la transformación digital, y su particular aplicación en los entornos productivos, comúnmente denominada como cuarta revolución industrial -RI4- o "Industria 4.0", plantearon un modelo de gestión completamente integrado e interconectado. Esta integración ha generado numerosos desafíos en torno a la seguridad e integridad de los sistemas de misión crítica, ya que la distinción entre los entornos productivos y empresariales ha comenzado a desvanecerse debido a los crecientes requerimientos de conectividad del hardware (y, por consiguiente, de sus fabricantes) que compone dichos entornos.

Esta propuesta de intervención profesional se centrará en el análisis de las debilidades y puntos de mejora en los flujos de comunicación dentro de los entornos SCADA. En base a los resultados, se desarrollará una propuesta que incluirá la implementación de un mecanismo de seguridad basado en infraestructuras de clave pública "PKI", tecnología ampliamente adoptada para la autenticación de usuarios y dispositivos en entornos digitales. La implementación de esta solución fortalecerá las comunicaciones entre los componentes del sistema SCADA, asegurando la integridad de la información almacenada y, por ende, la continuidad operativa de los sistemas que estas plataformas soportan.

Palabras Clave: control industrial, criptosistemas de clave pública, protección de las infraestructuras, redes scada

Abstract

Supervisory Control and Data Acquisition Systems, commonly known as SCADA, are designed to automate and manage complex industrial processes without human intervention. Originally, these systems were intended to operate on stand-alone networks, completely isolated from the business environment. However, the digital transformation and its application in production environments—often referred to as the Fourth Industrial Revolution (Industry 4.0)—have led to a fully integrated and interconnected management model. This integration has created numerous challenges regarding the security and integrity of mission-critical systems, as the separation between production and business environments has begun to blur due to the increasing connectivity requirements of installed hardware and its manufacturers.

This document will analyze the weaknesses and areas for improvement in communication flows within SCADA environments. Based on the findings, a professional proposal will be developed, which will include implementing a security mechanism based on Public Key Infrastructure "PKI." PKI is a widely adopted technology for user and device authentication in digital environments. Implementing this solution will enhance communication flows between SCADA system components, ensuring the integrity of stored information and, consequently, maintaining the operational continuity of the systems supported by these platforms.

Keywords: industrial control, infrastructure protection, public key cryptosystems, scada networks

Dedicatoria

(Por orden de aparición)

A Lili y Yanny, por haberme inculcado desde temprana edad que la educación era el camino por seguir.

A Ana Belén, por acompañarme en todos los ámbitos de mi vida y motivarme en mi desarrollo académico y personal.

A Filippa, por enseñarme a soltar, y a interpretar la vida con una visión más flexible.

Reconocimientos

A la Dra. Marcela Rosalba Samela, por su invaluable capacidad para transmitirle a todos sus alumnos valores fundamentales como la ética, la integridad y la responsabilidad, indispensables para el desarrollo de mejores profesionales, acordes a las demandas del mundo actual.

Al Mg. Jorge Alejandro Kamlofsky, por su disponibilidad e impecable labor como tutor en el desarrollo de este trabajo, compartiendo no únicamente su conocimiento, sino su visión y experiencia sobre la problemática abordada.

A mis compañeros de la universidad, por las horas compartidas, el trabajo en equipo y los vínculos que construimos, trascendiendo el ámbito académico.

Índice General

Índice de Figuras

Índice de Tablas

Estructura General del Trabajo Final

Capítulos

El capítulo 1 proporcionará una visión general de la propuesta de intervención en cuestión, partiendo de una problemática base, y los motivos que justifican el desarrollo e implementación de una solución acorde. Por otro lado, se proveerán detalles sobre el marco de aplicación, así como la definición de los objetivos generales y específicos de la propuesta.

En el capítulo 2 será desarrollado el estado del arte, abordando en primera instancia el impacto de la transformación digital en los procesos de manufactura, la convergencia entre las redes corporativas e industriales, y las amenazas asociadas con este tipo de integración.

El capítulo 3 proporcionará el marco teórico sobre el cuál la propuesta en cuestión estará desarrollada, haciendo especial énfasis en las redes industriales y los criptosistemas. Por otro lado, el desarrollo del proyecto será abarcado en el capítulo 4, detallando tanto los aspectos técnicos cómo aquellos relacionados con los recursos intervinientes. El capítulo 5 estará destinado a la evaluación del proyecto, con su correspondiente análisis FODA, factores condicionantes y análisis de costos asociados. Por último, el capítulo 6 incluirá las conclusiones de cierre, junto con una serie de recomendaciones finales.

Capítulo I - Introducción

1.1 Naturaleza del proyecto

Los Sistemas de Supervisión, Control y Adquisición de Datos (SCADA) se han consolidado como el estándar global para el monitoreo y control de infraestructuras críticas, desempeñando un papel fundamental tanto en entornos industriales como en infraestructuras esenciales para el funcionamiento de las naciones (Krutz, 2006). Gracias a esta tecnología, es posible centralizar la integración de datos recolectados desde diversos sensores de campo, equipos y PLCs, lo que facilita la entrega y continuidad de los servicios productivos. Entre estos servicios se incluyen, por ejemplo, las redes de distribución de energía, las plantas de tratamiento de efluentes y las plataformas de control de tráfico, entre otros (Alanazi et al., 2022).

1.2 Justificación

Tal como lo indican Bartman & Carson (2016), la creciente demanda de conectividad entre las soluciones SCADA e internet trae aparejado el riesgo potencial de sufrir ataques cibernéticos dirigidos hacia los componentes de nuestros sistemas de misión crítica. Debido a su propósito inicial, la falta de mecanismos de seguridad que garanticen la fiabilidad de las comunicaciones dentro de este tipo de entorno los convierte en un blanco para intentos de sabotaje y/o espionaje, representando un riesgo cada vez más significativo. El potencial atacante podría explotar las vulnerabilidades conocidas de cada componente, pudiendo causar un impacto catastrófico en la infraestructura instalada, y por consiguiente en los servicios que dependan de ella (Bartman & Carson, 2016).

1.3 Marco Institucional

La presente propuesta de intervención está dirigida principalmente a organismos y/o empresas que cuenten con entornos de misión crítica, entornos fabriles con líneas de producción, o bien con la provisión de servicios de soporte a las naciones. La solución por desarrollar es potencialmente aplicable a entornos productivos de menor tenor, aunque

existen limitantes (principalmente económicas) que podrían requerir una evaluación costo-beneficio en profundidad.

1.4 Objetivos del Trabajo Final de Carrera

1.4.1 Objetivo General

Proponer la implementación de una solución de cifrado basada en PKI sobre los flujos de comunicación del entorno SCADA, que permita verificar y autenticar los diferentes dispositivos de campo que interactúan con la estructura de supervisión (PLC maestro).

1.4.2 Objetivos Particulares

Para alcanzar el objetivo general, se deben cubrir los siguientes aspectos:

- Analizar las soluciones de seguridad criptográficas aplicables a este tipo de entorno.
- Plantear la implementación de un escenario integrando la tecnología PKI dentro de un entorno de misión crítica.
- Elaborar un estudio de viabilidad técnico-económico que complemente la solución técnica.

Capítulo II – Estado del Arte

2.1 La Industria 4.0 y su impacto en los sistemas de manufactura

2.1.1 Introducción

En la actualidad, la producción industrial está impulsada por la competencia global y la necesidad de adaptarse de manera prácticamente inmediata a las exigencias del mercado. Este tipo de demanda puede satisfacerse únicamente gracias a los avances radicales en las tecnologías de manufactura (Rojko, 2017). La *Industria 4.0* brinda un enfoque basado en la integración de los procesos empresariales y de fabricación, así como en la integración de todos los actores de la cadena de valor de la empresa (clientes y proveedores). Desde la perspectiva técnica, dicha integración se aborda a través de conceptos genéricos como los sistemas ciber-físicos (CPS, del inglés *Cyber-Physical Systems*) y de la Internet de las Cosas (IoT, del inglés *Internet of Things*) aplicados a los sistemas de producción convencionales (Rojko, 2017).

Según lo indica Rojko (2017), el sistema de ejecución sobre el cual se monta la industria 4.0 está compuesto por diversos bloques interconectados, con características propietarias, denominados bloques CPS o *CPS building blocks*; Dichos bloques son sistemas embebidos con control descentralizado y características de conectividad avanzada, lo que les permite recolectar e intercambiar información en tiempo real, con el objetivo de identificar, supervisar y optimizar los procesos de producción (Rojko, 2017). Por otro lado, los sistemas que soportan los procesos de manufactura (MES, del inglés *Manufacturing Execution Systems*) y la planificación de recursos (ERP, del inglés *Enterprise Resources Planning*) requieren del seguimiento, mantenimiento y soporte continuo para garantizar la correcta integración entre los procesos de manufactura y del negocio (Rojko, 2017).

Por último, es necesario mencionar que el volumen de la información recolectada de los procesos, maquinarias y productos no es para nada despreciable, y requiere de medios acordes para poder almacenarla, procesarla y, posteriormente, convertirla de datos “en crudo” a información útil para el negocio (Rojko, 2017).

El tiempo de respuesta de las naciones para implementar e impulsar la transición hacia las nuevas tecnologías representa una ventaja estratégica a la hora de posicionarse en los mercados globales; Tal es así que muchas de las iniciativas fueron impulsadas por los gobiernos, siendo

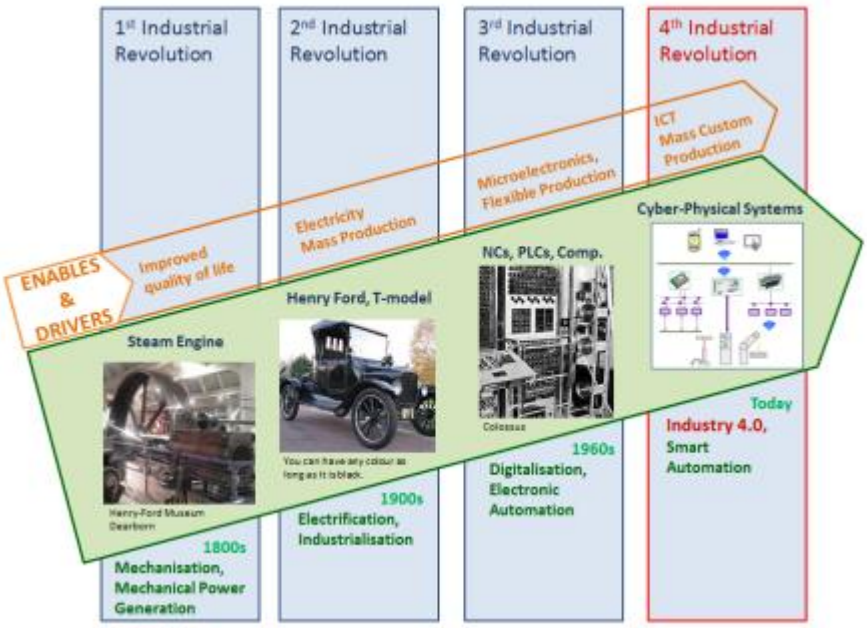
Alemania el pionero en implementar dicha iniciativa, además de acuñar el concepto en cuestión (Rojko, 2017).

2.1.2 Industria 4.0: Visión general

Las etapas del desarrollo de los sistemas de manufactura industrial, desde el trabajo manual hasta el concepto de Industria 4.0, pueden representarse como un hilo conductor a través de las cuatro revoluciones industriales. Dicha evolución se representa en la Figura 1:

Figura 1

Hitos y disparadores a través de las revoluciones industriales



*Nota. Obtenido de Industry 4.0 Concept: Background and Over*view, por Rojko, 2017

De acuerdo con lo indicado por Rojko (2017), la base tecnológica que caracteriza a la cuarta revolución industrial es la automatización de los sistemas ciber-físicos con control descentralizado y conectividad avanzada (funcionalidades IoT). Como consecuencia de dicha transición, los sistemas de manufactura clásicos (automatización jerárquica) pueden convertirse en sistemas de manufactura ciber-físicos, permitiendo ajustar los volúmenes de producción de manera flexible.

2.1.3 Origen de la Industria 4.0

La Industria 4.0 es una iniciativa estratégica del gobierno alemán que, históricamente, apoyó fuertemente el desarrollo del sector industrial. En este sentido, la Industria 4.0 también puede interpretarse como una iniciativa para mantener la posición influyente de Alemania como líder en la fabricación de maquinaria y automóviles (Rojko, 2017).

El concepto básico de Industria 4.0 fue introducido en la feria de Hannover en el año 2011; Desde su presentación, se ha convertido en un tema de debate e investigación recurrente, tanto en Alemania como en el resto del mundo, en diversos ámbitos (académicos, industriales, etc.). Según Rojko (2017), la idea principal es aprovechar el potencial de las nuevas tecnologías y conceptos como disponibilidad y uso de la internet e IoT, integración de los procesos tecnológicos y del negocio en las empresas, Mapeo digital y virtualización del mundo real y, por último, fábricas "inteligentes" que incluyan medios de producción industrial "inteligentes" y productos "inteligentes".

Además de las consecuencias propias de la introducción de conceptos como la digitalización y la adopción de nuevas tecnologías, la Industria 4.0 busca también lidiar con la escasez de los recursos utilizados para maximizar el beneficio en los procesos de manufactura, y encontrar otros recursos novedosos. En concreto, los costos de manufactura se redujeron de manera drástica con la introducción de metodologías como la producción "justo a tiempo", producción sin desperdicios (lean manufacturing) y, sobre todo, con la externalización de la producción a países con menores costos de mano de obra (Rojko, 2017).

Sin duda alguna, desde la perspectiva de la reducción de costos, la Industria 4.0 es una solución prometedora. En este aspecto, algunas fuentes coinciden en que la implementación de los conceptos antes mencionados podría traer aparejada una reducción en los costos de producción, logísticos y de control de calidad que rondan entre 10% y 30%.

Rojko (2017) menciona además que existen otras razones que podrían motivar la adopción temprana de la Industria 4.0, fuertemente vinculadas con la eficiencia en los procesos en general, tales como la reducción de plazos para el desarrollo y lanzamiento de nuevos productos al mercado y una mayor capacidad de respuesta a la demanda, posibilitando también una suerte de producción en serie a medida, sin incrementar notablemente los costos globales de producción, generando

también un entorno de laboral flexible, y contribuyendo con el planeta, haciendo uso eficiente de los recursos naturales y de la energía (Rojko, 2017).

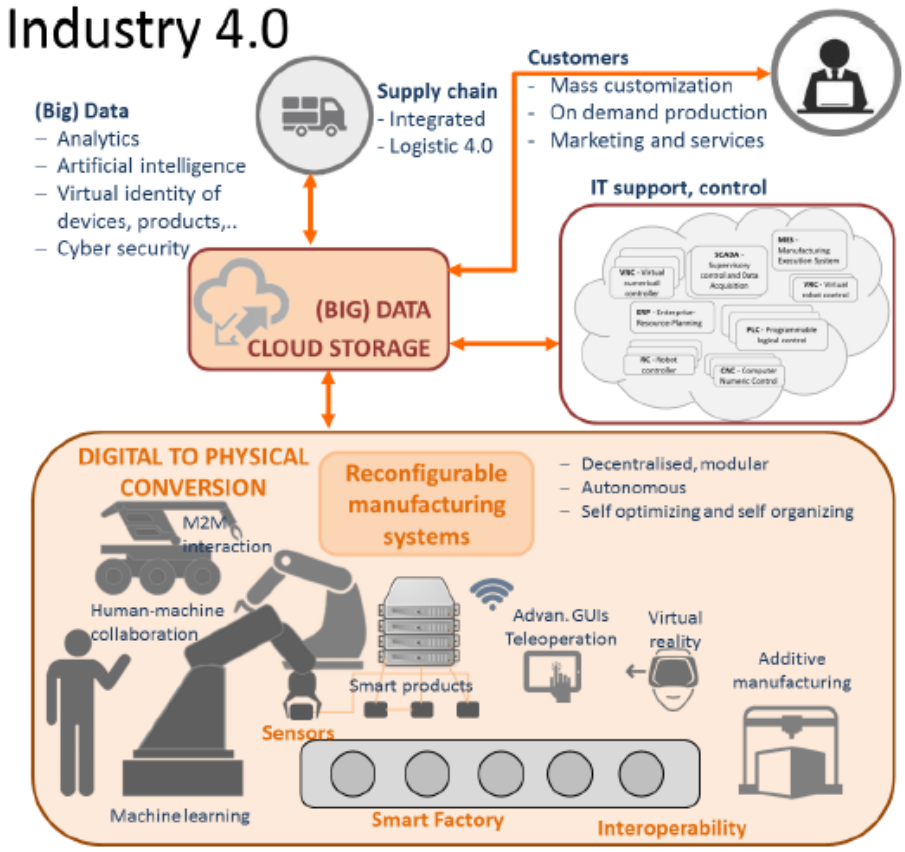
2.1.4 Industria 4.0: Fábricas inteligentes

La figura número 2, obtenida de (Rojko, 2017) ejemplifica la visión de fábrica inteligente bajo el concepto de la Industria 4.0. El proceso central está basado en la conversión digital a física en un sistema de manufactura reconfigurable. Este tipo de sistema podría considerarse el estado del arte en el desarrollo de sistemas de manufactura. Un sistema de producción tradicional está compuesto por líneas de producción fijas, con maquinaria dedicada a la realización de tareas específicas, de modo tal que puede producir un único tipo de producto (Rojko, 2017). La siguiente evolución se caracterizó por los sistemas de producción flexibles, incorporando máquinas programables, que permitieron la producción de una variedad de productos diferentes, pero no ofrecían flexibilidad en la capacidad de producción. Como resultado, en la actualidad existen sistemas de manufactura reconfigurables, capaces de adaptar sus componentes de hardware y

software para suplir los requisitos cambiantes del mercado en cuanto a tipo y cantidad de productos (Rojko, 2017).

Figura 2

Representación de una fábrica inteligente bajo el concepto Industria 4.0



Nota. Obtenido de *Industry 4.0 Concept: Background and Overview,* por Rojko, 2017

Las maquinarias que equipan una fábrica inteligente se conocen como sistemas ciber físicos, sistemas físicos integrados con componentes de TIC. Son sistemas autónomos, capaces de tomar decisiones basadas en algoritmos de aprendizaje automático y captura de datos en tiempo real, resultados de análisis y comportamientos exitosos registrados en el pasado. Típicamente, se utilizan máquinas programables (CNC, del inglés *Computer Numerical Control*, y NC, del inglés *Numerical Control*), con una gran cantidad de agentes móviles y robots capaces de organizarse y optimizarse de manera automática (Rojko, 2017).

Los productos de este tipo de fábricas son también “inteligentes”, contando con sensores integrados que utilizan la conectividad inalámbrica para la recolección de datos en tiempo real, tales como localización, estado y condiciones del ambiente. Asimismo, este tipo de producto cuenta con capacidades embebidas de control y procesamiento, pudiendo controlar su recorrido dentro de la línea de producción, e inclusive readaptarlo en tiempo real para optimizar el flujo de trabajo. Adicionalmente, los productos inteligentes son capaces de monitorear su propio estado durante su ciclo de vida, permitiendo llevar a cabo un programa de mantenimiento proactivo, basado en su estado de operación actual, siendo especialmente beneficioso en aquellos productos que integran sistemas de mayor envergadura (Rojko, 2017).

Otros elementos críticos que también forman parte del concepto de la Industria 4.0 son la conectividad y la interoperabilidad. El flujo continuo de información entre los diversos dispositivos y componentes, la interacción entre máquina y máquina (M2M, del inglés *Machine to Machine*), los sistemas de fabricación y otros actores debe abordarse de manera adecuada, a fin de proporcionar un medio sólido para que las maquinarias, productos y otros componentes del ecosistema industrial puedan interconectarse y comunicarse a través del IoT industrial (basado principalmente en redes inalámbricas) de fabricación y agentes. De este modo, las máquinas, los productos y las fábricas pueden conectarse y comunicarse a través del IoT industrial (basado principalmente en redes inalámbricas) (Rojko, 2017). Los conceptos de conectividad e interoperabilidad serán abordados con mayor nivel de detalle en los capítulos subsiguientes.

2.2 Sistemas SCADA

2.2.1 Introducción

Tal como lo define Krutz (2006), los Sistemas de Control y Adquisición de Datos (en adelante, SCADA) son componentes vitales en las infraestructuras críticas de la mayoría de los países. Este tipo de solución puede encontrarse en el control de oleoductos, sistemas de tratamiento y distribución de agua, sistemas de transporte, refinerías, y una amplia variedad de operaciones de manufactura.

Los sistemas SCADA proporcionan a la dirección datos en tiempo real sobre los procesos productivos, implementando paradigmas de control eficientes, contribuyendo además con la seguridad del entorno y el personal involucrado, y reduciendo al mismo tiempo los costos operativos. Estos beneficios pueden materializarse gracias al uso del software y hardware que

compone este tipo de soluciones, combinado además con protocolos de comunicación mejorados, y una mayor interconectividad con las redes externas, incluida internet (Krutz, 2006).

2.2.2 Definición

Según Rodriguez Penin (2013), un sistema SCADA podría definirse como una aplicación, o conjunto de aplicaciones de software, que permita el acceso a datos remotos de un proceso y permita, utilizando las herramientas de comunicación necesarias en cada caso, el control de este.

Aunque el alcance inicial de este tipo de solución se encontraba limitado a la supervisión y adquisición de datos en procesos de control, la evolución del hardware y los métodos de comunicación han permitido expandir el campo de acción e interconectar diversos entornos SCADA con un único ordenador principal de supervisión (Rodriguez Penin, 2013).

El sistema permite comunicarse con los dispositivos de campo (controladores autónomos, autómatas programables, sistemas de dosificación, etc.) para controlar el proceso en forma automática desde la pantalla del ordenador, que es configurada por el usuario y puede ser modificada con facilidad. Además, provee a diversos usuarios de toda la información que se genera en el proceso productivo (Rodriguez Penin, 2013).

2.2.3 Características

Un sistema SCADA típico posee ciertas características distintivas que lo hacen adecuado para supervisar y controlar procesos industriales y de infraestructura crítica. A continuación, se detallan algunas características clave:

a) Comunicación con Dispositivos Remotos: Una red SCADA está diseñada para comunicarse con dispositivos remotos distribuidos en una amplia área geográfica. Esto puede incluir sensores, actuadores y controladores ubicados en sitios remotos como plantas de energía, estaciones de tratamiento de agua o instalaciones de producción.
b) Adquisición de Datos en Tiempo Real: La capacidad de recopilar datos en tiempo real es fundamental en una red SCADA. Esto permite a los operadores monitorear el estado de los procesos en tiempo real y tomar decisiones rápidas en función de la información más reciente.

c) Interfaz de Usuario Gráfica: Las interfaces de usuario en los sistemas SCADA suelen ser gráficas e intuitivas. Esto permite a los operadores visualizar fácilmente datos de proceso, alarmas, tendencias y otros indicadores clave de rendimiento.
d) Control Remoto de Dispositivos: Además de la supervisión, una red SCADA también puede permitir el control remoto de dispositivos. Esto significa que los operadores pueden enviar comandos para iniciar, detener o ajustar equipos y procesos desde una ubicación centralizada.
e) Redundancia y Tolerancia a Fallos: Dada la importancia crítica de muchos sistemas supervisados por SCADA, las redes SCADA suelen incorporar redundancia y mecanismos de tolerancia a fallos para garantizar la disponibilidad continua del sistema, incluso en caso de fallos de hardware o comunicaciones.
f) Protocolos Específicos: Las redes SCADA a menudo utilizan protocolos de comunicación especializados, como Modbus, Modbus *TCP*, DNP3 o OPC, que están diseñados para funcionar en entornos industriales y proporcionar una comunicación eficiente y confiable entre dispositivos.

Estas características combinadas permiten a las redes SCADA supervisar, controlar y optimizar una amplia variedad de procesos industriales y de infraestructura crítica de manera eficiente y segura.

2.2.4 Arquitectura

En líneas generales, la arquitectura básica de un sistema SCADA podría dividirse en cinco bloques principales:

a) Operador: El operador humano a cargo del monitoreo y las funciones de supervisión y control del sistema SCADA para el entorno de aplicación. (Krutz, 2006)
b) Interfaz Humano-Máquina (o HMI): Presenta los datos al operador y proporciona parámetros de control en una variedad de formatos, incluyendo gráficos, esquemas, menús desplegables, pantallas táctiles, etc. (Krutz, 2006)
c) Unidad Terminal Maestra (o MTU): Representa a la unidad maestra en una arquitectura maestro-esclavo. La MTU presenta los datos al operador a través de la HMI, recoge los datos del componente remoto y le transmite las señales de control. La velocidad de

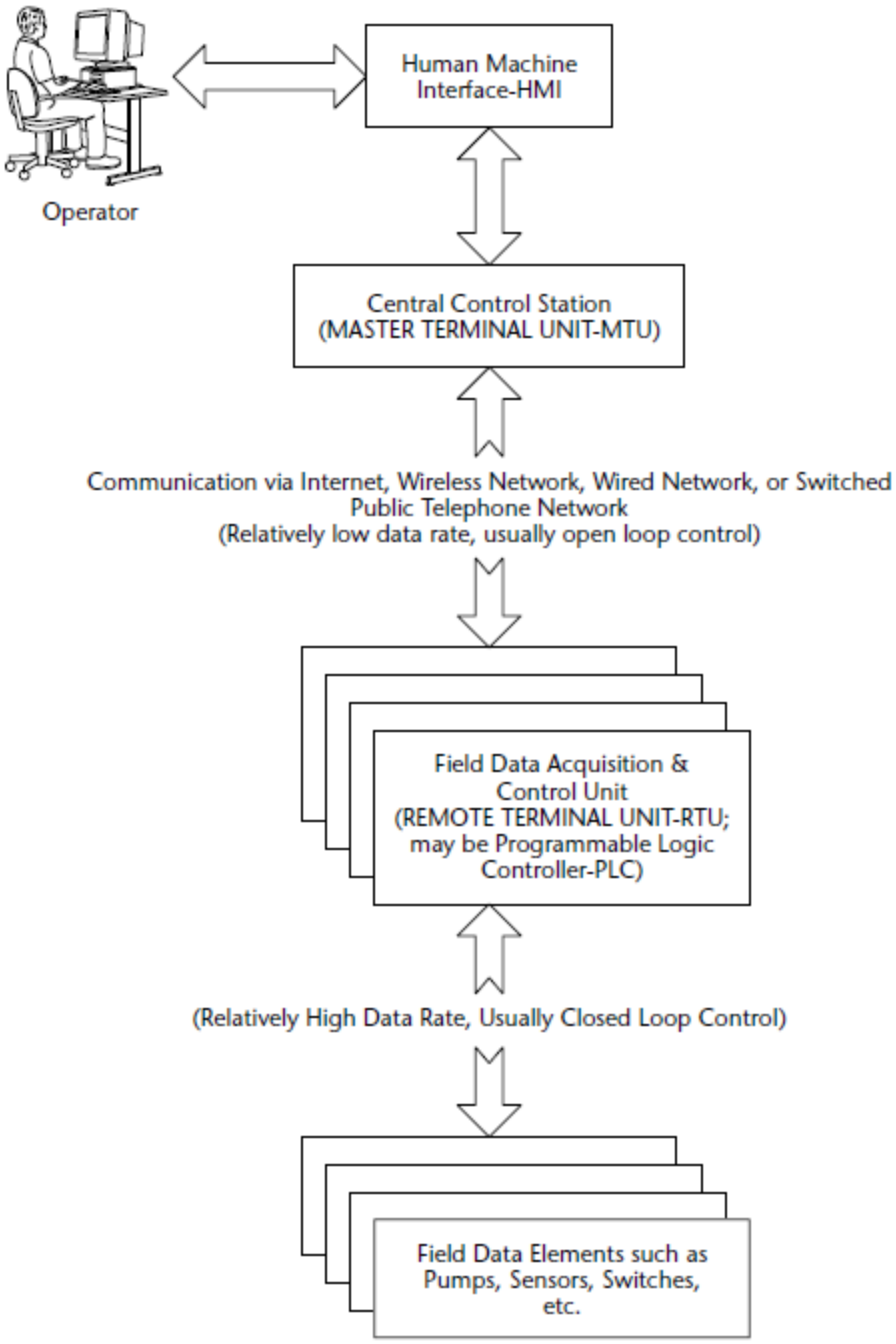
transmisión de datos entre la MTU y los componentes remotos es relativamente baja, y el método de control suele tratarse de un lazo abierto, debido a los posibles retrasos y/o interrupciones del flujo de datos. (Krutz, 2006)

d) Medios de interconexión: Métodos de comunicación entre la MTU y los componentes remotos. Entre los medios más comunes, podemos mencionar las redes de datos (cableadas o inalámbricas), redes de telefonía pública conmutada, o bien la internet. (Krutz, 2006)
e) Unidad Terminal Remota (o RTU): Representa al componente esclavo en una arquitectura maestro-esclavo. La RTU envía comandos a los dispositivos que controla, adquiriendo a su vez datos de estos dispositivos, y retransmitiéndolos a la MTU. La velocidad de transmisión de datos entre la RTU y los dispositivos que comanda es relativamente alta, y el método de control suele ser un lazo cerrado (Krutz, 2006). El ejemplo más común de una RTU podría ser un PLC.

La figura número 3, obtenida de (Djiev, 2003), representa la arquitectura básica de un sistema SCADA:

Figura 3

Arquitectura básica de un sistema SCADA



Nota. Obtenido de *Industrial Networks for Communications and Controls, por Djiev, 2003*

2.2.5 Aplicaciones comunes

Los sistemas SCADA desempeñan un papel fundamental en numerosas aplicaciones, principalmente industriales. Algunas de las industrias que utilizan este tipo de solución en su

operación diaria son las plantas de tratamiento y distribución de agua potable, así como aquellas que actúan sobre las aguas servidas. Los sistemas de generación, transmisión y distribución de energía eléctrica representan un ejemplo de aplicación ideal para este tipo de tecnologías, junto con otras fuentes de generación tales como los sistemas de tratamiento de petróleo y gas. Asimismo, este tipo de solución podría implementarse en cualquier proceso de manufactura que aporte valor al producto final (electrónica, indumentaria, alimentación, etc.) (Alanazi et al., 2022). A continuación, se proporciona una breve descripción de las aplicaciones comunes en las diversas industrias citadas:

- Sistemas de tratamiento de aguas: Los sistemas SCADA permiten monitorear y controlar en tiempo real los sistemas de bombeo para extracción del agua, así como para su posterior tratamiento (control de llenado/vaciado de tanques, apertura/cierre de compuertas, etc.). Asimismo, permiten gestionar el sistema de bombeo que regula la presión del suministro hacia el cliente final (Alanazi et al., 2022).
- Sistemas de tratamiento de aguas servidas: Los sistemas SCADA aplicados en el tratamiento de aguas residuales supervisan y controlan las estaciones elevadoras utilizadas para bombear las aguas servidas a las plantas de tratamiento. Una vez que las aguas residuales llegan a destino, el proceso de depuración se controla paso a paso mediante SCADA. Asimismo, los indicadores provistos por los sistemas de monitoreo pueden utilizarse para documentar las operaciones y generar informes que verifiquen el cumplimiento de las normativas gubernamentales vigentes (Alanazi et al., 2022).
- Sistemas de generación, transmisión y distribución de energía eléctrica: La aplicación de SCADA en este tipo de sistema comprende la supervisión de cada una de las fases de generación de electricidad, desde la entrada del material combustible hasta la línea de salida eléctrica. Las plantas generadoras deben ser capaces de responder instantáneamente ante las fluctuaciones de la demanda. Por otro lado, las distribuidoras de energía eléctrica utilizan soluciones SCADA para supervisar la cantidad de energía que se trasmite en tendidos de media y larga distancia, proporcionando supervisión y control de las subestaciones y líneas de distribución. Asimismo, proporcionan funciones de seguridad y protección; Al monitorear en tiempo real las tareas de transporte, cualquier

avería/interrupción en el circuito será detectada y subsanada a modo de restablecer el suministro eléctrico a la brevedad (Alanazi et al., 2022).

- Sistemas de tratamiento de petróleo y gas: A diferencia de los sistemas eléctricos y de telecomunicaciones, las soluciones SCADA aplicadas en la gestión de petróleo y gas se caracterizan por desplazar sustancias físicas a través de una infraestructura de gran envergadura y extensión a nivel geográfico. Dicha solución se utiliza para el monitoreo de los yacimientos petrolíferos y pozos de bombeo, además de controlar la presión y el flujo de las tuberías de distribución. Al igual que en los sistemas de generación, transmisión y distribución de energía eléctrica, el software SCADA proporciona una capa adicional de seguridad, ya que permite la detección de anomalías e intervención temprana a modo de evitar eventos catastróficos (Alanazi et al., 2022).
- Sistemas de manufactura: Los sistemas SCADA aplicados en sistemas de manufactura pueden controlar con precisión casi todas las operaciones de un entorno fabril. El monitoreo y control de las líneas de producción representa una de las aplicaciones básicas para este tipo de solución, gestionando parámetros complejos (temperatura, presión, humedad, entre otros), y permitiendo garantizar el cumplimiento de los objetivos productivos. Por otro lado, dichos sistemas permiten controlar componentes de automatización avanzados (ej.: brazos robotizados en las líneas de montaje), así como supervisar la utilización de materia prima, a modo de controlar el inventario en tiempo real (Alanazi et al., 2022).
- Sistemas de manufactura de alimentos: La aplicación de SCADA en este tipo de entornos procura garantizar la calidad total del producto, cumpliendo además con los objetivos de producción. La solución puede gestionar de manera integral el proceso de manufactura de alimentos, controlando la mezcla/proporción exacta de cada uno de los ingredientes, así como el tiempo de cocción y temperatura necesarias para el correcto procesamiento de los alimentos; Asimismo, los parámetros arrojados por este tipo de solución contribuyen con la generación de indicadores productivos, que a su vez podrían alimentar reportes de gestión y/o documentación de soporte para procesos de auditoría/cumplimiento de normativas gubernamentales (Alanazi et al., 2022).
- Sistemas de transporte masivos: Por último, la adopción de arquitecturas SCADA en sistemas de transporte público, de uso cotidiano, es prácticamente masiva. Los sistemas de

ferrocarriles y/o subterráneos implementan estas soluciones para cronometrar sus operaciones y gestionar los sistemas de control (ej.: cambios de vías) para que las formaciones puedan circular por los trazados de manera eficiente y segura, sin entrecruzarse; Asimismo, los sistemas de señalización ferroviarios están sincronizados y pueden operarse a distancia gracias a este tipo de solución. Por último, los sistemas de control viales (ej.: semáforos) también adoptan soluciones SCADA para mejorar el flujo de tráfico y maximizar la seguridad (Alanazi et al., 2022).

2.2.6 La importancia de la seguridad en entornos SCADA

Tal como lo indican Alanazi et al (2022), los sistemas SCADA son ampliamente utilizados para el control de oleoductos, sistemas de transmisión de energía eléctrica, yacimientos de gas y petróleo, redes de distribución de gas natural y generación de energía (convencional y/o nuclear). Con el objetivo de lograr mayor flexibilidad y eficiencia, los avances en las tecnologías de la información y telecomunicaciones impulsaron la interconexión de los sistemas SCADA con redes corporativas e incluso con Internet. Como resultado, los sistemas de control industrial (ICS) se vieron expuestos a amenazas y riesgos suponen serias consecuencias (Kamlofsky, 2019). Cualquier intrusión malintencionada o accidental en un sistema SCADA podría causar daños irreparables a nivel humano, material y económico. Tal como lo menciona Kamlofsky et al (2015) un claro ejemplo de ello es el ataque a una planta de enriquecimiento de uranio en Irán, a cargo del virus Stuxnet en 2010. Este hecho generó una conmoción en la comunidad internacional respecto a las vulnerabilidades en las infraestructuras basadas en estas tecnologías, quienes se encuentran actualmente trabajando en soluciones para esta problemática. Es por ello por lo que, para colaborar con la mitigación de este tipo de amenazas, es fundamental trabajar en la protección de los activos informáticos y redes de comunicaciones. El correcto análisis e implementación de un esquema de seguridad adecuado garantizará la continuidad de los servicios frente a acciones hostiles y/o ciberataques, garantizando también la resiliencia e integridad de los procesos y acciones. Para abordar esta cuestión, este documento analiza las vulnerabilidades y amenazas a la seguridad en este tipo de entornos, haciendo foco puntualmente en los flujos de comunicación internos, proponiendo una capa de seguridad sólida basada en criptosistemas.

Capítulo III – Marco Teórico

3.1 Redes Industriales

3.1.1 Introducción

Tal como lo indica Djiev (2003), a comienzos del siglo XX, los sistemas de manufactura y control de los procesos se diseñaron en base a componentes mecánicos, utilizando dispositivos analógicos para cumplir con las funciones de monitoreo y control. Posteriormente, la introducción de componentes neumáticos e hidráulicos hicieron posible el control y gestión de los sistemas remotos a través de una plataforma de control centralizada (Djiev, 2003).

A principios de los años 60, una computadora digital fue aplicada por primera vez como un controlador digital; El término DDC (*control digital directo*) fue utilizado para enfatizar el control directo que una computadora ejercía sobre un proceso en particular, aunque su aplicación para este tipo de finalidad resultaba realmente costosa. En paralelo, el desarrollo del *controlador lógico programable* (PLC, del inglés *Programmable Logic Controller*), permitió reemplazar los controladores convencionales, basados en relés, ofreciendo una amplia gama de funcionalidades que sus antecesores no podrían cubrir (Djiev, 2003). Es necesario aquí hacer un pequeño paréntesis para mencionar la importancia que revisten los *controladores lógicos programables* en el desarrollo de este trabajo: desde su introducción, los PLC han sido un mecanismo clave para simplificar, agilizar y automatizar una amplia variedad de las tareas comprendidas en los procesos industriales. Estos controladores permiten, entre otras cosas, la ejecución de determinadas tareas sin contar con la presencia y/o supervisión humana, convirtiéndolos en componentes ideales para sistemas críticos, que podrían comprometer la integridad y/o salud física del operador y su entorno más próximo. En la actualidad, la aplicación de este tipo de dispositivos rebasa ampliamente los entornos industriales, pudiendo encontrarse en las soluciones más diversas, tanto a nivel de *infraestructura* (sistemas de señalización e iluminación, control de tráfico, control hidráulico y/o eléctrico, entre otros), como a nivel *doméstico* (sistemas de riego, automatización de apertura de puertas, domótica, etc.)

Según explica Djiev (2003), con el uso generalizado de computadoras y sus tecnologías asociadas, las redes de comunicaciones industriales se desarrollaron, o bien adoptaron, en base a

la transmisión de señales digitales. Las redes de comunicación propietarias de uso industrial comenzaron a utilizarse en la década de 1960, vinculando computadoras con sistemas de automatización. A mediados de 1970, *Honeywell* anunció el primer sistema de control distribuido por computadora (de sus siglas en inglés DCCS, *Distributed Computer Control System*), presentado como un sistema de control jerárquico con un gran número de microprocesadores; Este concepto se extendió ampliamente en varios sistemas de automatización industrial, tales como centrales eléctricas, líneas de manufactura, etc. La instalación de sistemas de control distribuidos en las nuevas plantas de producción, o bien la renovación de arquitecturas del tipo analógicas y/o centralizadas es, hoy por hoy, una decisión regular en las juntas directivas de las empresas (Djiev, 2003).

El uso de redes de área local (de sus siglas en inglés LAN, *Local Area Network*) para interconectar las computadoras y los dispositivos de automatización dentro de un sistema de automatización industrial se ha hecho popular desde 1980. La gran capacidad de comunicación y el bajo costo que ofrecen este tipo de redes han convertido en realidad el modelo de computación distribuida, y junto con ello, la automatización de varios servicios (Djiev, 2003).

Los sistemas de automatización industrial suelen implementarse utilizando una arquitectura distribuida y abierta, con comunicaciones basadas en redes digitales. A medida que dichos sistemas se amplían, incrementando el número de dispositivos interconectados, se ha vuelto más y más evidente la necesidad de contar con un estándar de comunicación, que permita integrar cada componente, independientemente de su tipo, finalidad o fabricante, de una manera común. Como ejemplo de dicha normalización, podemos citar el modelo OSI (del inglés *Open Systems Interconnection*, o interconexión de sistemas abiertos), que permite a un par de dispositivos comunicarse de manera fiable, independientemente de su fabricante (Djiev, 2003). El modelo de referencia en cuestión está representado en la Figura 4.

Figura 4

Modelo de referencia OSI

Por otro lado, al plantear las bases de este "*lenguaje común*", será necesario también considerar la diversidad de aplicaciones que una red de automatización utiliza: en determinadas aplicaciones, el tipo de dispositivo y su rendimiento podrían también definir el tipo de red a utilizar.

3.1.2 Definición

Según Djiev (2003), una red industrial podría definirse como una serie de sensores, elementos de medición y otros dispositivos de entrada y salida, geográficamente distribuidos, interconectados entre sí. Generalmente, las redes de este tipo transfieren bits de información de manera serial, utilizando un cableado sencillo para facilitar el intercambio de datos. Este tipo de medio también representa una gran ventaja al momento de añadir nuevos componentes al sistema, al utilizar todos los dispositivos la misma línea de comunicación. Cómo se planteaba en el párrafo anterior, para que los componentes de la red puedan entenderse entre sí, es necesario definir un conjunto de reglas que garanticen los parámetros de transmisión, seguridad y calidad de la información trasmitida

En el caso de caso de las redes de comunicación de bajo nivel (a nivel campo), las soluciones de red de área local del tipo MAP (del inglés *Media Access Protocol*) resultan demasiado ostentosas, además de no cumplir con los tiempos de respuesta requeridos. Este tipo de necesidades sentaron las bases para la creación de los buses de campo (del inglés *"field buses"*),

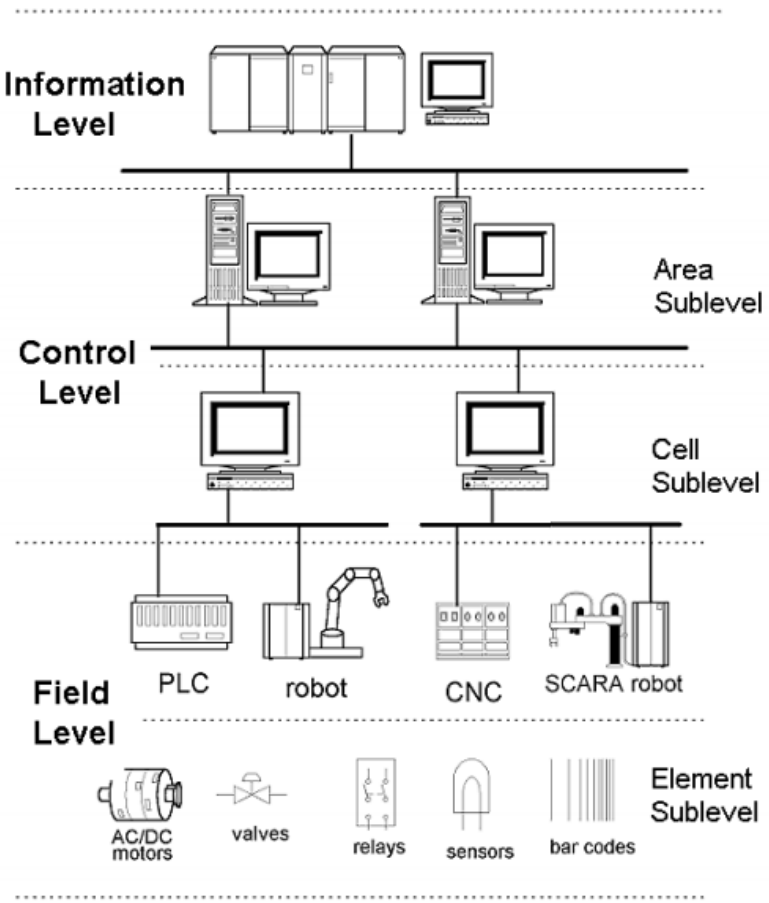
cuyo continuo desarrollo persigue la creación de un estándar para aplicaciones de automatización industrial (Djiev, 2003).

3.1.3 Niveles jerárquicos en un sistema de control industrial

Las redes industriales pueden ser clasificadas en diversas categorías en base a su funcionalidad y niveles de información. La figura número 5, obtenida de (Djiev, 2003) representa de manera gráfica las diferentes capas/niveles de un sistema de control industrial.

Figura 5

Niveles de un sistema de control industrial



Nota. Obtenido de *Industrial Networks for Communications and Controls, por Djiev, 2003*

a) Nivel 0 o *Nivel de Campo*: El nivel más bajo de la jerarquía de automatización es el nivel de campo, que incluye dispositivos tales como actuadores y sensores. La función principal de estos dispositivos consiste en transferir datos entre el producto manufacturado y el proceso de manufactura (Djiev, 2003). Los datos obtenidos pueden ser tanto binarios como analógicos, y pueden permanecer disponibles durante un período de tiempo determinado. Para la comunicación a nivel campo, se han utilizado varios tipos de conductores, siendo ampliamente adoptados aquellos del tipo paralelo y serial. Los estándares de comunicación seriales como RS232C, RS422 y RS485 son los protocolos más utilizados junto con el estándar de comunicación paralela IEEE488. Esos métodos de comunicación punto a punto han evolucionado hasta las redes de comunicaciones de tipo bus para hacer frente al costo del cableado y lograr una comunicación de alta calidad (Djiev, 2003).

   La lista de redes que conforman esta categoría es extensa, pudiendo distinguirse entre sí por características como el tamaño del mensaje y el tiempo de respuesta. En general, estas redes conectan dispositivos inteligentes que funcionan de manera cooperativa en una red distribuida y de misión crítica. Asimismo, las funcionalidades que ofrecen son relativamente acotadas, debido a su bajo costo y, por consiguiente, reducida capacidad de procesamiento (Djiev, 2003). En su forma más sofisticada, las redes de bus de campo trabajan con un esquema de control distribuido entre los dispositivos inteligentes como Foundation Fieldbus. Las redes comunes incluidas en las clases devicebus y fieldbus incluyen CANOpen, DeviceNet, Foundation Fieldbus, Interbus-S, LonWorks, Profibus-DP, y SDS.

   En la actualidad, el bus de campo se ha transformado en el estándar para la transferencia de información a nivel campo. Debido a los requisitos de tiempo, que deben ser estrictamente monitoreados en un proceso automatizado, las aplicaciones en los controladores de nivel de campo requieren funciones de transporte cíclico, que permitan transmitir la información a intervalos regulares. La representación de los datos debe ser lo más breve posible a fin de reducir el tiempo de transferencia de los mensajes en el bus (Djiev, 2003).

b) Nivel 1 o *Nivel de Control*: A nivel de control, el flujo de información consiste principalmente en la carga de programas, parámetros y datos. En un proceso productivo,

donde los tiempos de parada se reducen únicamente a intervalos breves y/o reajustes de las máquinas, la actualización de los parámetros de forma inmediata es crucial, siendo necesaria en algunos casos la carga de subrutinas durante los ciclos de producción. En base a este enfoque temporal, podríamos dividir las operaciones en dos subniveles: subniveles de célula y de área (Djiev, 2003).

a. Para las operaciones a nivel de célula, la sincronización de las máquinas y el manejo de eventos demandan respuestas en *tiempo real*. Este tipo de respuesta no podrá lograrse con la transferencia excesiva de programas y datos, siendo necesario adoptar algún tipo de segmentación en base al tamaño de los mensajes. A modo de cumplimentar los requerimientos de comunicación en este nivel, se han adoptado las redes de área local como medio de comunicación. Luego de la introducción de conceptos como CIM y DCCS, muchas empresas desarrollaron sus propias redes para el nivel celular de un sistema de automatización. La adopción del estándar ethernet junto con el protocolo TCP/IP fue aceptada casi de manera unánime como norma de facto para este nivel, aunque no es capaz de proporcionar una verdadera comunicación en tiempo real (Djiev, 2003).
b. El subnivel de área consiste en una o varias células combinadas en grupos. Las células están diseñadas con una funcionalidad orientada a la aplicación. Los controladores y/o operadores de este nivel llevan a cabo funciones de control e intervención, como el establecimiento de objetivos de producción, arranque y la parada de máquinas y actividades de emergencia (Djiev, 2003).

Las redes de control son generalmente utilizadas para enlaces peer-to-peer entre controladores lógicos programables, sistemas de control distribuido, interfaces humano-máquina (HMI), repositorios y control de supervisión. Los buses de control son utilizados para coordinar y sincronizar el control entre las unidades de producción y las células de fabricación (Djiev, 2003).

c) Nivel 2 o *Nivel de Supervisión*: En este nivel se albergan los distintos sistemas de control y supervisión. Para poder llevar a cabo la adecuada monitorización de los distintos procesos, se establece una comunicación entre estos sistemas y los elementos de supervisión del tipo interfaz humano-máquina, SCADA. En este nivel, el estándar de comunicación de facto es Ethernet TCP/IP (Djiev, 2003).

d) Nivel 3 o *Nivel de Gestión*: Este nivel se ubica en la cima de la pirámide y concentra la información de todos los niveles inferiores. Dicha información proporcionará a los directivos los indicadores para la correcta toma de decisiones. Análogamente, desde este nivel se enviarán órdenes a los niveles inferiores, a fin de implementar los cambios que el proceso de toma de decisiones considere necesarios (Djiev, 2003). La comunicación hacia los niveles inferiores no debe ser especialmente robusta ni rápida, pero debe soportar la transmisión de un gran volumen de datos. Por este motivo, se suelen emplear redes *Ethernet* estándar. En este nivel se albergan equipos de cómputo como ordenadores y servidores. ejecutando aplicaciones informáticas tales como ERP (Enterprise Resource Planning), MES (Manufacturing Execution Systems), CAD (Computer Aided Design), CAM (Computer Aided Manufacturing) y CAE (Computer Aided Engineering) (Djiev, 2003).

3.1.4 Métodos de transmisión

La transmisión de datos puede ser analógica o digital. Los datos analógicos toman valores que cambian continuamente, mientras que, en la comunicación digital, los datos sólo pueden tomar valores binarios (0 o 1). La transmisión en sí puede ser sincrónica o asincrónica, dependiendo de la forma en que se envíen los datos. En la transmisión en modo asíncrono, los caracteres se envían usando códigos de inicio y parada, y cada carácter puede ser enviado independientemente a una tasa no uniforme. La transmisión en modo sincrónico es un método más eficiente: los datos se transmiten en bloques de caracteres, y la hora exacta de salida y llegada de cada bit es predecible porque los relojes del emisor y del receptor están sincronizados (Djiev, 2003).

Los métodos de transmisión en las redes de comunicación industrial incluyen la banda base, banda ancha y la banda portadora. En una transmisión de banda base, el mensaje consiste en un conjunto de señales que se aplican al medio de transmisión sin ser traducidas en frecuencia. La transmisión de banda ancha utiliza una gama de frecuencias que puede dividirse en varios canales. La transmisión por portadora utiliza una sola frecuencia para transmitir y recibir información (Djiev, 2003).

La transmisión digital por fibra óptica se basa en la representación de pulsos digitales (ceros y unos) como pulsos de luz. El tipo de cableado físico o medio de transmisión es un factor importante a la hora de elegir una red de comunicación industrial concreta. El medio de transmisión

más común para este tipo de entornos es el cable de cobre, ya sea en forma de cable coaxial o de par trenzado. En la actualidad, es cada vez más habitual la utilización de fibra óptica y tecnologías inalámbricas aplicadas a los entornos industriales (Djiev, 2003).

El cable coaxial se utiliza para la transmisión de datos a alta velocidad a distancias de varios kilómetros. Se trata de un medio cuya disponibilidad en el mercado es alta, su costo de adquisición es insignificante y que, adicionalmente, su instalación y mantenimiento es relativamente sencilla. Es por ello que este tipo de medio es ampliamente utilizado en las redes de comunicación industriales (Djiev, 2003).

El par trenzado puede utilizarse para transmitir datos en banda base a varios Mbit/s en distancias de 1 km o más, pero a medida que aumenta la velocidad, se reduce la longitud máxima del cable. Este tipo de medio se ha utilizado durante muchos años, y su alcance también se extiende a los entornos de comunicación industriales. Su costo es aún menor que el del cable coaxial, pero no cuenta con una gran capacidad de transmisión, ni una buena protección (blindaje) contra las interferencias electromagnéticas (Djiev, 2003).

El cable de fibra óptica proporciona una capacidad de transmisión excepcional (Gigabit/s), y está libre de interferencias electromagnéticas. Sin embargo, el equipamiento asociado para implementar este tipo de medio implica una fuerte inversión inicial. Adicionalmente, si se utilizara para interconectar los sensores en el piso de producción, sería necesario también contar con un cableado independiente para la alimentación de los instrumentos, que también podría utilizarse para la transmisión de señales (ej. dispositivos tipo PoE) (Djiev, 2003).

En escenarios de alta movilidad y/o proyectos temporales, la utilización de tecnologías inalámbricas representa una buena alternativa, y su número de adeptos crece día a día.

En la actualidad, la interconexión de dispositivos discretos e instrumentos analógicos a través del cableado convencional (par trenzado) domina los sistemas de medición y automatización. Este tipo de medio junto con los estándares de instrumentación analógica 4-20 mA son compatibles con una amplia gama de dispositivos y fabricantes, proporcionando interoperabilidad entre los diversos componentes de la red industrial (Djiev, 2003).

Históricamente, las redes de medición y los sistemas de automatización han utilizado una combinación de redes digitales abiertas y propietarias para incrementar la disponibilidad de la información, y obtener un mayor rendimiento. La integración de dispositivos de proveedores diversos suele verse dificultada por la necesidad de interfaces personalizadas de software y

hardware. Por otro lado, las redes propietarias ofrecen interoperabilidad limitada entre fabricantes, limitando también el acceso a los dispositivos. En cambio, al utilizar redes industriales estándar, el usuario podrá determinar qué tipo de dispositivo es el más conveniente e implementarlo en base a sus características (Djiev, 2003).

3.1.5 Componentes de una red industrial

Los métodos y medios de transmisión citados en la sección anterior podrían aplicarse en cualquier tipo de entorno productivo. Teniendo en cuenta que la extensión de este tipo de ambientes es usualmente considerable, será necesario que el diseño que se adopte para nuestra red industrial cuente con una topología y un conjunto de componentes adecuados, que proporcionen el correcto aislamiento y desempeño de todo el conjunto (Djiev, 2003). En algunos casos (ej.: sitios productivos segregados en varias naves y/o localizaciones geográficas), será necesario incluir en la ecuación componentes adicionales, que permitan a los diversos interlocutores dialogar entre sí, independientemente de las distancias y/o tipo de red en que se encuentren hospedados. Se detalla a continuación los componentes básicos para este tipo de aplicaciones:

a) Repetidor (del inglés "*Repeater*"): Dispositivo que mejora ("amplifica") las señales eléctricas para extender la distancia entre los nodos. Este tipo de dispositivo trabaja a nivel físico (capa 1 del modelo OSI), permitiendo ampliar la cantidad de nodos en una red. Adicionalmente, facilita la convergencia entre diferentes medios físicos, tales como el cable coaxial, fibra óptica, par de cobre, etc. (Djiev, 2003).
b) Puente (del inglés "*Bridge*"): Dispositivo que facilita la conexión entre dos segmentos de una red, pudiendo contar con diferentes características eléctricas y protocolos. Este tipo de componente trabaja en la capa 2 del modelo OSI (enlace de datos) y actúa separando los dominios de colisión en redes del tipo ethernet (Djiev, 2003).
c) Enrutador (del inglés "*Router*"): Dispositivo que intercambia los paquetes entre diferentes segmentos de red, definiendo una ruta específica. Este tipo de equipo opera en la capa 3 del modelo OSI (red) (Djiev, 2003).
d) Punto de Acceso (del inglés "*Access Point*"): Este tipo de dispositivo podría considerarse como el punto de enlace entre las redes inalámbricas y cableadas. Su función principal es permitir la conectividad con la red, delegando las tareas de enrutamiento y direccionamiento a otros componentes tales como puentes y enrutadores. Se trata de un

dispositivo de capa 2, y por lo tanto opera sobre las capas 1 y 2 del modelo OSI (Djiev, 2003).

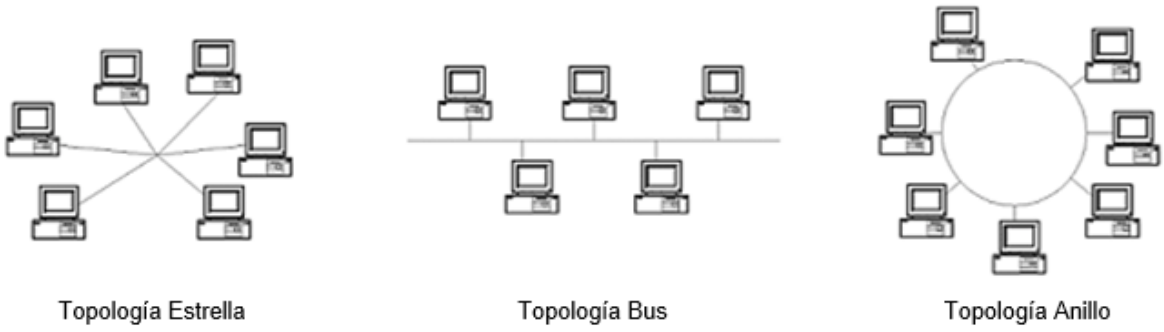
e) Puerta de Enlace (del inglés "*Gateway*"): El funcionamiento de un Gateway es similar al de un puente, proporcionando interoperabilidad entre buses de diferentes tipos y protocolos. Una pasarela permite unir dos redes disímiles, facilitando el intercambio de información entre las aplicaciones a través de ella (Djiev, 2003).

3.1.6 Topologías de red

Continuando con el enfoque aplicado en las secciones previas, la extensión y/o ampliación de las redes industriales deberá ser cuidadosamente planificada y ejecutada. A medida que los sistemas industriales incrementan su extensión y, por consiguiente, su cantidad de dispositivos interconectados, se debe considerar la correcta selección e implementación de una *topología de red*. Las topologías de red más comunes en son el *bus*, la *estrella*, o bien una red híbrida que combine ambas topologías. En las aplicaciones industriales, es habitual el uso de tres topologías: *estrella*, *bus* y *anillo*. La figura número 5, obtenida de (Djiev, 2003) representa gráficamente las topologías en cuestión:

Figura 6

Topologías de red



Nota. Obtenido de *Industrial Networks for Communications and Controls, por Djiev, 2003*

a) Topología *Estrella*: Consiste básicamente en un controlador central, al que se conectan todos los nodos; Esto representa una gran ventaja en el caso de las redes pequeñas, pero podrían requerirse controladores adicionales al alcanzar un número determinado de nodos.

Asimismo, el fallo de un nodo en este tipo de configuración no afectará al resto de los nodos, permitiendo añadir o quitar nodos a voluntad sin impactar la operación de la red. Como contrapunto, es necesario citar que un fallo en el concentrador central podría interrumpir la operación total de la red (SPOF, punto de falla único) (Djiev, 2003)

b) Topología *Bus*: En este tipo de configuración, cada nodo se encuentra conectado a un canal de comunicación común. Los mensajes transmitidos son recibidos por cada uno de los nodos. El fallo de un nodo no implica ningún tipo de impacto para la operación del resto, a menos que la falla interrumpa también el medio de transmisión (Djiev, 2003).
c) Topología *Anillo*: En este tipo de configuración, el medio de trasmisión se presenta en forma de bucle, y los nodos se conectan a intervalos alrededor de dicho anillo. Los mensajes se transmiten a través del anillo, pasando a través de cada nodo; Si un nodo falla, toda la red podría detenerse a menos que se implemente algún mecanismo de recuperación (Djiev, 2003).

La mayoría de las redes industriales están basadas en topologías híbridas, combinando los esquemas de bus y estrella, que permiten incrementar su tamaño y soportar cientos de nodos conectados. La implementación de este esquema hibrido permite integrar tecnologías populares como Ethernet, Foundation Fieldbus, DeviceNet, Profibus y CAN independientemente de los requisitos de las aplicaciones (Djiev, 2003).

Criptosistemas

Tal como lo indica Zwicke (2003), definimos un criptosistema como una combinación compleja de hardware y software, cuya finalidad principal es transformar mensajes de texto plano en una serie de caracteres ininteligibles, conocidos como texto cifrado, para que luego puedan volver a su formato original (texto plano). Un algoritmo de encriptación codifica los datos combinando los bits de la clave con los bits de los datos; Inversamente, el proceso de desencriptación descifra los datos separando los bits de datos de los bits de la clave. La encriptación es la base de la comunicación electrónica segura, pero no garantiza que un mensaje permanezca completamente seguro. La autenticidad e integridad de un mensaje cifrado requiere el uso de firmas digitales y hashes unidireccionales (Zwicke, 2003).

Los dos tipos de criptosistemas empleados en la actualidad (simétricos y asimétricos), se basan en el uso responsable de las claves y en las buenas prácticas de gestión para preservar su seguridad. Uno de los métodos más utilizados por los atacantes para intentar descifrar un mensaje privado consiste en obtener una copia de la clave utilizada para cifrarlo, debido a que la fortaleza de los de los criptosistemas modernos hace que la ruptura del código sea inviable desde el punto de vista computacional. Adicionalmente, es necesario destacar que la fuerza de un sistema criptográfico suele ser igual a su eslabón más débil. Ningún aspecto del diseño del sistema puede ser descuidado, desde la elección de los algoritmos hasta la distribución de claves y las políticas de uso (Zwicke, 2003).

3.1.7 Definición

Matemáticamente, un criptosistema puede definirse como una quíntupla (*M, C, K, E, D*), donde:

a) *M* representa el grupo de mensajes sin cifrar (texto plano) que pueden ser enviados.
b) *C* representa el conjunto de los posibles mensajes cifrados, o *criptogramas*.
c) *K* representa el conjunto de claves que pueden ser empleados en el criptograma.
d) *E* es el conjunto de *transformaciones de cifrado* o familia de funciones aplicables a cada elemento *M* para obtener como resultado un elemento *C*. Existe una transformación diferente E_k para cada valor posible de la clave *k*.
e) *D* es el conjunto de *transformaciones de cifrado*, análogo a *E*.

Considerando lo citado previamente, es posible afirmar que todo criptosistema debe cumplir con la siguiente condición:

$$D_k\,(E_k\,(m)) = m$$

es decir, si se parte de la base de un mensaje *m*, lo ciframos utilizando la clave *k*, y luego lo desciframos empleando la misma clave, se obtiene como resultado el mensaje original *m* (Rodriguez Penin, 2013)

3.1.8 Criptosistemas simétricos

Los criptosistemas de clave simétrica, o de *clave privada*, se basan en la misma clave para cifrar y descifrar el texto sin formato (que representa el mensaje o parte de los datos que se están codificando). El proceso de cifrado consiste básicamente en ejecutar un texto plano (*entrada*) a través de un algoritmo de encriptación determinado, que arrojará como resultado un texto cifrado (*salida*) (Rountree, 2011).

Al utilizar la misma clave tanto para cifrar como para descifrar los mensajes, es extremadamente importante asegurarse de que la integridad de esta no se vea comprometida. Tal como lo indica Zwicke (2003), la longitud de las claves utilizadas por los distintos sistemas varía dependiendo del tipo de solución aplicada. Los criptosistemas simétricos encriptan los datos en flujos, bit a bit, o en forma de bloque, agrupándolos en conjuntos de tamaño predeterminado (ej. el texto simple de 128 bits se cifra en el texto cifrado de 128 bits). Los sistemas de clave simétrica suelen utilizar longitudes de clave cortas (a mayor longitud de clave, mayor dificultad para descifrarla), proporcionando un desempeño fluido en la manipulación de los datos, y una gran rapidez en comparación con los sistemas de clave asimétrica. Las claves con una longitud de 256 bits se consideran altamente seguras, y en el plano teórico, podrían resistir sin inconvenientes un ataque de fuerza bruta a cargo de una computadora cuántica.

En la actualidad pueden encontrarse cientos de algoritmos de clave simétrica; Cada uno de ellos posee un conjunto propio de fortalezas y debilidades. A continuación, se proporcionará una breve descripción de los sistemas mayor renombre.

3.1.8.1 DES (Data Encryption Standard)

El *Estándar de Cifrado de Datos* fue desarrollado originalmente en los Estados Unidos a finales de los años ’70 como una iniciativa conjunta entre la NBS y la NSA (Zwicke, 2003). El objetivo principal del proyecto fue proporcionar un método estandarizado para proteger datos comerciales sensibles e información no clasificada, siendo ampliamente adoptado por las entidades gubernamentales, y convirtiéndose en un estándar federal en noviembre de 1976

En la actualidad, DES ya no considerado como un algoritmo seguro debido a que la potencia computacional permitiría que sea vulnerado en cuestión de horas o días. En su lugar, el algoritmo 3DES fue adoptado como solución estándar, considerándose altamente seguro aún en los tiempos que corren.

3.1.8.2 3DES (Triple DES)

El sistema *Triple DES* obtiene su nombre al aplicar el algoritmo *DES* tres veces a cada bloque de datos. Como se indica en el párrafo anterior, *3DES* fue desarrollado debido a la preocupación de los diversos organismos acerca de la debilidad de su predecesor, consolidándose como la solución de cifrado estándar en la actualidad (Zwicke, 2003).

Desde la perspectiva técnica, *3DES* opera básicamente en dos modos: *Triple ECB,* donde los mensajes se dividen en bloques y cada uno de ellos es cifrado por separado utilizando la misma clave $_k$. Si bien este modo es el más utilizado por su sencillez, el modo alternativo *Triple CBC* proporciona una capa adicional de seguridad (Zwicke, 2003).

El algoritmo *3DES* permite especificar una clave para cada una de las iteraciones de encriptación DES; Aunque es posible utilizar la misma clave en todas las iteraciones, la implementación es más segura utilizando una clave diferente en cada oportunidad. Si se utiliza la misma clave para las tres iteraciones, se considera que la fortaleza de la clave es de *56 bits* (al igual que *DES*). Por otro lado, si se utiliza la misma clave en dos iteraciones, y una clave diferente en la tercera, se considera que la fortaleza de la llave es de *112 bits*. Por último, si se utiliza una clave diferente para cada una de las iteraciones, se considera que la fortaleza del cifrado es de *168 bits* (Zwicke, 2003).

3.1.8.3 AES (Advanced Encryption Standard)

El *Estándar de Cifrado Avanzado* (también conocido como algoritmo *Rijndael*, pronunciado "*Rain Doll*" en inglés) fue desarrollado en Bélgica por los criptólogos *Joan Daemen* y *Vincent Rijmen*. Fue adoptado por el *Instituto Nacional de Estándares y Tecnología* como FIPS en 2001 luego de un proceso de estandarización que duró 5 años (Zwicke, 2003).

Desde la perspectiva técnica, el funcionamiento del sistema puede parecer complejo, pero en realidad es sencillo de entender: el algoritmo abarca tres tipos de cifrados de bloque: *AES-128*, *AES-192* y *AES-256*, representando los números la longitud en bits de la clave de cifrado (Zwicke, 2003).

En la actualidad, el algoritmo es ampliamente utilizado debido a que su funcionamiento es relativamente fácil de entender; Esto permite una fácil implementación, proporcionando además una gran rapidez en las operaciones de cifrado y descifrado. Por otro lado, los escasos requisitos

de memoria para su ejecución lo hacen muy adecuado para entornos con limitaciones, en los que también demuestra un excelente rendimiento. Por último, cuando alguna implementación requiera una capa extra de seguridad, *AES* puede combinarse con varios protocolos de seguridad como *WPA2*, o incluso otros tipos de cifrado como *SSL* (Zwicke, 2003).

3.1.8.4 IDEA (International Data Encryption Algorithm)

El *Algoritmo Internacional de Cifrado de Datos* fue concebido originalmente para sustituir al sistema DES. El sistema opera en bloques de 64-bits, y utiliza claves de cifrado de 128-bits de longitud. Sobre su adopción, si bien fue utilizado como sistema de cifrado en las primeras versiones de PGP (*PGP v2.0*), existen dos razones por las cuales su aplicación se ve restringida: el sistema está sujeto a una serie de claves débiles y, por otro lado, existen actualmente algoritmos más rápidos que producen el mismo nivel de seguridad (Zwicke, 2003).

3.1.8.5 RC4 (Cifrado de Rivest, 4ta versión)

El algoritmo *RC4* fue diseñado por *Ron Rivest* en 1987 para la compañía *RSA Data Security*. Su implementación es extremadamente sencilla y rápida: el sistema utiliza una clave de cifrado de longitud variable, que oscila entre 40 y 256-bits, aunque el tamaño de clave utilizado habitualmente es 128-bits (Zwicke, 2003).
RC4 ha sido uno de los algoritmos con mayor adopción a nivel mundial, utilizado para proteger el acceso en redes inalámbricas *WEP*/*WPA*, así como en *Secure Sockets Layer* (SSL*)* y *Transport Layer Security* (TLS) sobre el protocolo *Hypertext Transfer Protocol over SSL* (HTTPS*)*. Se trata de un algoritmo propietario y requiere de una licencia para su implementación (Zwicke, 2003).

3.1.8.6 RC5 (Cifrado de Rivest, 5ta versión)

RC5 se presenta como una evolución del algoritmo *RC4*. Incorpora parametrización con tamaño de bloques variable, tamaño de claves y número de rondas variables. Las opciones permitidas para el tamaño de bloque son 32 bits (únicamente con fines experimentales), 64 bits (para usar un reemplazo de DES) y 128 bits. El número de rondas puede ir de 0 a 255, mientras que el tamaño de la clave oscila entre 0 y 2040 bits. RC5 cuenta con tres rutinas: *expansión de la clave*, *cifrado y descifrado* (Rountree, 2011).

La tabla 1 detalla la longitud de las claves y tamaños de bloque con los que opera cada uno de los algoritmos citados:

Tabla 1

Algoritmos de Cifrado Simétricos

	Longitud de Clave	***Tamaño de Bloque***
DES	56 bits	64 bits
3DES	56, 112 o 168 bits	64 bits
AES	128, 192 o 256 bits	128 bits
IDEA	128 bits	64 bits
RC4	40 a 256 bits	Cifrado en flujo
RC5	0 a 2040 bits (128 bits recom.)	32, 64 o 128 bits (64 recom.)

Nota. Adaptado de Security for Microsoft Windows Administrators, Rountree, 2011

Criptosistemas asimétricos

Los sistemas criptográficos de clave asimétrica, comúnmente conocidos como criptosistemas de *clave pública*, emplean un par de claves en lugar de una clave única, tal como en los esquemas simétricos. Una de las claves puede divulgarse (*clave pública*), mientras que la otra debe mantenerse en secreto (*clave privada*) (St Denis, 2007).

El uso de dos claves en lugar de una produce también una variedad de diferencias funcionales entre el cifrado simétrico y el asimétrico. La complejidad de los algoritmos asimétricos los hace más lentos que los simétricos, es por ello que suelen utilizarse sólo para el intercambio inicial de claves; Al producirse dicho intercambio, la encriptación suele realizarse de forma simétrica. Dado que las claves públicas y privadas utilizadas en el cifrado asimétrico están matemáticamente relacionadas en algún grado, estas claves deben ser significativamente más largas para alcanzar un nivel de seguridad comparable al que proporcionan las claves simétricas más cortas (St Denis, 2007).

Asimismo, los algoritmos asimétricos se utilizan principalmente para resolver dos inconvenientes que los de clave simétrica no consiguen: la distribución de claves y el no repudio.

El primero ayuda a resolver problemas de privacidad, mientras que el segundo se enfoca en los problemas de autenticidad (St Denis, 2007).

El uso del cifrado de clave asimétrica y de los resúmenes de mensajes constituyen la base de la seguridad en las comunicaciones actuales de Internet. Las funciones de seguridad básicas que un sistema criptográfico debe ofrecer podrían resumirse en los siguientes conceptos:

a) Privacidad: Consiste en proteger la información de la divulgación no deseada y/o no autorizada. La privacidad se consigue encriptando la información con la clave pública del destinatario. Sólo puede descifrarse con la clave privada del destinatario y nadie más puede leer el mensaje cifrado (SafeNet, 2010).
b) Identidad: Es la capacidad de identificar inequívocamente al remitente de un mensaje. Dado que sólo la clave pública correspondiente a la clave privada del remitente puede descifrar su firma, la identidad del remitente puede garantizarse. En una PKI, los certificados de clave pública suelen utilizarse para la identidad (SafeNet, 2010).
c) Integridad: Consiste en proteger la información de modificaciones no deseadas y/o no autorizadas. Las funciones de *hash* permiten al receptor del mensaje verificar que el contenido no ha sido alterado durante la transmisión (SafeNet, 2010).

Por otro lado, existen funciones de seguridad adicionales, derivadas de las funciones básicas citadas en el párrafo anterior:

a) Autenticación: Consiste básicamente en la capacidad de demostrar una identidad declarada. La autenticación se consigue mediante una firma digital. Al verificar la firma de un mensaje, el destinatario puede estar seguro de la identidad del remitente (SafeNet, 2010).
b) Control de Acceso: Utilizando sus pilares la autenticación y la identidad, el control de acceso establece el acceso de una entidad ("quién") puede acceder a un determinado recurso ("qué"). Los controles de acceso pueden ser simples (ej: encriptación de archivos), o bien complejos como el uso de tarjetas inteligentes (del inglés "*SmartCards*") que contengan una clave privada utilizada para procesar un inicio de sesión a través de PKI (SafeNet, 2010)
c) No Repudio: Con la introducción de las técnicas de no repudio, una entidad no puede

> negar haber cometido una acción. La firma de una persona en un contrato es la prueba univoca de que ha aceptado sus condiciones. Si esa persona lo negara (repudiara) más tarde, el titular del contrato podría señalar la firma como prueba. En el mundo digital, la firma digital funciona de forma muy parecida: la naturaleza secreta de la clave privada significa que sólo una persona puede haber firmado el documento electrónico que contiene dicha firma electrónica (SafeNet, 2010).

Hoy en día, existe una amplia variedad de algoritmos asimétricos disponibles, pero la mayoría de ellos son inseguros o poco prácticos. Algunos resultan ineficaces porque el criptograma generado es significativamente mayor que el mensaje original, mientras que otros tienen claves extremadamente largas (Lucena López, 2011). A continuación, proporcionaremos una breve clasificación que incluye a los sistemas asimétricos de mayor adopción.

3.1.8.7 Diffie-Hellman

Se trata de una de las primeras soluciones de mayor adopción para el intercambio de claves de manera segura, a través de un canal inseguro. No fue hasta el año 1976 en que los algoritmos de clave pública hicieron su aparición en el campo, cuando *Whitfield Diffie* y *Martin Hellman* publicaron su artículo titulado "*New Directions in Cryptography*". En este trabajo colaborativo se describían los mecanismos de una innovadora solución, que posteriormente se conocería como el sistema de intercambio de claves *Diffie-Hellman.*

El propósito del intercambio de claves Diffie-Hellman es generar de manera segura claves compartidas que puedan usarse posteriormente para derivar otras claves adicionales; Estas claves se utilizarán posteriormente en *algoritmos simétricos* para asegurar la información. Como mencionamos en párrafos anteriores, los algoritmos simétricos tienden a utilizarse para el cifrado de grandes volúmenes de datos debido a su eficacia en comparación con los algoritmos de clave pública.

Técnicamente, este sistema puede utilizarse para establecer tanto claves públicas como privadas. Sin embargo, en la práctica se tiende a utilizar RSA en su lugar. Esto se debe a que el algoritmo RSA también es capaz de firmar certificados de clave pública, mientras que el intercambio de claves Diffie-Hellman no lo es.

3.1.8.8 RSA (Rivest Shamir Adelman Algorithm)

Tal como lo indica Manuel Lucena Lopez (2011), el algoritmo RSA es quizá el sistema más sencillo de comprender e implementar. Dicho algoritmo debe su nombre a sus inventores: Ronald Rivest, Adi Shamir y Leonard Adleman, quiénes mantuvieron su licencia hasta setiembre de 2000, por lo que la utilización comercial del producto estuvo restringida hasta esa fecha. En línea con este punto, es necesario destacar que las primeras versiones del sistema PGP incorporaban el algoritmo RSA como método de cifrado y firma digital, siendo desaconsejado su uso a partir de la versión 5, y en favor de otros algoritmos que contaban con licenciamiento libre.

El principio de funcionamiento de RSA está basado en la dificultad para factorizar números grandes. Tanto la clave pública como la privada son calculadas a partir de un número que se obtiene como producto de dos números primos grandes. El atacante se enfrentará, si quiere recuperar un texto claro a partir del criptograma y la clave pública, a un problema de factorización, o bien tendrá que resolver un logaritmo discreto (Lucena López, 2011, pág. 182).

El sistema RSA fue incorporado en una gran variedad de productos, plataformas e industrias, siendo integrado inclusive en varios sistemas operativos de Microsoft, Apple, Sun y Novell. Como contrapunto, vale la pena mencionar que se trata de un sistema considerablemente lento en aplicaciones de software, y al menos 1000 veces más lento que algoritmos simétricos como DES o AES al aplicarse en soluciones de hardware (Zwicke, 2003).

3.1.8.9 Curvas Elípticas

Las curvas elípticas constituyen un formalismo matemático conocido y estudiado desde hace más de 150 años, y presentan una serie de propiedades que da lugar a problemas análogos a los que presentaba la aritmética modular, lo cual las hace válidas para aplicar algunos de los algoritmos asimétricos más conocidos (Lucena López, 2011, pág. 93).

A alto nivel, son análogos a los criptosistemas de clave pública existentes en los cuales la aritmética modular se sustituye por operaciones definidas sobre curvas elípticas. Sobre su aplicación, si bien se trata de un sistema cuya utilización no es demasiado extendida, cuenta con una comunidad de soporte creciente. Los bajos recursos requeridos para su aplicación lo convierten en una solución atractiva para aquellas organizaciones que cuenten con una capacidad de procesamiento limitada (Zwicke, 2003).

3.1.8.10 Certificados Digitales

Un certificado digital es esencialmente una clave pública y un identificador, firmados digitalmente por una *autoridad de certificación* (en adelante, CA), cuya utilidad es demostrar que una clave pública pertenece a un usuario concreto. Dicha autoridad
de certificación debe encargarse de verificar previamente la autenticidad de la clave pública. (Lucena López, 2011, pág. 232).
Considerando que la implementación y el uso de los certificados digitales componen el contenido nuclear de esta propuesta, este tema será abordado con mayor profundidad en las secciones subsiguientes.

3.1.9 Consideraciones clave en la elección de un criptosistema

De acuerdo con lo expuesto en párrafos anteriores, existen un centenar de soluciones de criptografía para aquellas organizaciones y/o proyectos que requieran establecer flujos de comunicación seguros a través de medios que no lo son. Al elegir una solución que se adapte a las necesidades particulares de nuestro proyecto y/o aplicación, será de vital importancia considerar tanto las bondades como los puntos débiles de cada una de las soluciones. A continuación, se detallan algunos criterios para evaluar de manera adecuada la solución a implementar:

Rendimiento: Este parámetro suele variar en base a muchos factores. La longitud de las claves utilizadas influirá directamente en la velocidad del sistema; A mayor longitud de clave, mayor será el tiempo de procesamiento, incrementándose también la cantidad de recursos de cómputo requeridos. Asimismo, la elección del método de cifrado (cifrado en bloque, o bien en flujo) se trata de un factor que deberá someterse a un riguroso análisis. Por último, la complejidad del algoritmo de cifrado, y la cantidad de operaciones que requiera para su ejecución son parámetros que podrían impactar el rendimiento global del sistema.

Manejo de Claves: Como se menciona anteriormente, los criptosistemas simétricos ofrecen un rendimiento superior respecto a los asimétricos, pero requieren de un mecanismo seguro para el intercambio de las claves secretas (ej. *Diffie-Hellman* o *RC4/RC5*). Por otro lado, los sistemas

asimétricos no cuentan con limitaciones de este tipo, pero ofrecen un rendimiento considerablemente menor debido a su grado de complejidad.

Tipos de Datos: La sensibilidad de los datos que deben protegerse es uno de los factores determinantes al seleccionar un criptosistema.

Acceso a la Información: Es fundamental definir el número aproximado de usuarios y/o dispositivos que utilizarán la solución, así como su ubicación y frecuencia de uso.

Aceptación de la Comunidad: Sin dudas, una de las consideraciones más importantes a la hora de seleccionar un criptosistema es su nivel de aceptación dentro de la comunidad de ciberseguridad. Es fundamental que la solución elegida haya sido aplicada en soluciones reales, generando casos de éxito que permitan comprobar su funcionamiento por parte de los miembros de la comunidad.

Fortaleza del algoritmo: Es recomendable optar por un algoritmo potente. Utilizar una solución poco compleja en la actualidad, donde la capacidad de procesamiento crece exponencialmente minuto a minuto, conlleva riesgos que no vale la pena correr.

Costo: Como en cualquier proyecto tecnológico, es necesario considerar el costo de la solución en línea con los beneficios que traiga aparejados. Es importante destacar que el nivel de criticidad de la información a proteger debe estar en línea con la inversión requerida. En algunos casos, el tipo de información a resguardar podría no justificar la compra de un criptosistema que proporcione múltiples tipos de cifrado y claves de extensión astronómica.

3.2 Infraestructuras de Clave Pública (PKI)

3.2.1 Introducción

Las infraestructuras de clave pública o PKI (del inglés "*Public Key Infrastructures*") juegan un papel clave al permitir acelerar y simplificar la entrega de productos y servicios, proporcionando un marco electrónico a procesos que históricamente se han basado en la utilización de papel (Kuhn, 2001). Este tipo de arquitectura se ha convertido en un componente vital del abanico de soluciones de seguridad modernas, permitiendo garantizar la *confidencialidad*, la

integridad, la *autenticidad* y el *no repudio* de la información sensible. Basada en los esquemas de la criptografía asimétrica y las estructuras jerárquicas, PKI representa una potente herramienta que permite establecer canales de comunicación seguros entre grandes grupos de usuarios y nodos informáticos.

El principio de funcionamiento en el que se basa es bastante sencillo: un mensaje -o *certificado*- se cifra o firma con una clave privada y puede descifrarse o verificarse con la correspondiente clave pública; La entidad de origen podrá entonces firmar digitalmente un documento, permitiéndole al destinatario verificar su procedencia, comprobando también que no ha sido modificado sin el consentimiento de la entidad emisora.

Como en todo proyecto tecnológico, el despliegue de la arquitectura PKI en una organización requiere de una cuidadosa planificación, sumado a un profundo entendimiento de las tecnologías y/o componentes existentes en el entorno de aplicación.

En los párrafos subsiguientes, se presenta una visión generalizada sobre los componentes principales de la arquitectura, métodos de operación e implementación. Asimismo, se detallan los beneficios que esta arquitectura ofrece, así como las limitaciones y puntos de mejora que trae aparejados.

3.2.2 Definición

Las arquitecturas de seguridad modernas tienen entre sus objetivos la correcta protección y transferencia de la información en entornos distribuidos, independientemente de la ubicación física y espacio temporal en que se encuentren las entidades y/o recursos involucrados. Partiendo de este escenario, es posible afirmar que las PKI se han convertido en el principal mecanismo de seguridad, pudiendo encontrarse en innumerables aplicaciones, desde cifrado de correos electrónicos hasta operaciones bancarias en línea (Kuhn, 2001).

El término infraestructura de clave pública deriva de criptografía de clave pública, la tecnología en la que se basan las PKI. La criptografía de clave pública es la tecnología en la que se basan las técnicas modernas de firma digital.

De manera genérica, las PKI podrían definirse como una combinación de políticas, procedimientos y tecnologías necesarios para gestionar los *certificados digitales* en un esquema criptográfico de clave pública. Esta arquitectura vincula una clave pública con una entidad en particular,

permitiéndole a las otras entidades comprobar dicha relación, proporcionando además los servicios necesarios para la gestión de claves en entornos distribuidos (Kuhn, 2001).

Las PKI proporcionan un marco de seguridad que garantiza el cumplimiento de las siguientes condiciones:

a) Que la entidad y/o proceso identificado como emisor sea realmente quién origina la transacción.
b) Que el receptor de la transacción sea el destinatario previsto.
c) Que la integridad de los datos no haya sido comprometida en el proceso.

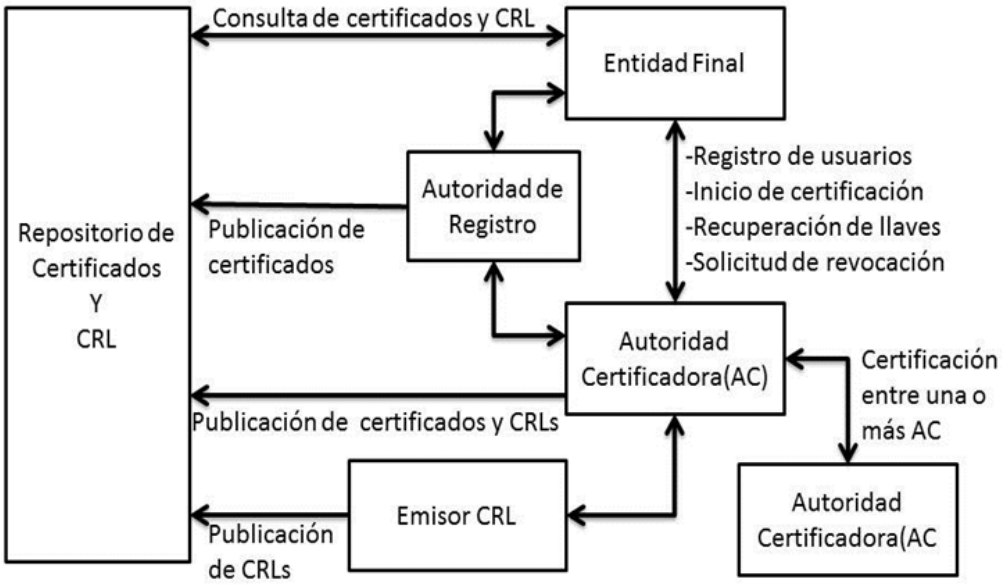
Un ejemplo de aplicación de PKI en una organización típica abarca la emisión de certificados digitales a las entidades intervinientes (usuarios, servidores, dispositivos inteligentes, etc.); software para llevar a cabo el enrolamiento de dichas entidades, integración con los directorios de certificados, y un conjunto de herramientas y servicios que permiten gestionar de forma ordenada los procesos de renovación y revocación de certificados (Kuhn, 2001).

3.2.3 Componentes de la arquitectura

Una infraestructura de clave pública está compuesta básicamente por tres elementos: los certificados digitales, una autoridad de certificación, y una autoridad de registro (Kuhn, 2001). Debido al marco particular sobre el cual se desarrolla este trabajo, se sugiere la incorporación de un cuarto componente, denominado como Módulo de Seguridad de Hardware (HSM), con el propósito de reforzar los procedimientos de encriptación/desencriptación y el correcto manejo de claves. La Figura 7 representa los componentes de una PKI y sus flujos de operación básicos:

Figura 7

Componentes de una infraestructura de clave pública



Nota. Obtenido de *Infraestructura de Firma Digital de la República Argentina,* Secretaría de Modernización Administrativa, 2016.

Al alojar estos elementos en un entorno seguro, una PKI podrá garantizar la autenticidad de las entidades, así como resguardar los parámetros críticos que requieran operaciones de seguridad digital, tales como inicios de sesión con tarjetas inteligentes, firmas SSL, documentos cifrados, etc.

Cada uno de los componentes citados será desarrollado en las secciones subsiguientes.

3.2.3.1 Certificados Digitales

Como se indicó a modo de introducción en párrafos anteriores, un certificado digital es esencialmente un conjunto compuesto por una clave pública y un identificador, firmados digitalmente por una autoridad de certificación, cuya utilidad es demostrar que una clave pública pertenece a un usuario concreto. Un certificado podría compararse con un documento oficial o un pasaporte.

Un certificado emitido por una autoridad de certificación (CA) garantiza que una clave pública pertenece realmente a una persona, grupo o empresa que afirma ser el/la propietario/a de la clave. Para ello, la información necesaria para identificar al titular de la clave pública se registra en el certificado. Una vez verificada la identidad a través de la autoridad de registro (RA), el

certificado es firmado por dicha CA, garantizando así la identidad. La CA firma el certificado en cuestión con su propia clave privada.

Los certificados pueden ser emitidos para diversas entidades (personas, grupos, empresas o servidores). Por lo tanto, se habla de certificados personales, de grupo, de empresa o de servidor. La emisión de los certificados es llevada a cabo a través de plataformas de software, siendo los del tipo PGP y X.509 los más utilizados. (Gbs, 2016, pág. 4)

Certificados X.509

El *Comité Consultivo Internacional Telegráfico y Telefónico* (CCITT) junto con la *Organización Internacional de Normalización* (ISO) trabajaron en la elaboración de un marco que permitiera estandarizar el tratamiento de los certificados digitales. El resultado de dicha colaboración fue la creación del *Directory Authentication Framework* (CITT509), también llamado protocolo *X.509* (Gbs, 2016, pág. 6). Si bien el estándar surgió originalmente en el año 1988, la última versión vigente, *X.509 v3*, se aprobó en 2008.

La principal razón para establecer este marco normativo es precisamente la implementación de una infraestructura de clave pública (PKI). Este aspecto es crítico, y establece una clara diferencia entre una clave criptográfica y un certificado digital. Las claves definidas por RSA son simplemente secuencias para cifrar y descifrar información. En contraste, el estándar X.509 define parámetros para identificar al propietario del certificado, al emisor (la autoridad de certificación), así como su fecha de emisión y caducidad, entre otros detalles. (Cutanda, 2014). El protocolo X.509 ha sido adoptado por entidades como ANSI e ISO, e implementado como estándar a nivel mundial (Gbs, 2016).

Tal como lo indica la Secretaría de Modernización Administrativa (2016), los elementos que componen un certificado tipo X.509 v3 son los siguientes:

a) Versión: El campo *version* describe la versión del certificado. Los valores aceptables son 1, 2 y 3.
b) Número de Serie: El campo *serialNumber* contiene un número asignado por el certificador a cada certificado. Este parámetro debe ser único para cada certificado emitido por cada CA del certificador.

c) Algoritmo de Firma: El campo *signature* debe contener el identificador de objeto (OID) del algoritmo y, si fueran necesarios, los parámetros asociados usados por el certificador para firmar el certificado. Este identificador debe ser alguno de los definidos en el [RFC4055] para RSA, [RFC5480] para curvas elípticas o [RFC5758] para DSA y ECDSA.

d) Nombre Distintivo del Emisor: El campo *issuer* debe identificar a la organización responsable de la emisión del certificado, mediante la utilización de un subconjunto de los siguientes atributos:

- Componente de dominio (OID 0.9.2342.19200300.100.1.25: *domainComponent*)
- Código de país (OID 2.5.4.6: countryName)
- Nombre de la organización (OID 2.5.4.10: *organizationName*)
- Nombre de la provincia (OID 2.5.4.8: *stateOrProvinceName*)
- Nombre de la localidad (OID 2.5.4.7: *localityName*)
- Número de serie (OID 2.5.4.5: s*erialNumber*)
- Nombre común (OID 2.5.4.3: *commonName*)

e) Validez (Desde, Hasta) (*validity* (*notBefore*, *notAfter*)): El período de la validez del certificado es el intervalo de tiempo durante el cual el suscriptor se encuentra habilitado para utilizarlo.

El campo se representa como una secuencia de dos fechas:

- *notBefore*: fecha en que el período de validez del certificado comienza.
- *notAfte*r: fecha en que el período de validez del certificado termina.

El período de validez de un certificado es el período de tiempo de "*notBefore*" a "*notAfter*" inclusive. Adicionalmente, es necesario recalcar que un certificador no debe emitir un certificado digital con vencimiento posterior al de su propio certificado.

f) Nombre Distintivo del Suscriptor: El campo *subject* identifica la entidad asociada a la clave pública guardada en el campo *subjectPublicKeyInfo*. Debe contener un nombre distintivo del suscriptor. Dicho nombre debe ser único para cada suscriptor de certificado emitido por un certificador durante todo el tiempo de vida de este.

La identidad del suscriptor debe quedar especificada utilizando los siguientes atributos:

- Código de país (OID 2.5.4.6: *countryName*)
- Nombre común (OID 2.5.4.3: *commonName*)
- Número de serie (OID 2.5.4.5: *serialNumber*)

g) Clave Pública del Suscriptor: El campo *subjectPublicKeyInfo* se utiliza para transportar la clave pública y para identificar el algoritmo con el cual se utiliza la clave. El identificador utilizado debe ser alguno de los definidos en [RFC4055] para RSA, [RFC5480] para curvas elípticas o [RFC5758] para DSA y ECDSA.

h) Identificador único del Emisor (*issuerUniqueID*): Este es un campo opcional que permite reutilizar nombres de emisor.

i) Identificador único del Suscriptor (*subjectUniqueID*): Este es un campo opcional que permite reutilizar nombres de sujeto.

j) Extensiones: Este campo tiene como propósito asociar información adicional a sujetos, claves públicas, etc. Un campo de extensión tiene tres partes:

   - Tipo de extensión: Es un identificador de objeto que proporciona la semántica y el tipo de información (cadena de texto, fecha u otra estructura de datos) para un valor de extensión.
   - Valor de la extensión: Este subcampo contiene el valor actual del campo.
   - Indicador de importancia: Es un atributo del tipo *bandera* que indica a una aplicación si es seguro ignorar el campo de extensión si no reconoce el tipo. El indicador proporciona una manera de implementar aplicaciones que trabajan de modo seguro con certificados y evolucionan conforme se van añadiendo nuevas extensiones.

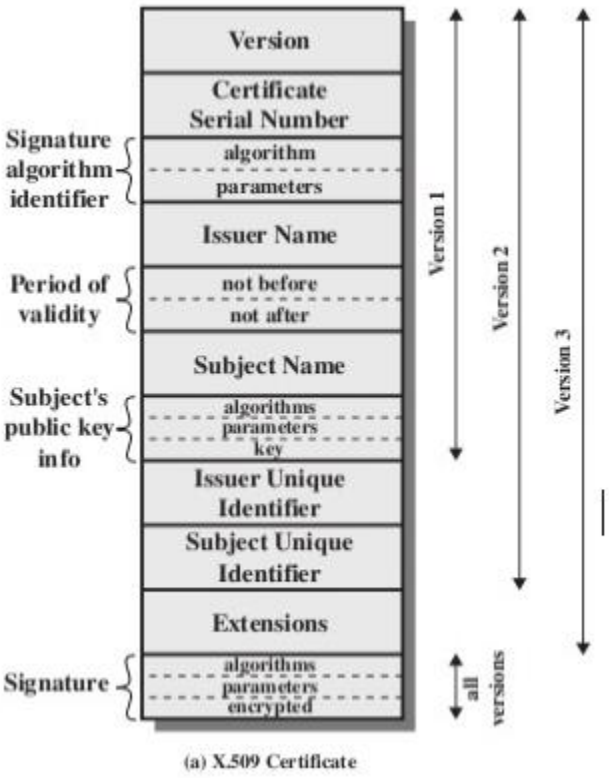
El ITU y el ISO/IEC han desarrollado y publicado un conjunto de extensiones estándar en un apéndice al X.509 v3, a saber:

- Limitaciones básicas: Este campo indica si el sujeto del certificado es una CA y el máximo nivel de profundidad de un camino de certificación a través de esa CA.
- Política de certificación: Este campo contiene las condiciones bajo las que la CA emitió el certificado y el propósito del certificado.
- Uso de la clave: Este campo limita el uso de la clave pública certificada, especificando, por ejemplo, que la clave debe ser empleada únicamente para firmar, para el cifrado de claves, cifrado de datos, etc. Este campo suele destacarse como importante, porque la clave está certificada solo para el propósito indicado, y cualquier otro uso no estaría autorizado por el certificado.

El formato de certificados X.509 se especifica en un sistema de notación denominado sintaxis abstracta uno (del inglés *Abstract Sintax One* o *ASN-1*). Para la transmisión de los datos se aplica el DER (*Distinguished Encoding Rules* o reglas de codificación distinguible), que transforma el certificado en formato ASN-1 en una secuencia de octetos apropiada para la transmisión en redes reales. (Secretaría de Modernización Administrativa, 2016, pág. 3) (Talens-Oliag, s.f.)

Figura 8

Estructura del certificado X.509 y sus versiones



Nota. Obtenido de Fundamentos sobre Certificados Digitales – El estándar X.509 y estructura de certificados, Cutanda, 2014.

Si bien la Figura 8 muestra el orden de campos con el propósito de identificar los cambios entre versiones, dicha estructura se organiza categóricamente en tres grupos principales, que son los siguientes:

a) *tbsCertificate*: Este campo contiene la información de emisor, sujeto, y periodo de validez, así como información adicional de interés.
b) *signatureAlgorithm*: Este campo proporciona la información necesaria para identificar de manera precisa el algoritmo criptográfico utilizado por la CA para firmar el certificado. Además, incluye campos opcionales que se emplearán según el tipo de algoritmo criptográfico utilizado.
c) *signatureValue*: Este campo alberga, como sugiere su nombre, la firma del certificado. Su función es garantizar, a través de la firma de la CA, que toda la información contenida en el campo *tbsCertificate* es auténtica. En esencia, este campo establece la cadena de confianza del certificado.
d) *Extensiones*: Las extensiones son un grupo de campos y parámetros opcionales que se pueden agregar al certificado, aunque no son obligatorios. Este campo fue introducido en la versión 3 del estándar *X.509.* (Cutanda, 2014)

Revocación de Certificados

Cuando una autoridad de certificación emite un certificado digital, establece un periodo de validez que generalmente varía entre tres y cinco años. El objetivo de este periodo de caducidad es obligar a la renovación de este, asegurando su actualización ante avances tecnológicos y reduciendo el riesgo de que sea vulnerado por nuevas tecnologías o amenazas emergentes. Como se mencionó anteriormente, la fecha de validez se especifica como uno de los atributos del certificado. No obstante, existen diversas circunstancias en las que la validez del certificado podría verse afectada, tales como el robo de claves privadas, información incorrecta y/o desactualizada, y procesos judiciales, entre otros (Cutanda, 2014).

Aquellos certificados que cumplan con esta condición deberán ser identificados y revocados, de forma visible para todos, utilizando para tal fin las llamadas Listas de Revocación de Certificados (del inglés *Certificate Revocation List*, o CRL). Las CRL son emitidas por las CA y poseen un periodo limitado de validez que por lo general consta de 1 año. Estas listas son emitidas con una estructura similar a la de un certificado, sin embargo, poseen otras características que describen la lista de certificados que serán revocados (Cutanda, 2014). Por otro lado, la actualización de las CRL debe realizarse constantemente en las PKI como una buena práctica, definiendo una fecha de

expiración a corto plazo para los certificados, y evitando así los posibles ataques a la identidad de las diversas entidades. Las CRL publicadas esporádicamente se deben consultar siempre para comprobar que un certificado no haya vencido en su validez (Cutanda, 2014).

Estructura de las CRL

Tal como lo indica la Secretaría de Modernización Administrativa (2016), la estructura de las listas de revocación está definida en el estándar ITU-T X.509 (CRL versión 2), este posee una estructura similar a la de los certificados digitales y los campos que lo conforman son los siguientes:

a. Versión: El campo *version* describe la versión de la CRL.
b. Algoritmo de Firma: El campo *signature* debe contener el identificador de objeto (OID) de los algoritmos y, de ser necesarios, los parámetros asociados usados por el certificador para firmar la CRL. Este identificador debe ser alguno de los definidos en el [RFC4055] para RSA, [RFC5480] para curvas elípticas (en el caso de utilizarse) o [RFC5758] para DSA y ECDSA.
c. Nombre Distintivo del Emisor: El campo *issuer* identifica a la entidad que firma y emite la CRL. Los contenidos y tipos de los atributos deben respetar las pautas establecidas para el campo *issuer* de un certificado.
d. Día y Hora de Vigencia: El campo *ThisUpdate* debe estar presente e indicar la fecha de emisión de la CRL. La fecha de revocación de un certificado de la lista no debe ser posterior a esta fecha. La CRL debe estar disponible para consulta inmediatamente después de emitida.
e. Próxima Actualización: El campo *NextUpdate* indica la fecha límite de emisión de la próxima CRL. Este campo debe estar presente en todas las CRL emitidas.
f. Certificados Revocados: El campo *RevokedCertificates* contiene la lista de certificados revocados indicando su número de serie y su fecha de revocación (Secretaría de Modernización Administrativa, 2016).

Asimismo, la Secretaría de Modernización Administrativa (2016), indica que deberán incluirse extensiones específicas para cada elemento de esta lista, de acuerdo con los criterios establecidos a continuación:

a) Identificación de Clave de la Autoridad Certificante: La extensión *AuthorityKeyIdentifier* proporciona un medio para identificar la clave pública que corresponde a la clave privada utilizada para firmar una CRL. Esta extensión debe estar presente en todas las listas de revocación de certificados.
b) Número de CRL: La extensión *CRLNumber* contiene un número de secuencia creciente para una CRL y emisor dado. Esta extensión permite que los usuarios determinen fácilmente cuándo una CRL particular reemplaza otra CRL. Esta extensión debe estar incluida en todas las listas de revocación de certificados.
c) Indicador de Delta CRL: La extensión *DeltaCRLIndicator* permite indicar que una CRL es una CRL incremental o "*delta CRL*". El certificador podría utilizar este tipo de extensión; En caso de existir, debe tratarse como una extensión crítica.
d) Punto de Distribución del Emisor: La extensión *IssuingDistributionPoint* identifica el punto de distribución y el alcance de una CRL particular. Indica, por ejemplo, si la CRL cubre la revocación de certificados del suscriptor solamente, certificados del certificador solamente, etc. El certificador podría utilizar este tipo de extensión; En caso de existir, debe tratarse como una extensión crítica.
e) CRL más Reciente – Punto de Distribución de la Delta CRL: La extensión *FreshestCRL* indica dónde puede obtenerse la información de la CRL de una CRL completa. Esta extensión no debería ser utilizada en "*delta CRL*" ni se trata de una extensión crítica. (Secretaría de Modernización Administrativa, 2016, pág. 17)

Autoridad de Certificación (CA)

La autoridad de certificación (o CA, del inglés *Certification Authority*), es el pilar sobre el cuál se basan las PKI, y podría definirse como un conjunto compuesto por el hardware, el software y las personas que la operan. Asimismo, una CA posee dos atributos distintivos: su nombre y su clave pública (Kuhn, 2001).

Una CA posee 4 funciones básicas: la emisión de certificados (creación y firma); la actualización del estado de los certificados, y correspondiente emisión de las CRL's; la publicación de los certificados y CRL's actuales (para que todas las entidades y/o usuarios puedan implementar los servicios de seguridad con la información actualizada) y, por último, mantiene el registro sobre

los certificados emitidos ya expirados. Estos requisitos pueden plantean cierto nivel de complejidad al ejecutarse simultáneamente, es por ello que la CA puede delegar ciertas funciones en los demás componentes de la infraestructura (Kuhn, 2001).

Una CA puede emitir certificados para usuarios, para otras CA, o para ambos. Al emitir un certificado, la CA está certificando que el sujeto (la entidad mencionada en dicho certificado) posee la clave privada correspondiente a la clave pública contenida en el certificado. Si la CA añade información adicional en el certificado, también está confirmando que dicha información corresponde al sujeto en cuestión. Esta información adicional puede incluir datos de contacto (como una dirección de correo electrónico), o detalles sobre políticas (por ejemplo, los tipos de aplicaciones que podrán utilizar esta clave pública). Cuando el sujeto del certificado es otra CA, el emisor está garantizando que los certificados emitidos por esa CA también son de confianza (Kuhn, 2001).

La CA inserta su nombre en cada certificado (y CRL) que genera, y los firma con su clave privada. Una vez que las entidades establecen una relación de confianza con la CA (directamente, o a través de una ruta de certificación), se indica que los certificados emitidos por esa CA son confiables; Posteriormente, las entidades podrán identificar fácilmente los certificados emitidos por la CA de confianza comparando su nombre. Para asegurarse de que el certificado es auténtico, verifican la firma utilizando la clave pública de la CA. Por lo tanto, es importante que la CA proporcione una protección adecuada para su propia clave privada. (Kuhn, 2001)

Autoridad de Registro (RA)

La autoridad del registro (o RA, del inglés *Registration Authority*) cumple el papel de verificar el contenido de cada certificado emitido por una CA. El contenido del certificado puede reflejar información presentada por la entidad que lo solicita, como una licencia de conducir o un talón de pago; Asimismo, podría reflejar información proporcionada por terceros (ej.: el límite de crédito asignado a una tarjeta de crédito refleja información obtenida de una entidad bancaria). La autoridad de registro agrega estas entradas y proporciona esta información a la CA (Kuhn, 2001).

En línea con lo indicado para las CA's, las autoridades de registro también se basan en un conjunto de hardware y software, y son operadas por una o más personas. A diferencia de las CA's, una autoridad de registro suele contar con un operador único. Cada CA mantendrá una lista de RA's

acreditadas; es decir, una lista de RA's con las cuales se ha establecido una relación de confianza (Kuhn, 2001). La CA identifica una RA por un nombre y una clave pública. Al verificar la firma de la autoridad de registro en un mensaje, la autoridad de certificación podrá validar que una autoridad de registro confiable proporcionó la información, por lo que es de vital importancia que las autoridades de registro cuenten con un nivel de protección adecuado para su propia clave privada. (Kuhn, 2001).

Por último, y al igual que las autoridades de certificación, las RA's cuentan con la posibilidad de delegar determinadas funciones (ej.: proceso de firma de certificados) a otros componentes de la PKI. Proporcionaremos mayores detalles acerca de estos dispositivos y su implementación en las secciones subsiguientes.

3.2.3.2 Módulo de Seguridad de Hardware (HSM)

Denominamos módulo de seguridad de hardware (o HSM, del inglés *Hardware Security Module*) a un procesador criptográfico especializado, diseñado específicamente para salvaguardar el ciclo de vida de las claves criptográficas. Los HSM actúan como plataformas de confianza que protegen la infraestructura criptográfica de las organizaciones, gestionando, procesando y almacenando de manera segura las claves criptográficas dentro de un dispositivo robusto y resistente a manipulaciones o alteraciones por parte de terceros.

El rol del HSM en la infraestructura PKI

Los módulos de seguridad de hardware desempeñan un papel crucial al incrementar el nivel de seguridad de la infraestructura de clave pública, proporcionando un entorno seguro y estable para la producción, procesamiento, control de acceso y almacenamiento de las claves criptográficas. Dentro de las principales características de los módulos de seguridad de hardware, pueden destacarse la mejora en la gestión de las claves, la descarga de operaciones intensivas y los mecanismos de autorización y control de acceso.

Mejoras en la gestión de las claves*:* La función principal de los HSM es salvaguardar las claves criptográficas utilizadas en la infraestructura de clave pública (Ssl, 2023). Estos módulos ofrecen

un entorno seguro para la creación, almacenamiento y control de acceso a las claves. Los HSM refuerzan la seguridad de las claves de las siguientes maneras:

Generación de claves seguras: Los HSM facilitan la creación de claves criptográficas y representan una fuente confiable para la generación de números aleatorios, garantizando la integridad y robustez de las claves al no depender de interacciones externas (Ssl, 2023).
Diseño resistente: Los HSM están diseñados con mecanismos de seguridad física que previenen la manipulación física por parte de terceros. Generalmente, cuentan con carcazas metálicas reforzadas, sensores de detección de impacto o sabotaje, y en algunos, mecanismos de autodestrucción que se activan al detectar intentos de alteración del dispositivo (Ssl, 2023).
Seguridad en el almacenamiento de claves: Los HSM ofrecen un entorno seguro para almacenar las claves criptográficas dentro de su hardware, evitando accesos no autorizados. Las claves se cifran y se almacenan en una memoria interna, previniendo su extracción o manipulación. De esta forma, todas las claves almacenadas en el HSM permanecen seguras, incluso si el atacante logra acceder físicamente al módulo (Ssl, 2023).

Descarga de operaciones intensivas*:* Los HSM incrementan la eficiencia al externalizar los procesos criptográficos (que suelen requerir una carga de procesamiento) desde la capa de software hacia un módulo de hardware especializado (Ssl, 2023). Esta transferencia aporta beneficios en varios aspectos:

Optimización de operaciones criptográficas: Los HSM están diseñados para realizar operaciones criptográficas de manera eficiente. Las organizaciones pueden mejorar significativamente la velocidad y el rendimiento de tareas como la generación de claves, la firma y el descifrado al aprovechar el hardware del HSM (Ssl, 2023).
Reducción de carga de procesamiento*:* Al delegar las funciones criptográficas en los HSM, se libera la capacidad de cómputo en servidores y otros dispositivos, permitiendo que esa potencia se utilice para otras tareas críticas. Esto contribuye a mejorar el rendimiento y la escalabilidad del sistema, especialmente en entornos con un alto volumen de operaciones criptográficas (Ssl, 2023).
Protección contra ataques de canal lateral: Los ataques de canal lateral, que explotan la información revelada durante las operaciones criptográficas, están diseñados para ser

contrarrestados por los HSM. Los componentes internos del HSM trabajan para mitigar este tipo de ataques, protegiendo la integridad de las claves (Ssl, 2023).

Autorización y control de acceso*:* Los HSM incorporan funciones específicas de control de acceso para asegurar que sólo personas y procesos autorizados puedan acceder y utilizar las claves criptográficas (Ssl, 2023). Entre las medidas de control de acceso se incluyen:

Autenticación: Los HSM exigen técnicas de autenticación como contraseñas, claves criptográficas o datos biométricos para acceder a las claves almacenadas. Esto previene que usuarios no autorizados puedan acceder al dispositivo, o bien extraer las claves almacenadas (Ssl, 2023).
Políticas de autorización: Las organizaciones pueden configurar los HSM para establecer políticas de autorización detalladas que determinen que entidades o procesos tienen permiso para acceder a ciertas claves y realizar acciones criptográficas. Estas políticas aseguran el menor nivel de privilegio necesario y evitan el uso indebido o no autorizado de las claves (Ssl, 2023).
Auditoría y documentación: Los HSM mantienen registros detallados de auditoría sobre la gestión de claves, incluyendo el uso de estas, intentos de acceso y cambios en la configuración. Estos registros permiten a las organizaciones monitorear y revisar las actividades relacionadas con las claves, identificar irregularidades y asegurar el cumplimiento de las normas de seguridad (Ssl, 2023).

3.2.4 Beneficios de la arquitectura PKI

Tal como se detalla en los párrafos anteriores, una infraestructura de clave pública es una solución global de seguridad aplicable a los entornos más heterogéneos. A continuación, se enumeran algunas ventajas aparejadas con la implementación de esta arquitectura:

Gestión de credenciales e inicio de sesión único (o SSO, del inglés *Single Sign On*)*:* Una PKI resuelve los inconvenientes comunes relacionados a la gestión de credenciales de acceso (usuario/contraseña) de los esquemas de autenticación tradicionales, de manera consistente y sencilla para los operadores (Valdiviezo Echeverría, 2012, pág. 89).
Firmas digitales: Una PKI permite firmar digitalmente documentos, contando este tipo de firma con validez legal. Esto hace posible el reemplazo del papel por formularios electrónicos,

incrementando además la velocidad de procesamiento, y proporcionando herramientas de trazabilidad no soportadas por otro tipo de medios (Valdiviezo Echeverría, 2012, pág. 89).

Cifrado: Fácil cifrado de datos para cada individuo (sin intercambio previo de información) mediante el acceso al certificado que contiene la clave pública (Valdiviezo Echeverría, 2012, pág. 89).

Simplicidad: Al reducir la cantidad de contraseñas requeridas, se maximiza la comodidad del usuario u operador. Las PKI ofrecen un mecanismo consistente de autenticación, brindando procedimientos sencillos para las operaciones de cifrado, y firma, facilitando su adopción (Valdiviezo Echeverría, 2012, pág. 90).

Administración coherente de la seguridad: Emisión y revocación centralizada de credenciales. Identificación consistente de cada entidad al emitir las credenciales. Mecanismo de autenticación unificado para todas las aplicaciones o servicios de red, permitiendo también maximizar la inversión en hardware y software debido a la interoperabilidad que PKI ofrece (Valdiviezo Echeverría, 2012, pág. 90).

Interoperabilidad con otras instituciones: La confianza entre organizaciones y/o empresas permite firmar y cifrar correos, firmar documentos, autenticación en aplicaciones compartidas (Valdiviezo Echeverría, 2012, pág. 90).

Soluciones basadas en estándares: Los estándares proporcionan interoperabilidad entre los diferentes fabricantes, permitiendo así la integración de los diversos componentes en un entorno homogéneo (Valdiviezo Echeverría, 2012, pág. 90).

3.2.5 Limitaciones y puntos de mejora

Conociendo las ventajas y beneficios de las PKI, en inevitable no mencionar que este tipo de soluciones cuenta también con puntos débiles. En la actualidad, las PKI dependen en gran medida de la integridad de las autoridades de certificación y las autoridades de registro asociadas, que no siempre funcionan con la precisión y diligencia esperables. Asimismo, la gestión de errores de las PKI representa otro eslabón débil que debería abordarse.

Otra limitación conocida subyace en la falta de autenticación multifactorial en la gran mayoría de las implementaciones y/o entornos donde se aplique este tipo de arquitectura; Independientemente de la evolución de las herramientas y/o tecnologías que buscan vulnerar las credenciales de acceso,

las PKI no cuentan con un método de segregación que incluya varios niveles de autorización antes de darle curso a una petición.

Por otro lado, cabe destacar que la usabilidad general de este tipo de solución nunca ha sido ideal. La mayoría de las veces, las implementaciones de PKI revisten una gran complejidad, generando en algunos casos una negación por parte de los usuarios, que prefieren resignar el uso de una arquitectura de autenticación multifactorial a cambio de un proceso de seguridad más cómodo y práctico.

Por último, la tecnología PKI es conocida por su escasa flexibilidad para adaptarse fácilmente a los avances del mundo digital. Los usuarios de este tipo de soluciones manifiestan habitualmente una gran disconformidad respecto a la falta de herramientas y soporte para la integración de nuevas aplicaciones, orientadas a mejorar la seguridad, la comodidad y la escalabilidad.

Capítulo IV - Desarrollo del proyecto

4.1 Propuesta técnica

Considerando todos los aspectos detallados en capítulos anteriores, la presente propuesta contempla el cifrado del flujo de comunicaciones entre las RTUs (en este caso específico, el PLC maestro) y la MTU. Como parte del escenario, se asume que las RTUs poseen una baja potencia computacional, debido a que están diseñadas para ejecutar un conjunto limitado de operaciones, conteniendo a menudo la lógica de control específica para una aplicación determinada. En base a esta limitación, todas las operaciones de cifrado/descifrado, almacenamiento y gestión de llaves serán llevadas a cabo por el módulo de seguridad de hardware (HSM), que también cumplirá el rol de CA, concentrando en un único componente todas las operaciones para la correcta implementación de una capa de seguridad sólida en el sistema SCADA.

4.1.1 Prerrequisitos y suposiciones

La presente propuesta contempla el desarrollo de una solución de seguridad basada en PKI sobre un entorno SCADA preexistente. Considerando que existen múltiples escenarios de aplicación para este tipo de solución, es importante definir una serie de requerimientos y acciones que deberán analizarse detalladamente para determinar la viabilidad o no del proyecto. A continuación, se detallan algunos prerrequisitos claves para garantizar su correcta implementación:

a) Evaluación de los requisitos de seguridad: Será necesario ejecutar una evaluación sobre los requisitos de seguridad específicos del entorno SCADA. Será fundamental contar con el detalle de los activos que deban protegerse, detectar cualquier vulnerabilidad y/o potencial amenaza, requerimientos regulatorios y cualquier otra consideración relacionada con la seguridad del entorno.
b) Estado de la infraestructura: La evaluación de la infraestructura existente del entorno SCADA será fundamental para garantizar el soporte de la solución PKI. Esta revisión deberá contemplar la arquitectura de red, los componentes de hardware y de software, requisitos de conectividad y opciones de escalabilidad para escenarios futuros.
c) Evaluación y mitigación de riesgos: Llevar a cabo una evaluación exhaustiva de riesgos será fundamental para identificar las vulnerabilidades y potenciales amenazas que podrían

comprometer la implementación de la PKI. Asimismo, será necesario elaborar estrategias de mitigación y planes de contingencia para abordar aquellos riesgos que pudieran identificarse, garantizando así la seguridad y resiliencia de la infraestructura.

d) Políticas y procedimientos: Será necesario contar con una serie de políticas, procedimientos y lineamientos que regulen el uso de PKI en el entorno SCADA. En caso de no contar con estas políticas, será necesario desarrollarlas, definiendo correctamente las funciones, responsabilidades y alcances de cada uno de los actores participantes, buenas prácticas para la gestión de los certificados, gestión del ciclo de vida de las claves y procedimientos de respuesta ante incidentes.
e) Cumplimiento de normativas y reglamentos: Será necesario validar que el ambiente cumplimente las normas del sector y los requisitos normativos relacionados con la seguridad de PKI y SCADA. Esto podría incluir normas como NIST SP 800-53, NCICC, IEC 62443, NERC CIP, GDPR y otras, en función del rubro de aplicación, jurisdicción, etc.
f) Integración con los componentes existentes: Será necesario evaluar los requisitos de integración para implementar una solución PKI en el entorno SCADA. La compatibilidad entre los módulos de software, hardware, protocolos e interfaces de comunicación SCADA serán fundamentales para garantizar la correcta interoperabilidad del entorno.

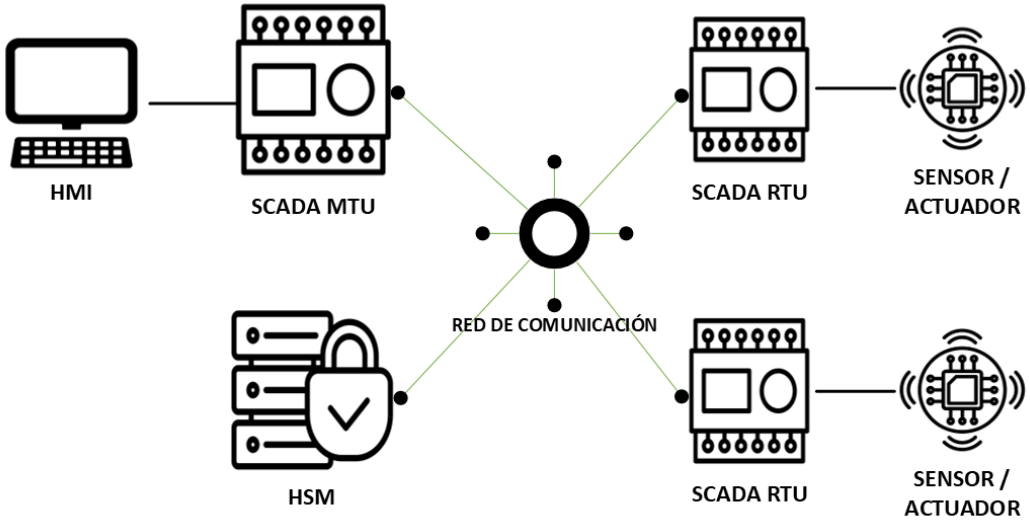
Si bien el desarrollo de los prerrequisitos antes mencionados no forma parte del alcance de este trabajo, se considera que el escenario de aplicación cuenta con los requisitos mínimos, políticas, procedimientos y componentes de hardware/software para la correcta implementación de la solución PKI.

4.2 Visión general del sistema

La arquitectura del sistema SCADA modelo se encuentra representada en la Figura 9. Como en la mayoría de los sistemas SCADA, el diseño simplificado consta de una MTU, una RTU (en esta aplicación en particular, el PLC maestro) y un canal de comunicación.

Figura 9

Arquitectura modelo SCADA



Nota. Figura de autoría propia.

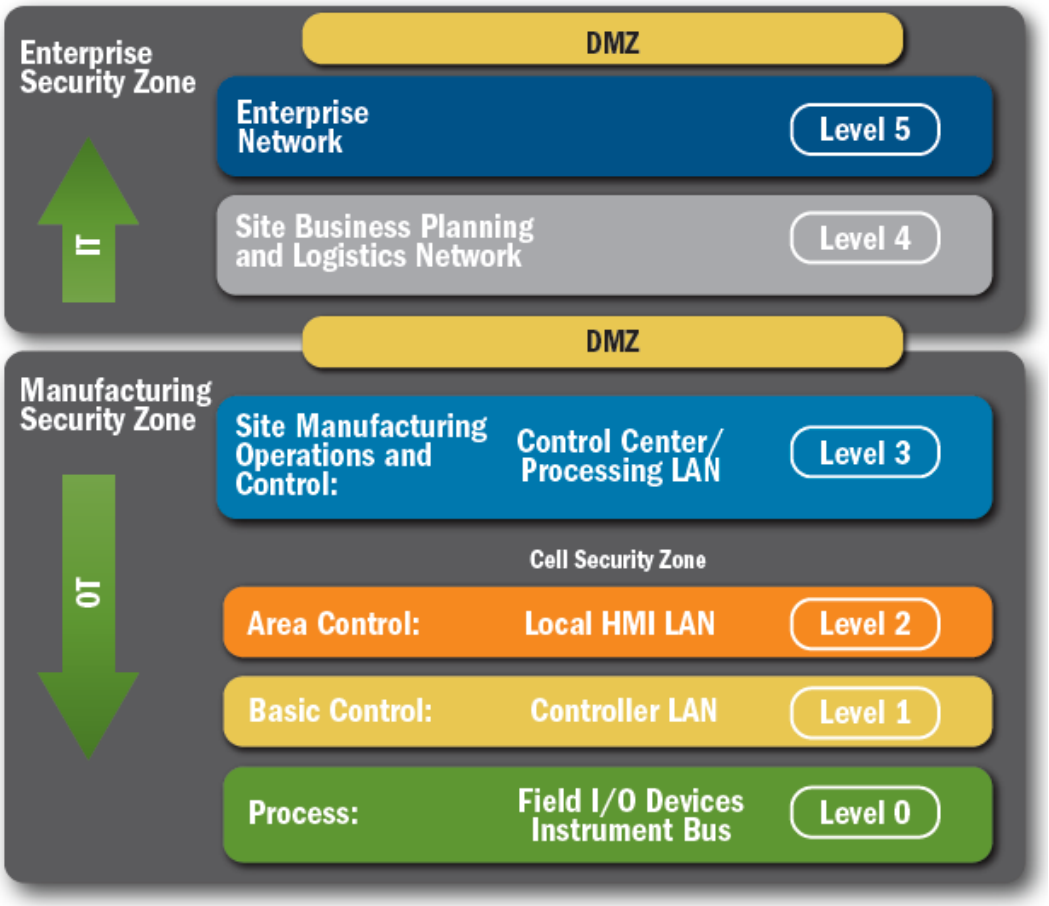
Las RTU y la MTU están interconectadas mediante una red del tipo ethernet. Sobre el protocolo a utilizar, considerando factores como compatibilidad, eficiencia y escalabilidad, se optará en este caso por el estándar TCP/IP, posibilitando la correcta integración del módulo de seguridad de hardware (HSM) en el entorno existente.

4.2.1 Arquitectura de red

Tal como se menciona en el apartado prerrequisitos y suposiciones de este trabajo, se presupone que la arquitectura de red existente se encuentra normada por los estándares y buenas prácticas aceptadas y aplicadas globalmente. La siguiente figura representa un modelo de segregación de los segmentos de red a través de niveles; Asimismo, existe una demarcada frontera entre ambas zonas de seguridad (zona corporativa y zona de control productivo), representada a través de una zona desmilitarizada (o DMZ, del inglés "*Demilitarized Zone"*), que proporciona una capa de aislación adicional entre los segmentos de red IT y OT. La posibilidad de establecer DMZ's entre las redes corporativa y de control representa una importante mejora facilitada por el uso de los cortafuegos (del inglés "*firewall*"). El esquema de segmentación en cuestión se detalla en la Figura 10, obtenida de (Nccic / Ics-Cert, 2016).

Figura 10

Segmentación de zonas ICS y red Corporativa



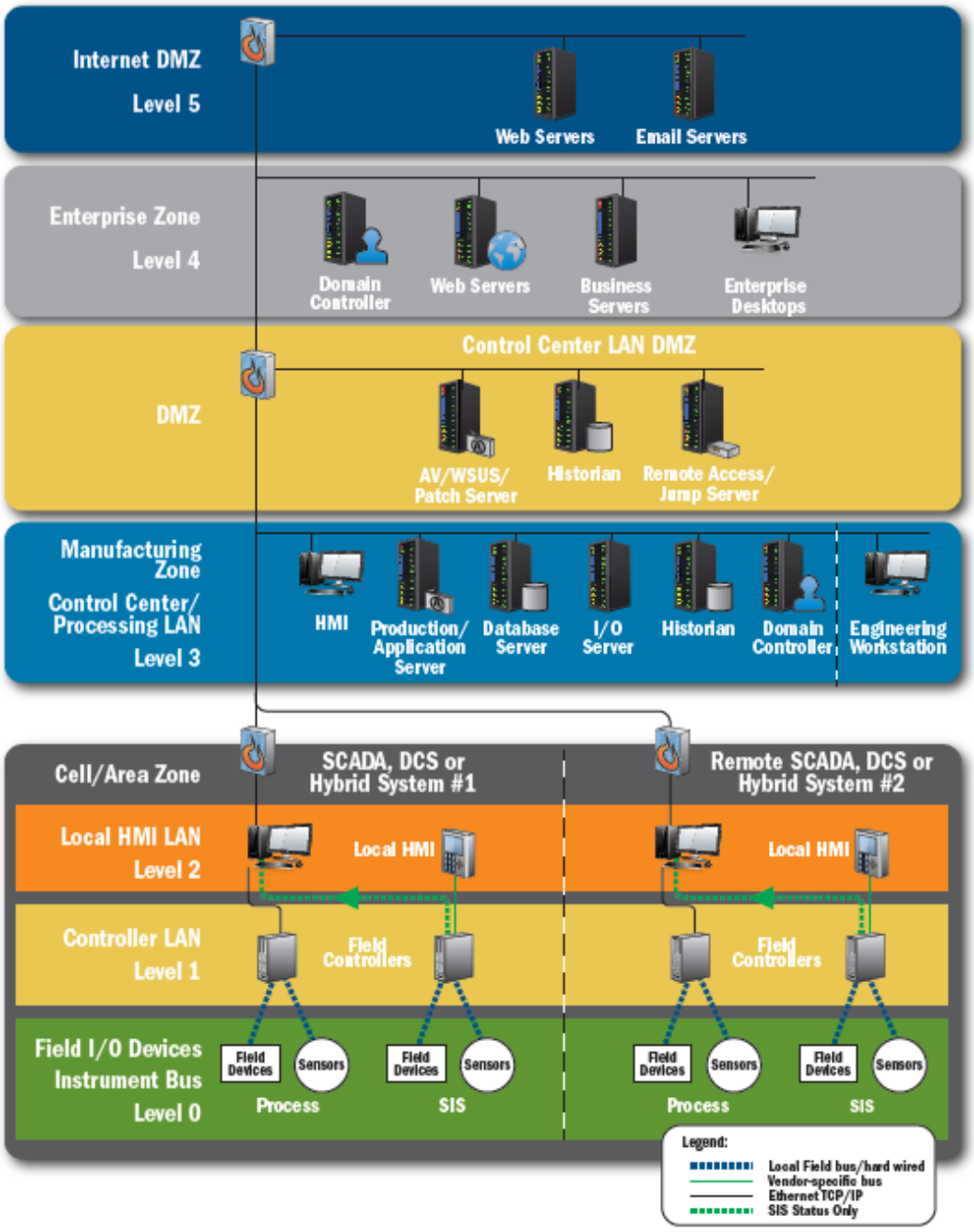
Nota. Obtenido de *Improving Industrial Control System Cybersecurity with Defense-in-Depth Strategies*, Ncicc/Ics-Cert, 2016

Los dispositivos dentro del alcance del presente documento se encontrarán emplazados en la zona de seguridad de manufactura, siendo el Nivel 3 denominado segmento de control y operación del sitio, y el nivel inferior (Nivel 2) denominado como control de área. El Nivel 3 usualmente aloja dispositivos de monitoreo, control operativo y adquisición de datos. Se trata de un segmento crítico para garantizar la continuidad y correcta gestión de la red de control. Por otro lado, el Nivel 2 contiene sistemas y dispositivos empleados para la administración y el control de otros equipos localizados en el mismo segmento de red, o bien en segmentos inferiores, tales como HMI's instalados en el área de producción, PLC's y sus controles (Nivel 1), y otros dispositivos de

entrada/salida tales como actuadores o sensores (Nivel 0) (ICCCERT, 2016, pág. 19). El grado de importancia de estos niveles es crítico, ya que son las áreas donde las funciones de control tienen un impacto directo sobre los dispositivos físicos de los niveles inferiores. Considerando el grado de criticidad de ambos niveles, el enfoque propuesto consistirá en la implementación del módulo de seguridad de hardware emplazado entre los niveles 2 y 3 para el aseguramiento del tráfico entre la MTU y los RTUs. La arquitectura propuesta se encuentra definida en detalle en la Figura 11, obtenida de (Nccic / Ics-Cert, 2016).

Figura 11

Arquitectura de red recomendada



Nota. Obtenido de *Improving Industrial Control System Cybersecurity with Defense-in-Depth Strategies,* Ncicc/Ics-Cert, 2016

Flujos de comunicación

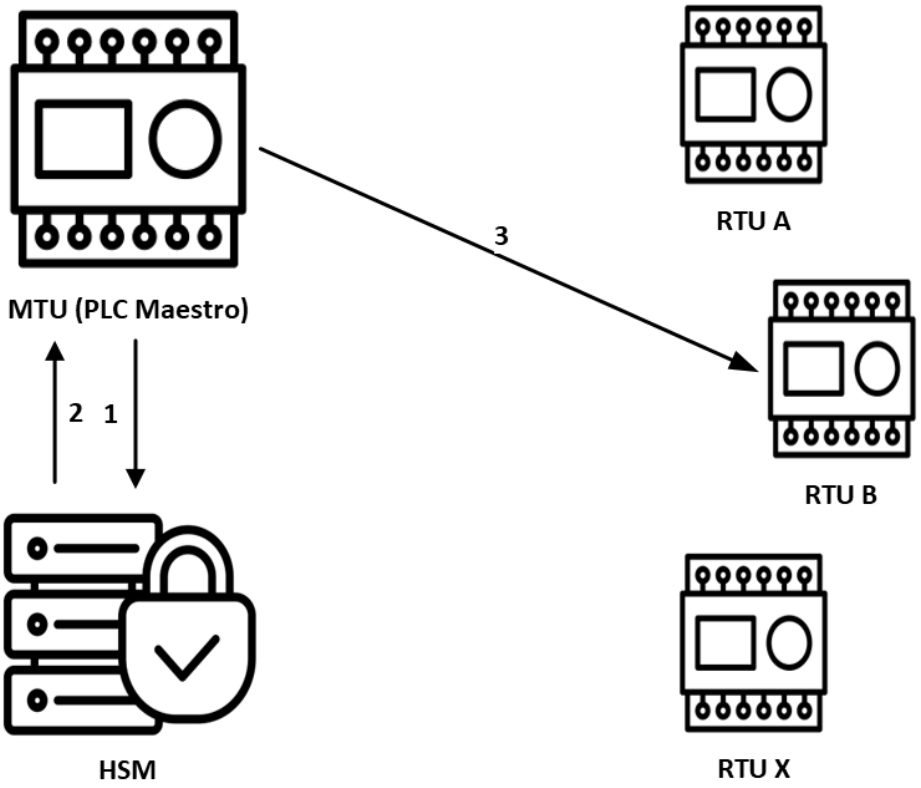
Tal como se detalla en párrafos previos, el escenario de aplicación está compuesto por 3 componentes: la MTU (*Master Terminal Unit*), la RTU (*Remote Terminal Unit*) y el HSM

(*Hardware Security Module*). Existen tres tipos de comunicación posibles para el intercambio de mensajes y autenticación: HSM hacia MTU hacia RTU (Figura 12), MTU hacia RTU (Figura 13) y, finalmente, RTU hacia RTU (Figura 14), quedando este último por fuera del alcance de este trabajo.

El esquema asume que la MTU y las RTUs cuentan con un escaso poder computacional, delegando todas las operaciones de cifrado, descifrado, almacenamiento y gestión de llaves en el módulo HSM.

Figura 12

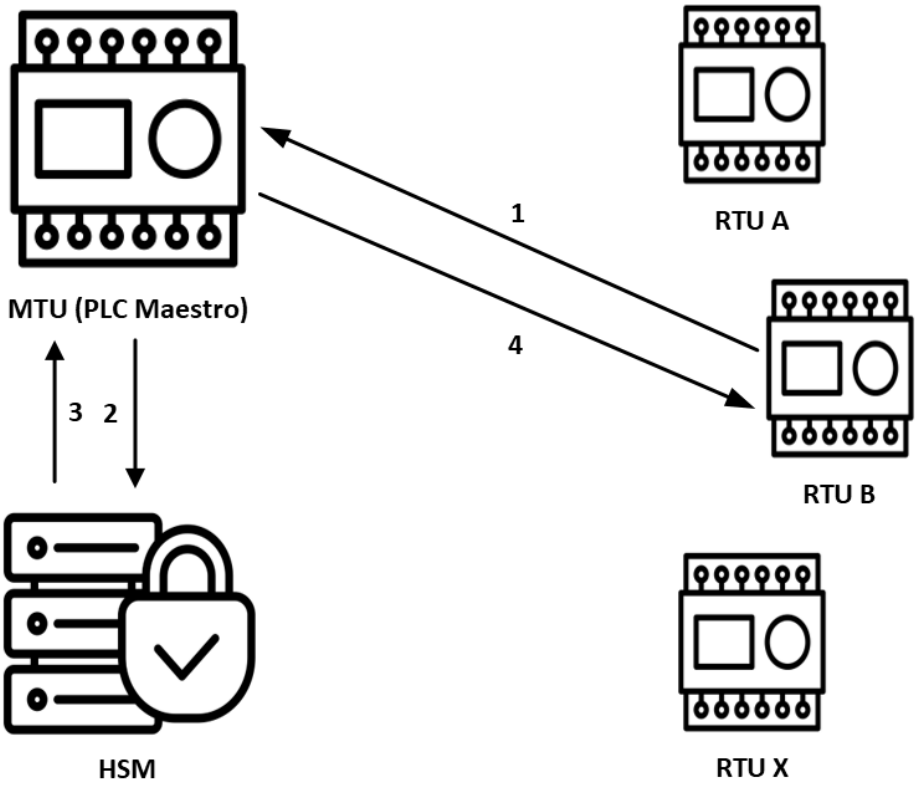
Comunicación entre MTU y RTU



Nota. *Adaptado* de Customized PKI for SCADA System, Saxena *et al*, 2010

Figura 13

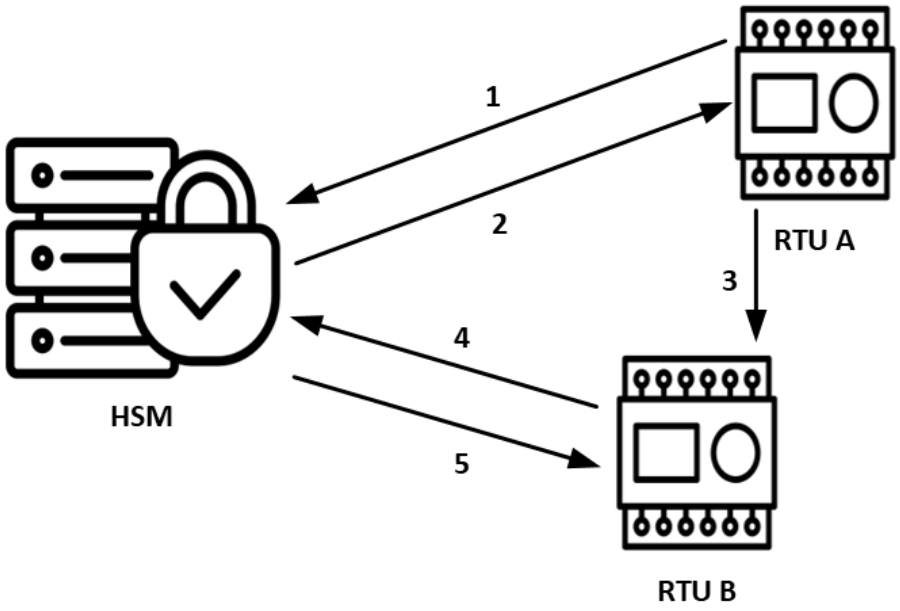
Comunicación entre RTU y MTU



Nota. Adaptado de *Customized PKI for SCADA System,* Saxena et al, 2010

Figura 14

Comunicación entre RTU y RTU



Nota. Adaptado de Customized PKI for SCADA System, Saxena et al, 2010

Flujo de autenticación PKI

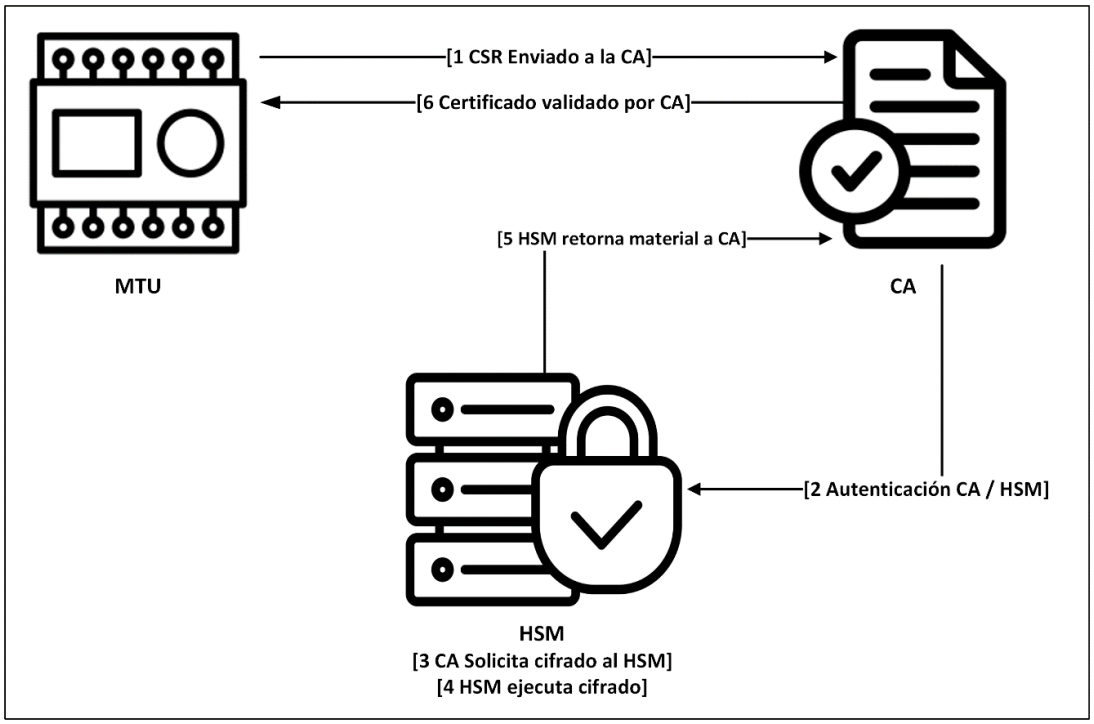
1) El HSM genera un par de claves (pública y privada) y crea un certificado digital para validar su identidad. El certificado es firmado por la CA para garantizar su validez. Las claves generadas permanecerán almacenadas en el repositorio de claves del HSM. Por otro lado, el MTU genera su propio par de claves, y obtiene un certificado digital de la CA.
2) El certificado del HSM y su clave pública se distribuyen entre los componentes que requieran validar su identidad (MTU). Por otro lado, la MTU distribuye su certificado y clave pública con su contraparte (HSM). De esta forma, los dispositivos se configuran para generar una autenticación mutua (cada dispositivo deberá conocer la identidad y la clave pública del otro).
3) Cuando la MTU necesita comunicarse con el HSM, inicia una solicitud de conexión. La CA solicita los atributos de identificación de propietario de la clave privada y los verifica. La clave pública y los atributos se codifican en una solicitud de firma de certificado (o CSR, del inglés: *Certificate Signing Request*) y son enviados al dispositivo solicitante.
4) La CA envía el certificado firmado hacia el dispositivo de destino.

5) El dispositivo utiliza el certificado para identificarse. Con la autenticación y el intercambio de claves de sesión completados, el HSM y la MTU establecen un canal de comunicación cifrado. Esto garantiza que la información intercambiada entre ambos dispositivos esté protegida contra sabotaje o manipulación.
6) Si el certificado se encuentra próximo a expirar, deberán repetirse los pasos 2-4.

El flujo de autenticación modelo se encuentra representado de manera gráfica en la Figura 15, obtenida de (Gratz, 2021).

Figura 15

Flujo de autenticación modelo



Nota. Adaptado de *Components of a PKI, Part 5: Hardware Security Modules,* Gratz, 2021

Planificación de los recursos

La implementación de un dispositivo HSM para gerenciar las operaciones de cifrado requiere una cuidadosa planificación y asignación de los recursos humanos que intervendrán en el proyecto. A continuación, se detallarán los perfiles que el autor considera necesarios para la correcta ejecución de la propuesta en cuestión:

Tabla 2

Perfil de puesto: Gerente de Proyecto

Rol	**Gerente de Proyecto (PM)**
Responsabilidades	▪ Desarrollar el alcance y los objetivos del proyecto, involucrando a todas las partes interesadas, y garantizando su viabilidad técnica. ▪ Establecer un plan de proyecto detallado para controlar su progreso. ▪ Coordinar los recursos internos y de terceros/proveedores para la correcta ejecución del proyecto. ▪ Garantizar la correcta ejecución de los hitos para entregar el proyecto a tiempo, considerando el alcance y presupuesto definidos. ▪ Garantizar la disponibilidad y correcta asignación de recursos. ▪ Evaluar el rendimiento del proyecto utilizando técnicas y herramientas acordes. ▪ Mantener informados a todos los participantes sobre el estado de avance, escalando los puntos críticos a los stakeholders. ▪ Crear y mantener la documentación de soporte del proyecto.

Tabla 3

Perfil de puesto: Arquitecto de Seguridad

Rol	**Arquitecto de Seguridad (SAR)**
Responsabilidades	▪ Desarrollar y aplicar una estrategia de seguridad multinivel. ▪ Identificar y evaluar los potenciales riesgos de seguridad. ▪ Implementar medidas de seguridad para la correcta mitigación de los riesgos.

	▪ Diseñar y mantener controles de seguridad en las aplicaciones e infraestructuras afectadas al proyecto. ▪ Garantizar el correcto cumplimiento de normativas y regulaciones vigentes aplicables al segmento/industria en cuestión. ▪ Concientizar a todos los involucrados cuestiones relacionadas con la seguridad informática.

Tabla 4

Perfil de puesto: Analista de Seguridad

Rol	**Analista de Seguridad (SAN)**
Responsabilidades	▪ Ejecutar evaluaciones de seguridad y definición de un orden de prioridades para la corrección de los potenciales hallazgos. ▪ Diseñar y mantener controles de seguridad en las aplicaciones e infraestructuras afectadas al proyecto. ▪ Reforzar las herramientas de control y supervisión para la pronta detección de comportamiento anómalos. ▪ Promover la concienciación y la formación en materia de seguridad dentro del grupo de trabajo.

Tabla 5

Perfil de puesto: Administrador de Infraestructura

Rol	**Administrador de Infraestructura (IA)**
Responsabilidades	▪ Referente principal para las necesidades de infraestructura del proyecto. ▪ Recomendar mejoras para los componentes de infraestructura de TI afectados. ▪ Coordinar los recursos internos y de terceros/proveedores para la correcta ejecución del proyecto. ▪ Ofrecer asistencia técnica para los potenciales incidentes relacionados con sistemas informáticos, hardware, redes y servicios.

	▪ Garantizar el correcto cumplimiento de normativas y regulaciones vigentes aplicables al segmento/industria en cuestión.

Tabla 6

Perfil de puesto: Ingeniero de Networking

Rol	**Ingeniero de Networking (NE)**
Responsabilidades	▪ Configurar e instalar equipamiento y servicios de red (*routers, switches, firewalls, load balancers, VPNs, QoS,* etc.) ▪ Realizar el mantenimiento de la red, actualizaciones de firmware de los componentes críticos, paquetes de servicios, parches, correcciones urgentes y configuraciones de seguridad. ▪ Supervisar el rendimiento y garantizar la disponibilidad y fiabilidad de la red informática. ▪ Supervisar la utilización de los recursos del sistema, las tendencias y la planificación de la capacidad. ▪ Proporcionar asistencia de nivel 2/3 para escenarios de conectividad complejos. ▪ Gestionar los cambios requeridos a través de un marco de *Change Management*, garantizando la correcta documentación, aprobación e implementación de los cambios en la infraestructura afectada.

Tabla 7

Perfil de puesto: Analista de Soporte Técnico

Rol	**Analista de Soporte Técnico (TS)**
Responsabilidades	▪ Configurar e instalar dispositivos de hardware, software y controladores. ▪ Gestionar las opciones y el software de seguridad en ordenadores y redes para mantener la privacidad y la protección frente a potenciales ataques. ▪ Realizar actualizaciones periódicas para garantizar el correcto funcionamiento y solidez de la infraestructura instalada.

	▪ Ofrecer asistencia técnica y concientizar a los usuarios sobre las buenas prácticas de uso de los sistemas informáticos.

Tabla 8

Perfil de puesto: Capacitador

Rol	**Capacitador (TR)**
Responsabilidades	▪ Desarrollar el programa de capacitación técnica de acuerdo con los requisitos del proyecto. ▪ Estipular el contenido de los cursos en línea con el alcance del proyecto. ▪ Preparar el material de capacitación (presentaciones, hojas de cálculo, etc.) ▪ Celebrar sesiones de capacitación, seminarios, talleres, etc. considerando el perfil de cada uno de los miembros participantes. ▪ Mantener un registro de datos sobre los cursos impartidos, las ausencias, los problemas, etc. y elaborar informes. ▪ Observar y evaluar los resultados de los programas de capacitación ▪ Desarrollar métricas para determinar la efectividad general de los programas de capacitación y efectuar mejoras en caso de ser necesario.

Tabla 9

Perfil de puesto: Especialista SCADA

Rol	**Especialista SCADA (SS)**
Responsabilidades	▪ Colaborar con el equipo de proyecto para diseñar y adaptar las soluciones SCADA existentes a los procesos y requisitos industriales estipulados en el alcance. ▪ Configurar, programar y desplegar componentes de hardware y software SCADA, tales como HMI's, PLC's y protocolos de comunicación. ▪ Supervisar continuamente la infraestructura SCADA para garantizar su estabilidad, seguridad y eficiencia de los procesos industriales. Asimismo, deberá responder rápidamente ante alarmas y anomalías.

▪ Analizar datos históricos y en tiempo real para identificar tendencias, anomalías y problemas potenciales. Desarrollar estrategias de optimización de procesos basadas en la información obtenida. ▪ Diagnosticar y resolver fallos del sistema SCADA y errores de software. Establecer un plan de mantenimiento rutinario, actualizaciones de software y las copias de seguridad del sistema. ▪ Desplegar y mantener medidas de ciberseguridad para proteger los sistemas SCADA de accesos no autorizados, ciber amenazas y vulnerabilidades. ▪ Mantener una documentación de soporte actualizada, incluyendo respaldos de archivos de configuración, diagramas de red y procedimientos operativos.

Cronograma de trabajo

En línea con la planificación de los recursos previamente desarrollada, se enumera a continuación el plan de trabajo para implementar la solución en cuestión. Dicho plan se divide en varias fases para estructurar las tareas, y garantizar que cada etapa del proyecto se ejecute de manera organizada y eficiente.

4.2.2 Cuadro de tareas

La tabla 10 proporciona el detalle de las tareas requeridas para la correcta ejecución de la propuesta en cuestión. El cuadro de tareas fue dividido en varias fases, que a su vez incluyen un conjunto de subtareas, para la correcta visualización del estado de avance del proyecto.

Tabla 10

Cuadro de Tareas

Fase 1 - Tareas Preliminares
a) Definición de objetivos y alcance del proyecto.
b) Identificación / documentación de los requisitos del HSM.
c) Evaluación del entorno SCADA preexistente y cómo se integrará el HSM.
d) Elaboración del plan de proyecto detallado (incluyendo cronograma y presupuesto).

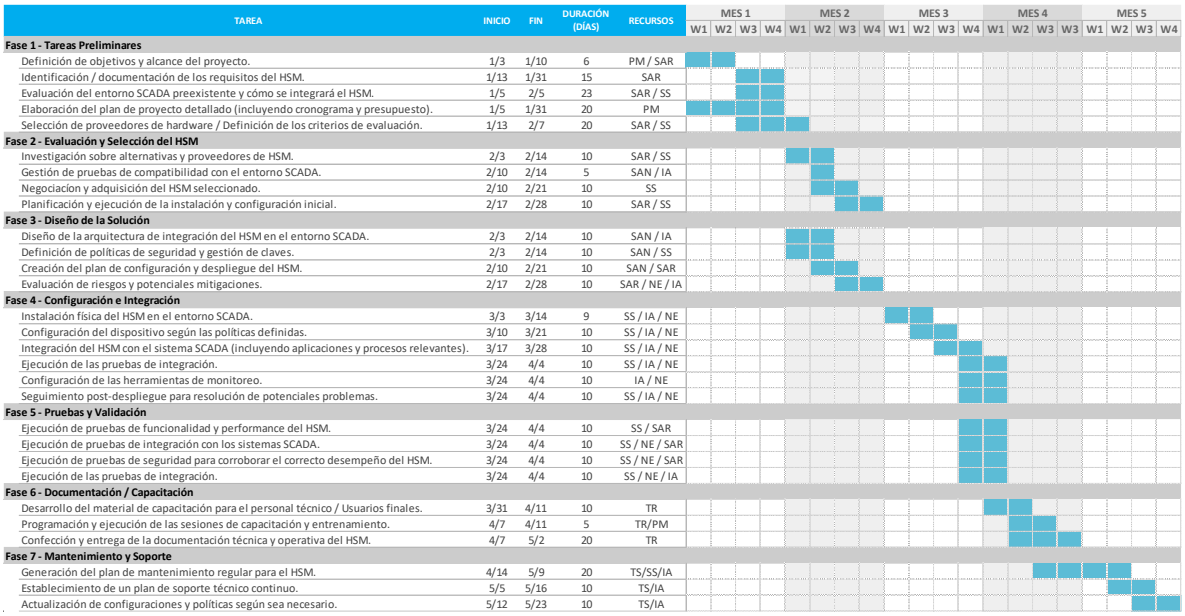
e) Selección de proveedores de hardware / Definición de los criterios de evaluación.
Fase 2 - Evaluación y Selección del HSM
a) Investigación sobre alternativas y proveedores de HSM.
b) Gestión de pruebas de compatibilidad con el entorno SCADA.
c) Negociación y adquisición del HSM seleccionado.
d) Planificación y ejecución de la instalación y configuración inicial.
Fase 3 - Diseño de la Solución
a) Diseño de la arquitectura de integración del HSM en el entorno SCADA.
b) Definición de políticas de seguridad y gestión de claves.
c) Creación del plan de configuración y despliegue del HSM.
d) Evaluación de riesgos y potenciales mitigaciones.
Fase 4 - Configuración e Integración
a) Instalación física del HSM en el entorno SCADA.
b) Configuración del dispositivo según las políticas definidas.
c) Integración del HSM con el sistema SCADA (incluyendo aplicaciones y procesos relevantes).
d) Ejecución de las pruebas de integración.
e) Configuración de las herramientas de monitoreo.
f) Seguimiento post-despliegue para resolución de potenciales problemas.
Fase 5 - Pruebas y Validación
a) Ejecución de pruebas de funcionalidad y performance del HSM.
b) Ejecución de pruebas de integración con los sistemas SCADA.
c) Ejecución de pruebas de seguridad para corroborar el correcto desempeño del HSM.
d) Ejecución de las pruebas de integración.
Fase 6 - Documentación / Capacitación
a) Desarrollo del material de capacitación para el personal técnico / Usuarios finales.
b) Programación y ejecución de las sesiones de capacitación y entrenamiento.
c) Confección y entrega de la documentación técnica y operativa del HSM.
Fase 7 - Mantenimiento y Soporte
a) Generación del plan de mantenimiento regular para el HSM.
b) Establecimiento de un plan de soporte técnico continuo.
c) Actualización de configuraciones y políticas según sea necesario.

4.2.3 Diagrama de Gantt

El cronograma de la propuesta de intervención, que incluye las tareas, recursos, fases y duración de cada una de estas últimas, se encuentra detallado en la Figura 16.

Figura 16

Diagrama de Gantt



TAREA	INICIO	FIN	DURACIÓN (DÍAS)	RECURSOS	MES 1				MES 2				MES 3				MES 4				MES 5			
					W1	W2	W3	W4	W1	W2	W3	W4	W1	W2	W3	W4	W1	W2	W3	W4	W1	W2	W3	W4
Fase 1 - Tareas Preliminares																								
Definición de objetivos y alcance del proyecto.	1/3	1/10	6	PM / SAR																				
Identificación / documentación de los requisitos del HSM.	1/13	1/31	15	SAR																				
Evaluación del entorno SCADA preexistente y cómo se integrará el HSM.	1/5	2/5	23	SAR / SS																				
Elaboración del plan de proyecto detallado (incluyendo cronograma y presupuesto).	1/5	1/31	20	PM																				
Selección de proveedores de hardware / Definición de los criterios de evaluación.	1/13	2/7	20	SAR / SS																				
Fase 2 - Evaluación y Selección del HSM																								
Investigación sobre alternativas y proveedores de HSM.	2/3	2/14	10	SAR / SS																				
Gestión de pruebas de compatibilidad con el entorno SCADA.	2/10	2/14	5	SAN / IA																				
Negociacion y adquisición del HSM seleccionado.	2/10	2/21	10	SS																				
Planificación y ejecución de la instalación y configuración inicial.	2/17	2/28	10	SAR / SS																				
Fase 3 - Diseño de la Solución																								
Diseño de la arquitectura de integración del HSM en el entorno SCADA.	2/3	2/14	10	SAN / IA																				
Definición de políticas de seguridad y gestión de claves.	2/3	2/14	10	SAN / SS																				
Creación del plan de configuración y despliegue del HSM.	2/10	2/21	10	SAN / SAR																				
Evaluación de riesgos y potenciales mitigaciones.	2/17	2/28	10	SAR / NE / IA																				
Fase 4 - Configuración e Integración																								
Instalación física del HSM en el entorno SCADA.	3/3	3/14	9	SS / IA / NE																				
Configuración del dispositivo según las políticas definidas.	3/10	3/21	10	SS / IA / NE																				
Integración del HSM con el sistema SCADA (incluyendo aplicaciones y procesos relevantes).	3/17	3/28	10	SS / IA / NE																				
Ejecución de las pruebas de integración.	3/24	4/4	10	SS / IA / NE																				
Configuración de las herramientas de monitoreo.	3/24	4/4	10	IA / NE																				
Seguimiento post-despliegue para resolución de potenciales problemas.	3/24	4/4	10	SS / IA / NE																				
Fase 5 - Pruebas y Validación																								
Ejecución de pruebas de funcionalidad y performance del HSM.	3/24	4/4	10	SS / SAR																				
Ejecución de pruebas de integración con los sistemas SCADA.	3/24	4/4	10	SS / NE / SAR																				
Ejecución de pruebas de seguridad para corroborar el correcto desempeño del HSM.	3/24	4/4	10	SS / NE / SAR																				
Ejecución de las pruebas de integración.	3/24	4/4	10	SS / NE / IA																				
Fase 6 - Documentación / Capacitación																								
Desarrollo del material de capacitación para el personal técnico / Usuarios finales.	3/31	4/11	10	TR																				
Programación y ejecución de las sesiones de capacitación y entrenamiento.	4/7	4/11	5	TR/PM																				
Confección y entrega de la documentación técnica y operativa del HSM.	4/7	5/2	20	TR																				
Fase 7 - Mantenimiento y Soporte																								
Generación del plan de mantenimiento regular para el HSM.	4/14	5/9	20	TS/SS/IA																				
Establecimiento de un plan de soporte técnico continuo.	5/5	5/16	10	TS/IA																				
Actualización de configuraciones y políticas según sea necesario.	5/12	5/23	10	TS/IA																				

Nota. Figura de autoría propia.

Capítulo V - Evaluación del proyecto

5.1 Análisis FODA

Tal como se detalla en los capítulos previos, el aseguramiento de un entorno SCADA con una solución basada en PKI implica una serie de fortalezas, debilidades, oportunidades y amenazas, detalladas en la Figura 17:

Figura 17

Matriz FODA de la propuesta de intervención

Nota. Figura de autoría propia.

Fortalezas

PKI proporciona mecanismos *robustos* de cifrado, garantizando una comunicación segura entre los dispositivos SCADA y el sistema de control central, protegiendo los datos sensibles de filtraciones y/o alteraciones.

Asimismo, permite una *autenticación mejorada* entre los dispositivos SCADA y los usuarios, garantizando que sólo las entidades autorizadas puedan acceder al sistema. Esto ayuda a evitar accesos no autorizados y actividades maliciosas.

PKI permite la verificación de la *integridad* de los datos, garantizando que la información transmitida entre los componentes SCADA sea fiable y permanezca inalterada durante las comunicaciones, garantizando la fiabilidad y precisión del sistema en sí.

Por último, las soluciones PKI son ampliamente *escalables* y pueden adaptarse a entornos SCADA grandes y distribuidos, proporcionando seguridad en una amplia gama de dispositivos y ubicaciones.

5.1.1 Oportunidades

La implementación de una solución basada en PKI puede ayudar a las organizaciones a cumplir con las regulaciones de la industria y los estándares de ciberseguridad (*conformidad mejorada*) relacionados con la seguridad de SCADA, como NERC CIP, IEC 62443 y otros.

Asimismo, al aprovechar la PKI para una comunicación y autenticación seguras, los entornos SCADA pueden ser más resistentes a las ciber amenazas, tales como ataques del tipo man-in-the-middle, filtraciones de datos y los intentos de acceso no autorizados, convirtiéndolos en entornos *resilientes*.

Por último, las soluciones PKI pueden integrarse a menudo con la infraestructura y los sistemas de gestión SCADA existentes, ofreciendo amplias *facilidades de integración*, aprovechando las inversiones en tecnología y experiencia.

5.1.2 Debilidades

La implementación de una solución basada en PKI para la seguridad de SCADA puede ser *compleja* y requerir muchos recursos. Este tipo de solución requiere de una cuidadosa planificación, configuración y gestión de certificados digitales, claves y otros componentes criptográficos.

Asimismo, la implementación y el mantenimiento de una infraestructura PKI implican generalmente un *alto costo*, incluyendo hardware, software, personal y gastos de mantenimiento fijos. Este factor generalmente representa un impedimento para aquellas organizaciones con presupuestos limitados.

Los sistemas SCADA basados en PKI dependen de autoridades de certificación para la emisión y gestión de certificados digitales. Cualquier incidente o fallo de la infraestructura de la CA podría socavar la seguridad de todo el sistema, siendo altamente dependientes de esta última.

5.1.3 Amenazas

A pesar de sus características de seguridad, los entornos SCADA basados en PKI siguen siendo vulnerables a diversos *ciberataques*, tales como el comprometimiento de las claves, falsificación de certificados y otras amenazas internas. La supervisión y actualización continua de los componentes son esenciales para la correcta mitigación de estos riesgos.

Asimismo, cualquier interrupción de la infraestructura PKI, tal como la expiración, revocación o configuración incorrecta de los certificados, puede interrumpir las operaciones SCADA, provocando tiempos de inactividad significativos, impactando la operación en general.

Por otro lado, la incorrecta gestión de los certificados digitales, políticas de seguridad y otros *errores humanos* pueden favorecer la explotación de vulnerabilidades, comprometiendo la eficacia de la solución PKI.

5.2 Factores condicionantes

El éxito o fracaso en la adopción de una solución como la propuesta en entornos SCADA puede verse influido por diversos condicionantes. A continuación, se detallarán algunos de los factores clave que podrían influir en el resultado del proyecto.

5.2.1 Factores de éxito

a) Claridad en la definición de objetivos y requisitos: Es crucial definir claramente los objetivos y requisitos de la implementación de la PKI. Comprender las necesidades específicas de seguridad y las normas del entorno SCADA ayudará a garantizar que la solución PKI cumpla los objetivos de la organización.
b) Apoyo del equipo gerencial y los stakeholders: Obtener el apoyo de la dirección ejecutiva e implicar a las partes interesadas clave de los departamentos de IT, operaciones, seguridad y compliance puede facilitar el éxito de la implementación. La colaboración y el compromiso de todas las partes involucradas representan una gran ventaja para afrontar los retos y garantizar la alineación con las prioridades de la organización.
c) Planificación minuciosa y evaluación de riesgos: La planificación exhaustiva y la evaluación de riesgos son esenciales para identificar posibles retos, vulnerabilidades y estrategias de mitigación. Evaluar los riesgos asociados con la implementación de PKI, tales como la gestión de los certificados, escalabilidad y potenciales problemas de

interoperabilidad, puede ayudar a las organizaciones a desarrollar planes de implementación eficaces.

d) Gestión eficaz del cambio: La implementación de una solución PKI implica cambios significativos en los procesos, tecnologías y flujos de trabajo existentes. Las buenas prácticas de gestión del cambio, tales como la comunicación, capacitación y participación de las partes interesadas, pueden ayudar a minimizar la resistencia y garantizar una transición fluida hacia el nuevo sistema.
e) Escalabilidad y flexibilidad: Diseñar la infraestructura PKI teniendo en cuenta la escalabilidad y la flexibilidad es crucial para adaptarse a potenciales crecimientos en el futuro, y a la evolución de los requisitos de seguridad. La elección de arquitecturas escalables que puedan adaptarse a las necesidades cambiantes de la organización contribuirá a garantizar el éxito a largo plazo.
f) Cumplimiento de normativas y reglamentación vigente: Garantizar el cumplimiento de las normas y los requisitos reglamentarios pertinentes del sector, como NERC CIP, IEC 62443 y GDPR, será un factor esencial para el éxito de la implementación de la PKI. El alineamiento con las directrices de seguridad establecidas y las mejores prácticas puede ayudar a las organizaciones a evitar sanciones y daños a su reputación.

5.2.2 Factores de fracaso

a) Falta de apoyo ejecutivo y financiación: No contar con apoyo suficiente del equipo directivo, o bien no obtener una financiación acorde al proyecto, podrían representar un gran desafío para una implementación de este tipo de soluciones, pudiendo traducirse como escasez de recursos, prioridades contrapuestas, o bien resistencia al cambio, entre otros.
b) Planificación y ejecución deficientes: La planificación inadecuada, la estimación errónea de los recursos necesarios y posterior implementación precipitada pueden provocar retrasos severos en la ejecución del proyecto, incrementando sustancialmente los costos e impactando la calidad del resultado en general. Es de suma importancia que la evaluación de riesgos, la definición de requisitos y el establecimiento de los plazos sean analizados y estipulados correctamente, ya que el éxito de la implementación dependerá en gran parte de una correcta estimación.

c) Controles de seguridad insuficientes: Los controles de seguridad inadecuados, como algoritmos de cifrado débiles, gestión de claves inadecuadas y falta de capacidades de supervisión, pueden exponer la infraestructura PKI a filtraciones y vulnerar la seguridad del sistema en general. La falta y/o incorrecta aplicación de medidas de seguridad sólidas podría socavar la fiabilidad en el sistema y comprometer datos sensibles.
d) Problemas de interoperabilidad e integración: Los problemas de compatibilidad, las dificultades de interoperabilidad y la complejidad de la integración podrían dificultar la correcta implementación de soluciones PKI en entornos SCADA. Si no se garantiza una perfecta integración entre los sistemas, aplicaciones y dispositivos existentes, podrían producirse interrupciones operativas y problemas de compatibilidad.
e) Mala gestión de los certificados digitales: La gestión inadecuada de los certificados digitales (incluso aquellos ya caducados), los fallos en el proceso de revocación de certificados, o las relaciones de confianza mal configuradas, podrían provocar vulnerabilidades de seguridad y disrupciones en la operación. La aplicación de prácticas inadecuadas en la gestión del ciclo de vida de los certificados también representa un gran factor de riesgo, impactando directamente sobre la fiabilidad y eficacia de la infraestructura PKI.
f) Resistencia al cambio y falta de capacitación: La resistencia al cambio, la falta de concientización de los usuarios y una capacitación inadecuada pueden impedir la adopción y aceptación de la solución PKI entre los empleados, administradores y usuarios finales. Será crucial involucrar a los usuarios finales para abordar sus inquietudes, proporcionarles una capacitación adecuada y reforzar el valor agregado y las ventajas que la solución PKI traerá aparejadas. Omitir o no cumplir con alguno de estos factores podría obstaculizar la implementación y utilización adecuada de la solución.

5.3 Análisis de Costos

Para llevar a cabo la estimación de costos asociada al proyecto, fueron considerados aspectos tales como la correcta selección de los proveedores y el hardware requerido, su presencia en el mercado local, y respaldo a nivel global. Asimismo, fue adoptado un criterio temporal respecto a la disponibilidad del hardware en cuestión, considerando únicamente aquellos dispositivos con disponibilidad inmediata, o bien aquellos que requieran de un

proceso de importación / nacionalización específicos, estableciendo un periodo de hasta 90 días hábiles para ese fin. Los valores del equipamiento y servicios profesionales requeridos se encuentran detallados en las tablas debajo, junto con una serie de consideraciones para facilitar la interpretación de las propuestas.

5.3.1 Hardware

Las tablas 11, 12 y 13 contienen el detalle del hardware sugerido y valor aproximado para la ejecución de la propuesta en cuestión.

Tabla 11

Estimación Hardware / Vendor: Thales

Item	Cant.	Valor
Thales Luna Network Maximum Performance A790 HSM	1	≈ 45.000,00
TOTAL		**≈ 45.000,00**

Tabla 12

Estimación Hardware / Vendor: Utimaco

Item	Cant.	Valor
Utimaco CryptoServer General Purpose HSM	1	≈ 19.000,00
TOTAL		**≈ 19.000,00**

Tabla 13

Estimación Hardware / Vendor: EJBCA

Item	Cant.	Valor
KeyFactor Hardware Appliance HSM	1	≈ 9.500,00
TOTAL		**≈ 9.500,00**

5.3.2 Servicios Profesionales

La tabla 14 contiene el detalle de los recursos, horas/hombre y valores para la ejecución de la propuesta en cuestión.

Tabla 14

Estimación de Servicios Profesionales

Recurso	Cant. Horas	Valor Hora	Valor Total
Gerente de Proyecto (PM)	240	59	14.160,00
Arquitecto de Seguridad (SAR)	360	72	25.920,00
Analista de Seguridad (SAN)	80	52	4.160,00
Administrador de Infraestructura (IA)	560	61	34.160,00
Ingeniero de Networking (NE)	280	52	14.560,00
Analista de Soporte Técnico (TS)	240	28	6.720,00
Capacitador (TR)	120	37	4.440,00
Especialista SCADA (SS)	600	43	25.800,00
TOTAL			**129.920,00**

Consideraciones generales:

a) El valor de cada ítem se encuentra expresado en dólares estadounidenses.
b) Respecto a la provisión del hardware, al tratarse de componentes altamente especializados, para aplicaciones específicas, no se cuenta con la valuación exacta de mercado. El valor indicado en cada caso se trata de una aproximación, basada en las tendencias de precios globales.
c) Asimismo, la estimación de esfuerzos profesionales está basada en tendencias de precios globales para cada rol (se estima una carga horaria de 8 unidades diarias, totalizando 40 unidades por semana).
d) Los valores expresados no incluyen licencias, pólizas de garantía extendida, ni gastos relacionados con las operaciones de importación y manipulación de los ítems.

Capítulo VI - Conclusiones

6.1 Conclusiones y recomendaciones finales

Como se ha manifestado a lo largo del trabajo, la correcta protección y aislamiento de los entornos SCADA se ha transformado en un requerimiento crítico al momento de implementar este tipo de soluciones. En algunos casos, debido a la sensibilidad y/o tenor de las infraestructuras soportadas, se trata de un requerimiento completamente ineludible, donde proporcionar mecanismos de vanguardia es una condición *sine qua non*.

Asimismo, la creciente utilización de este tipo de tecnologías las ha convertido también en un objetivo de alto valor para los *hackers*. De acuerdo con lo que indica el estudio llevado a cabo por la consultora Forrester, "*el 56% de las organizaciones que utilizan soluciones SCADA reportaron algún tipo de violación durante el año 2018, y sólo el 11% indicó no haber sufrido ningún tipo de ataque*". Independientemente del motivo que persiga el atacante, es importante destacar que este tipo de acciones pueden causar daños realmente severos.

Tal cómo se detalla en el capítulo III, el modelo propuesto implementa un esquema de autenticación robusto, basado en PKI, que permite establecer un canal de comunicación cifrado entre los diversos componentes del entorno SCADA. Asimismo, la arquitectura de conectividad planteada aumenta el nivel de aislamiento entre los diversos componentes y/o áreas del entorno productivo, disminuyendo así los riesgos que podrían presentarse debido a la incorrecta segregación de los segmentos de red.

Por último, cabe mencionar una serie de recomendaciones basadas en los relevamientos y tareas de campo llevadas a cabo para la elaboración de este documento:

a) *Segregación de los niveles de red:* la correcta segmentación de la red, aislando los entornos SCADA/ICS de la red corporativa, permitirá reducir la propagación de malware y los movimientos laterales de los posibles atacantes una vez comprometida la red objetivo. Es recomendable contemplar las buenas prácticas acerca de segregación de redes y uso de VLAN's citadas en el capítulo III.
b) *Actualizaciones de Firmware y Software*: es recomendable contar con alguna plataforma que permita gestionar las actualizaciones de *software* en el equipamiento de misión crítica. Considerando que la aplicación de parches podría generar un impacto en el entorno

productivo, se recomienda programar cautelosamente el plan de actualizaciones, a modo de reducir el tiempo de parada al mínimo posible. La actualización del *firmware* en los dispositivos de campo plantea una complejidad aún mayor, considerando que este tipo de entornos alberga generalmente una gran variedad de componentes, provenientes de diversos fabricantes.

c) *Configuración por defecto de los dispositivos*: considerando la sensibilidad de la información gestionada dentro de los entornos SCADA, es recomendable eliminar/actualizar la configuración por defecto de los componentes. La configuración de fábrica, incluidas las contraseñas predeterminadas, podría permitir a los atacantes comprometer uno o más componentes del entorno, proporcionándoles además la facilidad de enumerar y comprometer fácilmente otros equipos emplazados en el mismo segmento de red.
d) *Administración de los niveles de acceso y cuentas de usuario*: Es fundamental evaluar el nivel de autorización y acceso a los sistemas SCADA. La creación de cuentas tipo "*root"* (nivel privilegiado), debe ser estrictamente supervisada, prestando especial atención en aquellas cuentas utilizadas por proveedores y/o personal externo. Este ítem engloba también a las cuentas de usuario creadas por defecto, que deberán ser eliminadas y/o renombradas.

6.2 Trabajos futuros relacionados

Como trabajos futuros por realizar serán citados algunos tópicos de interés para su desarrollo en otras propuestas ya que, debido a su extensión, o nivel de profundidad requerido, se encuentran fuera del alcance de esta propuesta.

Tal como se menciona en los capítulos 3 y 4 de este trabajo, tanto el algoritmo de encriptación elegido (PKI) como su entorno de aplicación (ambientes SCADA) cuentan con una serie de limitaciones, estrictamente relacionadas con la complejidad de su operación, consumo de recursos, falta de poder de cómputo, u otras limitaciones a nivel *hardware*. La lista que se presenta a continuación enumera algunos aspectos prioritarios, elegibles para análisis futuros:

Respecto al algoritmo PKI, sería necesario analizar las dependencias entre las autoridades de certificación y las autoridades de registro asociadas, evaluando algún esquema alternativo que permita que todo el conjunto opere correctamente. Asimismo, podría explorarse la integración entre una solución del tipo cadena de bloques (del inglés "*Blockchain*") y PKI, pudiendo explotar los beneficios de ambas tecnologías, utilizando, por ejemplo, PKI para el proceso de autenticación, y cadena de bloques para fines de auditoría y seguimiento de los certificados.

Sobre el entorno de aplicación, debería evaluarse la posibilidad de desarrollar alguna solución de autenticación multifactorial (MFA, del inglés "*Multi-Factor Authentication"*) que permita incrementar el nivel de seguridad, principalmente para los operadores con acceso privilegiado.

Respecto al hardware, algunos de los componentes del entorno SCADA, tales como las RTU's, poseen una baja capacidad de cómputo. Sería interesante evaluar la adopción de dispositivos complementarios, que puedan anexarse a los dispositivos de campo existentes, incrementando su potencia de cómputo, y extendiendo también la vida útil de los mismos.

Por último, debería evaluarse el nivel de tolerancia a fallos y resiliencia en ambientes de misión crítica, tales como los entornos SCADA. El análisis de soluciones de alta disponibilidad (o HA, del inglés *"High Availability"*), capaces de tolerar y gestionar fallos de manera automatizada, podrían considerarse vitales para garantizar la operación ininterrumpida de este tipo de ambientes.

Referencias Bibliográficas

Alanazi, M., Mahmood, A., & Morshed Chowdhury, M. J. (2022). SCADA vulnerabilities and attacks: A review of the state-of-the-art and open issues. *Department of Computer Science and Information Technology School of Engineering and Mathematical Science La Trobe University*, 29.

Bartman, T., & Carson, K. (05 de Febrero de 2016). Securing Communications for SCADA and Critical Industrial Systems. *Sensible Cybersecurity for Power Systems: A Collection of Technical Papers Representing Modern Solutions*. Obtenido de https://cms-cdn.selinc.com/assets/Literature/Publications/Technical%20Papers/6678_SecuringCommunications_TB_20160205_Web3.pdf?v=20190403-203429-

Beaver Cheryl., G. D. (Marzo de 2002). Key Management for SCADA. *SAND REPORT*.

Cutanda, D. (7 de Abril de 2014). *Fundamentos sobre Certificados Digitales – El estándar X.509 y estructura de certificados*. Fonte: Security Artwork: https://www.securityartwork.es/2014/04/07/fundamentos-sobre-certificados-digitales-el-estandar-x-509-y-estructura-de-certificados/

Djiev, S. (2003). Industrial Networks for Communications and Controls. *Elements of Industial Automation*. Obtenido de https://data.kemt.fei.tuke.sk/SK_rozhrania/en/industrial%20networks.pdf

Fortinet. (2019). *Independent Study - Pinpoint Significant SCADA/ICS Security Risks.* California: Fortinet. Obtenido de https://www.fortinet.com/content/dam/fortinet/assets/white-papers/WP-Independent-Study-Pinpoints-Significant-Scada-ICS-Cybersecurity-Risks.pdf

Gbs. (2016). *PKI Fundamentals.* Manchester: Group Business Software Europa GmbH. Fonte: https://www.gbs.com/gb/whitepapers?file=files/whitepaper/email/en/PKI_Fundamentals.pdf

Gratz, M. (Junio de 2021). *Components of a PKI, Part 5: Hardware Security Modules.* Fonte: Ravenswood Technology Group: https://www.ravenswoodtechnology.com/components-of-a-pki-part-5/

ICCCERT. (2016). *Recommended Practice: Improving Industrial Control System Cybersecurity with Defense-in-Depth Strategies.*

Kamlofsky, J. (2019). *Seguridad en redes industriales - Clave para la Ciberseguridad de las infraestructuras críticas.* Mar del Plata: Universidad FASTA.

Kamlofsky, J., Colombo, H. R., Sliafertas, M., & Pedernera, J. (2015). Un enfoque para disminuir los efectos de los ciber-ataques a las infraestructuras críticas.

Krutz, R. L. (2006). *Securing SCADA Systems.* Indianapolis, IN, United States: Wiley Publishing, Inc.

Kuhn, R. H.-J. (2001). *Introduction to Public Key Technology and the Federal PKI Infrastructure.* National Institute of Standards and Technology, U.S. Department of Commerce. Gaithersburg: NIST. Fonte: https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-32.pdf

Lucena López, M. J. (2011). *Criptografía y Seguridad en Computadores.* Jaén: Universidad de Jaén.

Nccic / Ics-Cert. (2016). Recommended Practice: Improving Industrial Control System Cybersecurity with Defense-in-Depth Strategies. 49.

Paganini, L. (15 de Julio de 2020). *SCADA & security of critical infrastructures [updated 2020]*. (Infosec, Editor, P. Luigi, Productor, & Infosec) Obtenido de Infosec Institute: https://resources.infosecinstitute.com/topic/scada-security-of-critical-infrastructures/

Rodriguez Penin, A. (2013). *Sistemas SCADA* (3 ed.). (A. G. Editor, Ed.) México, México DF, México: MARCOMBO S.A.

Rojko, A. (2017). Industry 4.0 Concept: Background and Overview. *International Journal of Interactive Mobile Technologies*, 90.

Rountree, D. (2011). *Security for Microsoft Windows Administrators.* Burlington: Elsevier.

SafeNet. (2010). *Introduction to PKI & SafeNet Luna Hardware Security Modules with Microsoft Windows.* SafeNet.

Saxena, A., Pal, O., Saquib, Z., & Patel, D. (2010). Customized PKI for SCADA System. *Journal of Advanced Networking and Applications*, 282-289.

Secretaría de Modernización Administrativa. (2016). *Infraestructura de Firma Digital de la República Argentina - Perfiles de los certificados y de las listas de certificados revocados.* Ministerio de Modernización - República Argentina, Secretaría de Modernización Administrativa. Buenos Aires: Ministerio de Modernización. Fonte: http://servicios.infoleg.gob.ar/infolegInternet/anexos/265000-269999/266312/res399-3.pdf

Ssl. (6 de Septiembre de 2023). A guide to PKI Protection using Hardware Security Modules. *Ssl.com*. Fonte: https://www.ssl.com/article/a-guide-to-pki-protection-using-hardware-security-modules-hsm/

St Denis, T. J. (2007). *Cryptography for Developers.* Rockland, Maine, USA: Syngress Publishing, Inc.

Talens-Oliag, S. (s.d.). *Introducción a los certificados digitales*. Fonte: Universitat de Valencia: https://www.uv.es/sto/articulos/BEI-2003-11/certificados_digitales.html

Valdiviezo Echeverría, T. A. (2012). *Análisis de la tecnología PKI y su aplicación en el aseguramiento de los servicios corporativos WWW, FTP y HTTP.* Fonte: http://dspace.espoch.edu.ec/bitstream/123456789/2915/1/98T00030.pdf

Zwicke, A. (2003). An Introduction to Modern Cryptosystems. *Global Information Assurance Certification Paper*.

Anexo I: Acrónimos

3DES Triple DES

ADP Producción Digital Avanzada (del inglés *Advanced Digital Production)*

AES Estándar de Cifrado Avanzado (del inglés: *Advanced Encryption Standard*)

ANSI Instituto Nacional de Estándares Americanos (del inglés: *American National Standards Institute*)

ASN-1 Sintaxis Abstracta Uno (del inglés *Abstract Sintax One*)

CA Autoridad de Certificación (del inglés: *Certification Authority*)

CAD Diseño Asistido por Computadora (del inglés: *Computer Aided Design*)

CAE Ingeniería Asistida por Computadora (del inglés: *Computer Aided Engineering*)

CAM Manufactura Asistida por Computadora (del inglés: *Computer Aided Manufacturing*)

CBC Encadenado de Bloques de Cifrado (del inglés: *Cipher-block chaining*)

CITT Comité Consultivo Internacional Telegráfico y Telefónico (del inglés: *Consultative Committee for International Telegraphy and Telephony*)

CIM Sistema de Manufactura Computarizada (del inglés: *Computer Integrated Manufacturing*)

CNC Control Numérico Computarizado (del inglés: *Computer Numerical Control*)

CPS Sistemas Cyber Físicos (del inglés: *Cyber Physical Systems*)

CRL Lista de revocación de certificados **(**del inglés: *Certificate Revocation List*)

CSR Solicitud de Firma de Certificado (del inglés: *Certificate Signing Request*)

DER Reglas de Codificación Distinguible (del inglés: *Distinguished Encoding Rules*)

DES Estándar de Cifrado de Datos (del inglés: *Data Encryption Standard*)

DCCS Sistema de Control Computarizado Distribuido (del inglés: *Distributed Computer Control System*)

DDC Controlador Digital Directo (del inglés: *Digital Direct Controller*)

DMZ Zona Desmilitarizada (del inglés: *Demilitarized Zone*)

ECB Libro de Código Electrónico (del inglés: *Electronic Code Book*)

ERP Sistema de Planificación Empresarial (del inglés: *Enterprise Resource Planning*)

FIPS Estándares Federales de Procesamiento de la Información (del inglés: *Federal Information Processing Standards*)

GDPR Reglamento General de Protección de Datos (del inglés: *General Data Protection Regulation*)

HA Alta Disponibilidad (del inglés: *High Availability*)

HMI Interfaz Humano-Máquina (del inglés: *Human-Machine Interface*)

HSM Módulo de Seguridad de Hardware (del inglés: *Hardware Security Module*)

HTTPS Protocolo de Transferencia de Hipertexto sobre SSL (del inglés: *Hypertext Transfer Protocol over SSL*)

ICS Sistemas de Control Industrial (del inglés: *Industrial Control Systems*)

IEC Comisión Electrotécnica Internacional (del inglés: *International Electrotechnical Commission*)

IDEA Algoritmo Internacional de Cifrado de Datos (del inglés: *International Data Encryption Algorithm*)

IOT Internet de las Cosas (del inglés: *Internet of Things*)

ISO Organización Internacional de Normalización (del inglés: *International Organization for Standardization*)

IT Tecnología de Información (del inglés: *Information Technology*)

LAN Red de Área Local (del inglés: *Local Area Network*)

MAP Protocolo de Acceso al Medio (del inglés: *Media Access Protocol*)

MFA Autenticación Multifactorial (del inglés: *Multi-Factor Authentication*)

MES Sistema de Ejecución de Fabricación (del inglés: *Manufacturing Execution System*)

MTU Unidad Terminal Maestra (del inglés: *Master Terminal Unit*)

NBS Bureau Nacional de Estándares (del inglés: *National Bureau of Standards*)

NC Control Numérico (del inglés: *Numerical Control*)

NCCIC Centro Nacional de Seguridad Cibernética y de Integración de Comunicaciones (del inglés: *National Cybersecurity and Communications Integration Center*)

NERC-CIP Corporación Norteamericana para la Confiabilidad Eléctrica - Protección de la Infraestructura Crítica (del inglés: *North America Electric Reliability Corporation - Critical Infraestructure Protection*)

NIST Instituto Nacional de Estándares y Tecnología (del inglés: *National Institute of Standards and Technology*)

NSA Agencia Nacional de Seguridad **(**del inglés: *National Security Agency***)**

OID Identificador de Objeto (del inglés: *Object Identifier*)

OSI Interconexión de Sistemas Abiertos (del inglés: *Open Systems Interconnection*)

OT Tecnología Operacional (del inglés: *Operational Technology*)

PGP Privacidad Bastante Buena (del inglés: *Pretty Good Privacy*)

PKI Infraestructura de Clave Pública (del inglés: *Public Key Infrastructure*)

PLC Controlador Lógico Programable (del inglés: *Programmable Logic Controller*)

PoE Alimentación a través de Ethernet (del inglés: *Power Over Ethernet*)

RC4 Algoritmo Rivest Cipher, versión 4

RC5 Algoritmo Rivest Cipher, versión 5

RSA Algoritmo Rivest Shamir Adelman

RTU Unidad Terminal Remota (del inglés: *Remote Terminal Unit*)

SCADA Control de Supervisión y Adquisición de Datos (del inglés: *Supervisory Control and Data Acquisition*)

SDN Redes definidas por software (del inglés: *Software Defined Networks*)

SPOF Punto de Falla Único (del inglés: *Single Point of Failure*)

SSL Capa de Sockets Seguros (del inglés: *Secure Sockets Layer*)

SSO Inicio de Sesión Único (del inglés: *Single Sign On*)

TCP/IP Protocolo de Control de Transmisión / Protocolo de Internet (del inglés: *Transfer Control Protocol / Internet Protocol*)

TLS Seguridad de la Capa de Transporte (del inglés: *Transport Layer Security*)

VLAN Red de Área Local Virtual (del inglés: *Virtual Local Area Network*)

WEF Foro Económico Mundial (*del inglés: World Economic Forum*)

WEP Privacidad Equivalente a Cableado (*del inglés: Wired Equivalent Privacy*)

WPA Acceso Wi-Fi Protegido (*del inglés: Wi-Fi Protected Access*)

WPA2 Acceso Wi-Fi Protegido, versión 2 (*del inglés: Wi-Fi Protected Access 2*)

Anexo II: Product brief – Dispositivos HSM Thales

Anexo III: Product brief – Dispositivos HSM Utimaco

Solution Leaflet

General Purpose Hardware Security Modules

Data security is becoming increasingly crucial in infrastructures and organizations throughout various industries, and this brings a range of obligations and responsibilities related to how this information is processed, stored, and used. General Purpose Hardware Security Modules (HSMs) protect sensitive assets against disclosure, manipulation, and misuse.

Utimaco's General Purpose HSMs have been designed to meet the needs and standards of a wide range of use cases and market segments in a highly reliable and secure manner.

With a rich history of 40 years in hardware-based security, Utimaco has honed its expertise to develop and optimize a family of General Purpose HSMs. These models cater to different performance and physical security levels, making them a reliable choice across industries.

Centrally monitor and manage your Utimaco's General Purpose HSMs with our u.trust 360 Solution.

u.trust 360

- Single pane of glass for management and monitoring
- Real-time alerts and status updates
- Role Based Access Control model (RBAC) for users and HSMs
- Logically group, monitor and manage 100s of HSMs

On-Premises HSMs

- u.trust Anchor General Purpose HSM
- CryptoServer General Purpose HSM CSe-Series
- CryptoServer General Purpose HSM

HSM-as-a-Service

- CryptoServer Cloud

Creating Trust in the Digital Society

utimaco®

Anexo IV: Product brief – Dispositivos HSM EJBCA

Anexo V: Diagrama de Gantt

SCADA_PKI

TAREA	INICIO	FIN	DURACIÓN (DÍAS)	RECURSOS	MES 1				MES 2				MES 3				MES 4				MES 5			
					W1	W2	W3	W4	W1	W2	W3	W4	W1	W2	W3	W4	W1	W2	W3	W3	W1	W2	W3	W4
Fase 1 - Tareas Preliminares																								
Definición de objetivos y alcance del proyecto.	1/3	1/10	6	PM / SAR																				
Identificación / documentación de los requisitos del HSM.	1/13	1/31	15	SAR																				
Evaluación del entorno SCADA preexistente y cómo se integrará el HSM.	1/5	2/5	23	SAR / SS																				
Elaboración del plan de proyecto detallado (incluyendo cronograma y presupuesto).	1/3	1/31	20	PM																				
Selección de proveedores de hardware / Definición de los criterios de evaluación.	1/13	2/7	20	SAR / SS																				
Fase 2 - Evaluación y Selección del HSM																								
Investigación sobre alternativas y proveedores de HSM.	2/3	2/14	10	SAR / SS																				
Gestión de pruebas de compatibilidad con el entorno SCADA.	2/10	2/14	5	SAN / IA																				
Negociacion y adquisición del HSM seleccionado.	2/10	2/21	10	SS																				
Planificación y ejecución de la instalación y configuración inicial.	2/17	2/28	10	SAR / SS																				
Fase 3 - Diseño de la Solución																								
Diseño de la arquitectura de integración del HSM en el entorno SCADA.	2/3	2/14	10	SAN / IA																				
Definición de políticas de seguridad y gestión de claves.	2/3	2/14	10	SAN / SS																				
Creación del plan de configuración y despliegue del HSM.	2/10	2/21	10	SAN / SAR																				
Evaluación de riesgos y potenciales mitigaciones.	2/17	2/28	10	SAR / NE / IA																				
Fase 4 - Configuración e Integración																								
Instalación física del HSM en el entorno SCADA.	3/3	3/14	9	SS / IA / NE																				
Configuración del dispositivo según las políticas definidas.	3/10	3/21	10	SS / IA / NE																				
Integración del HSM con el sistema SCADA (incluyendo aplicaciones y procesos relevantes).	3/17	3/28	10	SS / IA / NE																				
Ejecución de las pruebas de integración.	3/24	4/4	10	SS / IA / NE																				
Configuración de las herramientas de monitoreo.	3/24	4/4	10	IA / NE																				
Seguimiento post-despliegue para resolución de potenciales problemas.	3/24	4/4	10	SS / IA / NE																				
Fase 5 - Pruebas y Validación																								
Ejecución de pruebas de funcionalidad y performance del HSM.	3/24	4/4	10	SS / SAR																				
Ejecución de pruebas de integración con los sistemas SCADA.	3/24	4/4	10	SS / NE / SAR																				
Ejecución de pruebas de seguridad para corroborar el correcto desempeño del HSM.	3/24	4/4	10	SS / NE / SAR																				
Ejecución de las pruebas de integración.	3/24	4/4	10	SS / NE / IA																				
Fase 6 - Documentación / Capacitación																								
Desarrollo del material de capacitación para el personal técnico / Usuarios finales.	3/31	4/11	10	TR																				
Programación y ejecución de las sesiones de capacitación y entrenamiento.	4/7	4/11	5	TR/PM																				
Confección y entrega de la documentación técnica y operativa del HSM.	4/7	5/2	20	TR																				
Fase 7 - Mantenimiento y Soporte																								
Generación del plan de mantenimiento regular para el HSM.	4/14	5/9	20	TS/SS/IA																				
Establecimiento de un plan de soporte técnico continuo.	5/5	5/16	10	TS/IA																				
Actualización de configuraciones y políticas según sea necesario.	5/12	5/23	10	TS/IA																				