MÁSTER EN SEGURIDAD DE LAS TECNOLOGÍAS DE LA INFORMACIÓN Y DE LAS COMUNICACIONES

Curso Académico 2017/2018

Trabajo Fin de Máster

AD-HOC INCIBE - PROTECCIÓN EN INFRAESTRUCTURAS CRÍTICAS

INSTITUTO NACIONAL DE CIBERSEGURIDAD

Junio de 2018

Autor: Miguel Calvo Matalobos

Tutor: Marco Antonio Lozano Merino

RESUMEN

La Protección de Infraestructuras Críticas es un marco que engloba gran cantidad de aspectos, tanto en materia normativa, leyes y regulaciones, como en la configuración del equipamiento técnico y la estructuración de la topología de red en este tipo de organizaciones, centrándose en todo momento en la ciberseguridad.

A pesar de que en el pasado no se ha enfatizado demasiado en el cumplimiento y/o la regulación de las Infraestructuras Críticas (IC), mediante sin las cuales la sociedad no podría mantener el ritmo de vida que ha mantenido anteriormente (entre las que se encuentran las potabilizadoras de agua, las centrales nucleares, las eléctricas, etc.), en estos últimos años, se está apreciando un gran aumento en la preocupación por mantener, proteger y supervisar de manera exhaustiva estas infraestructuras para que, en todo momento, puedan hacer frente a cualquier tipo de adversidad.

La Ley de Protección de Infraestructuras Críticas (Ley 8/2011 [1]), respaldada por las Disposiciones 18439 del 15 de noviembre de 2011 [2] y 10060 del 18 de septiembre de 2015 [3], en las cuales se establecen los contenidos mínimos de los Planes de Seguridad del Operador y los Planes de Protección Específicos conforme a lo dispuesto en el Real Decreto 704/2011, de 20 de mayo, por el que se aprueba el Reglamento de protección de las infraestructuras críticas [4], es, a día de hoy, la regulación aplicable a cualquier Infraestructura Crítica ubicada en el territorio español y vinculada a los sectores estratégicos de la administración, el espacio, la industria nuclear, la industria química, las instalaciones de investigación, el agua, la energía, la salud, las tecnologías de la información y las comunicaciones, el transporte, la alimentación y el sistema financiero y tributario. Esta Ley obliga a cumplir con determinados aspectos burocráticos, así como a documentar y llevar a cabo el inventariado de activos y elementos que soportan la Infraestructura Crítica, las medidas de seguridad implantadas y/o a implantar en ellas, la realización de un análisis de riesgos, etc.

Por otro lado, además del marco normativo, existen recomendaciones y buenas prácticas aplicables a los Sistemas de Control Industrial (utilizados en las IC para administrar, ordenar, dirigir y/o regular el comportamiento de otros sistemas o maquinaria de forma automática) de forma más técnica. Entre estas acciones y disposiciones, con las que se consigue una mejora significativa de la seguridad y la confiabilidad en las IC, pueden incluirse el uso de cortafuegos, la segmentación y segregación de la red, la aplicación de una defensa en profundidad, la capacidad de los sistemas para tolerar fallos, el empleo de una autenticación y una autorización fuerte, así como el desarrollo de los planes de respuesta a incidentes y la recuperación del sistema, entre otros.

Palabras clave: Protección en Infraestructuras Críticas, Ciberseguridad Industrial, Ley PIC, Sistemas de Control Industrial, SCADA, DCS, PLC.

ABSTRACT

Critical Infrastructure Protection is a field that involves a plethora of different aspects such a regulation, law and compliance; technical infrastructure configuration and network topology definition.

Although in the past there has not been a significant interest in defining specific regulations for this kind of infrastructures or in complying with existing ones, even when societies could not keep their way of life without this kind of infrastructures (examples such as water purification facilities, nuclear and power plants, etc. must be pointed), this situation is evolving quickly. Recent natural disasters, terrorist threats or state-sponsored cyber-attacks are increasing the concern for exhaustively supervise, control and protect these infrastructures ensuring they can cope with any adversity with proper guarantees for citizens.

The Spanish Law for Critical Infrastructure Protection (Law 8/2011 [1]) is supported by Provisions 18439 of November 15, 2011 [2] and 10060 of September 18, 2015 [3]. At the same time, the minimum contents of Operator Security and Specific Protection Plans are established in accordance with the provisions of Royal Decree-Law 704/2011, of May 20, by which the regulation for the Critical Infrastructure Protection [4] is approved. Currently, the Law 8/2011 is the applicable regulation to any Critical Infrastructure located in the Spanish territory and link to the strategic sectors of administration, space, nuclear industry, chemical industry, research centres, water, energy, health, information and communication technologies, transport, food and the financial and tax system. This Law forces to comply with certain bureaucratic aspects, as well as to document and carry out the inventory of the assets and elements that support the Critical Infrastructure, the implemented security measures and/or to be implemented, the accomplishment of a risk analysis and so on.

In addition to this regulatory framework, there are recommendations and good practices applicable to Industrial Control Systems (used at Critical Infrastructures to automatically manage, order, run and/or regulate the other systems or machine behaviours) from a more technical perspective. With these actions and provisions, a significant improvement of the security and reliability of the CI can be achieved. They may include the use of firewalls, network segmentation and segregation, the application of defense-in-depth, the capacity of the systems to put up with failures, the use of strong authentication and authorization, as well as the development of the response to incidents and the recovery of the system plans, among others.

Keywords: Critical Infrastructure Protection, Industrial Cybersecurity, CIP Law, Industrial Control Systems, SCADA, DCS, PLC.

ÍNDICE

ÍNDICE DE FIGURAS

ÍNDICE DE TABLAS

CAPÍTULO 1. INTRODUCCIÓN Y OBJETIVOS DEL TRABAJO

1.1. Contexto del TFM

En los últimos años, la protección de las infraestructuras críticas en materia informática ha despertado la preocupación de las grandes organizaciones y de los gobiernos, al quedar de manifiesto que, cada vez más e impulsada por las tecnologías emergentes y la automatización de los procesos, están siendo el objetivo de gran parte de los ciberataques orquestados por delincuentes informáticos.

Cuando se habla de Protección de Infraestructuras Críticas (PIC), lo más razonable, es pensar que se trata de grandes organizaciones, que disponen de gran cantidad de recursos (materiales, económicos y/o humanos), pero esto no es siempre así, también existen pequeñas o medianas empresas encargadas de administrar Infraestructuras Críticas. Por lo tanto, es de gran importancia, independientemente del tamaño de la empresa u organización, cumplir con las obligaciones, la normativa legal y las recomendaciones en materia de ciberseguridad industrial cuando se opera en Infraestructuras Críticas.

Además de cumplir con las obligaciones y leyes dictadas por los diferentes estados, es imprescindible una correcta estructuración de la topología de red dentro de la empresa, así como la instalación y la correcta configuración de dispositivos que permitan disuadir y minimizar la probabilidad de que se produzca un ataque informático y de los sistemas de control industrial, llevando a cabo, periódicamente, gestiones y evaluaciones de los riesgos que puedan surgir.

1.2. Objetivos

1.2.1. Objetivos generales

El principal objetivo de este trabajo es analizar y realizar un estudio sobre el estado actual de las Infraestructuras Críticas en materia de protección, así como las obligaciones y deberes que tienen las distintas organizaciones, dependiendo del sector al que pertenezcan, para cumplir con las distintas leyes impuestas por el estado español.

Así mismo, de forma teórica, se estudiarán los aspectos más importantes a considerar para asegurar los sistemas de control industrial, la gestión y evaluación de riesgos en las

distintas Infraestructuras Críticas y los programas de seguridad, incluyendo los beneficios, consecuencias, políticas y procedimientos, etc.

1.2.2. Objetivos específicos

Se tratará, en primer lugar, de adquirir un conocimiento previo de la protección en Infraestructuras Críticas y del estado actual en materia de leyes y regulaciones en España, adquiriendo las competencias específicas imprescindibles para el desarrollo del trabajo. Se estudiará en profundidad el cumplimiento normativo en materia de protección de Infraestructuras Críticas, desarrollando y comprendiendo la Ley de Protección de Infraestructuras Críticas (Ley 8/2011 de 28 de abril, por la que se establecen medidas para la protección de Infraestructuras Críticas [1], vulgarmente conocida como Ley PIC), los planes sectoriales que surgen a partir de esta Ley, así como el Plan de Protección Específico (PPE), el Plan de Seguridad del Operador (PSO) y el Análisis de Riesgos requerido.

Una vez adquiridos estos conocimientos previos, se procederá al estudio de los sistemas de control industrial, completando la investigación con las principales consideraciones que deben tenerse en cuenta: la arquitectura, la distribución de los sistemas de control, sistemas SCADA (*Supervisory Control and Data Acquisition*), etc. Además, se determinará y contextualizará el proceso de gestión y evaluación de riesgos y los programas de seguridad, detallando los beneficios que estos aportan, las consecuencias de las brechas de seguridad y la definición de las políticas y procedimientos.

1.3. Planificación del trabajo

El trabajo comienza con un estudio general del estado actual de la protección en Infraestructuras Críticas en España, así como unas primeras pinceladas introductorias, en las que se explican y detallan las definiciones y conceptos básicos más relevantes que deben ir surgiendo a lo largo del desarrollo de este trabajo.

Una vez adquiridos los conocimientos necesarios, se investigan y estudian en profundidad las obligaciones en materia legal para cumplir con las normativas, regulaciones y leyes españolas en las diferentes Infraestructuras Críticas, según el servicio y criticidad de este.

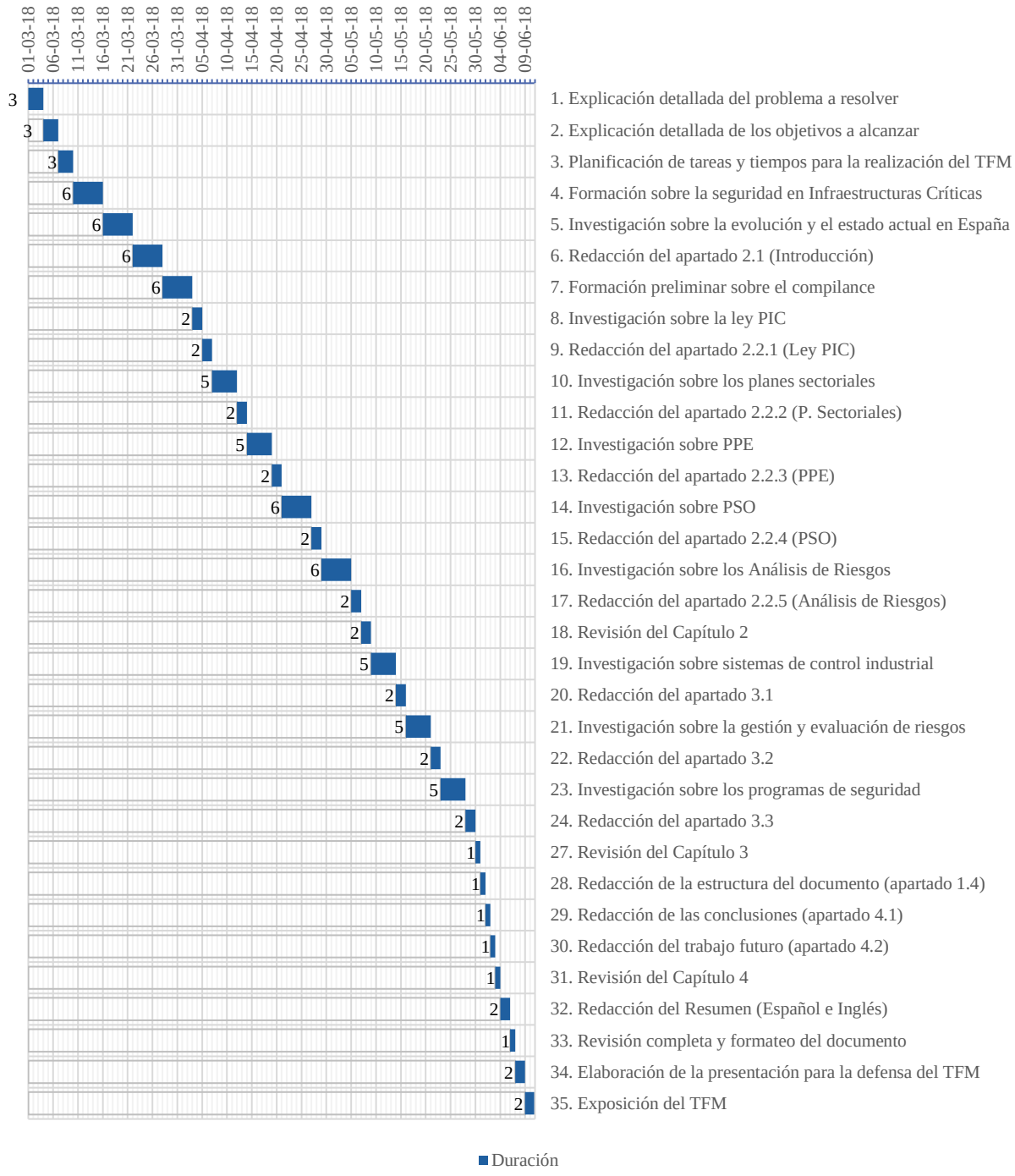


Figura 1.1: Diagrama de Gantt de la planificación del trabajo.

Tras el estudio en profundidad de los términos legales y obligaciones, debe llevarse a cabo una investigación de la evolución, sectores y distintos componentes en materia de sistemas de control industrial, así como la gestión y evaluación de riesgos y su proceso. También es necesario conocer e investigar sobre los programas de seguridad y el aporte de estos (beneficios, consecuencias, etcétera).

La planificación de las tareas a realizar y la estimación de la duración de estas se detallan en el diagrama de Gantt expuesto en la Figura 1.1.

1.4. Estructura del documento

El resto de este documento se estructura de la manera que sigue. El Capítulo 2, incluye una pequeña introducción a la Protección en Infraestructuras Críticas, así como los conceptos básicos necesarios para comprender el resto del capítulo, la evolución en materia normativa para estos entornos y su estado actual. En esta misma sección, se exploran las necesidades y requerimientos necesarios para un correcto cumplimiento de la legislación vigente en materia de Protección de Infraestructuras Críticas en España (seguimiento de los Planes Estratégicos Sectoriales, creación del Plan de Seguridad del Operador y el Plan de Protección Específico, cumplimiento de los Planes de Apoyo Operativos, realización del Análisis de Riesgos, etc.).

En el Capítulo 3, se presentan algunos de los Sistemas de Control Industrial del mercado y se exponen determinadas formas de gestión y evaluación de riegos sobre ellos. En este mismo capítulo, se muestran ciertas recomendaciones y buenas prácticas a la hora de diseñar y desplegar arquitecturas de seguridad para los Sistemas de Control Industrial. Por último, se materializan (utilizando el ejemplo de una fábrica de refrescos) estas recomendaciones.

En el Capítulo 4, se comentan las conclusiones y cuestiones surgidas tras el desarrollo del trabajo, así como las principales líneas a seguir tras esta investigación.

CAPÍTULO 2. PROTECCIÓN EN INFRAESTRUCTURAS CRÍTICAS

2.1. Introducción a la Protección de Infraestructuras Críticas

La preocupación de los gobiernos sobre la forma en la que hacer frente a las amenazas que surgen en los últimos años como consecuencia de la aparición de nuevas tecnologías y el temor de empresas y organizaciones a la posible pérdida de activos, tiempo de fabricación, etc. causados por ataques propiciados por delincuentes informáticos, han hecho que se preste una mayor importancia a la Protección de Infraestructuras Críticas (PIC).

Cuando se habla de Infraestructuras Críticas, tiende a pensarse en empresas u organizaciones de gran tamaño, encargadas de realizar procesos de gran envergadura, contando, para ello, con gran cantidad de recursos (materiales, económicos y/o humanos). Pero, la realidad es otra, existiendo, además de estas empresas de gran tamaño, otras mucho más pequeñas y de recursos más limitados encargadas de la gestión de Infraestructuras Críticas. Estas entidades se encuentran en clara desventaja a la hora de lograr el cumplimiento que exigen las distintas leyes de protección de infraestructuras del país en el que operan. Por lo tanto, el tamaño de las empresas y organizaciones que operan con infraestructuras críticas no es relevante a la hora de aplicar medidas de seguridad y cumplir las respectivas leyes.

Es habitual que la protección de Infraestructuras Críticas esté regulada desde un marco legislativo, imponiendo exigencias de obligado cumplimiento a las distintas entidades y que, desde este marco, se extienda a los niveles inferiores (hasta llegar a la protección de maquinaria, sensores, etc.). Este método, origina que el valor impuesto en la dirección de las empresas u organizaciones termine disminuyendo su capacidad a medida que baja por los distintos niveles, haciendo que las medidas no aporten el valor requerido y/o se realicen acciones necesarias únicamente para lograr el cumplimiento legislativo exigido [5].

2.1.1. Definiciones y conceptos básicos

Las **Infraestructuras Críticas** (IC), son, según el Artículo 2, Apartado e) de la Ley 8/2011 de 28 de abril, por la que se establecen medidas para la protección de Infraestructuras Críticas [1], "*las infraestructuras estratégicas cuyo funcionamiento es indispensable y no permite soluciones alternativas, por lo que su perturbación o destrucción tendría un grave*

impacto sobre los servicios esenciales.", o de una forma más vulgar, aquellas sin las cuales una sociedad no puede mantener el ritmo de vida que ha mantenido con anterioridad y que deben ser mantenidas, protegidas y supervisadas de forma exhaustiva para que siempre puedan hacer frente a cualquier tipo de adversidad, ya que su funcionamiento es indispensable y no permite soluciones alternativas. En comparación, las **Infraestructuras Estratégicas**, según el Artículo 2, Apartado d) de la Ley 8/2011 de 28 de abril, por la que se establecen medidas para la protección de Infraestructuras Críticas [1], que dice así: "*las instalaciones, redes, sistemas y equipos físicos y de tecnología de la información sobre las que descansa el funcionamiento de los servicios esenciales.*", son aquellos elementos o instalaciones relacionados con la tecnología de la información que sostienen los servicios esenciales de un país, Comunidad Autónoma, etc.

Por otra parte, la **ciberseguridad** es el conjunto de herramientas, políticas, conceptos, salvaguardas, directrices, métodos de gestión de riesgos, acciones, formación, buenas prácticas y tecnologías que pueden aplicarse para la protección de activos de una empresa u organización y los usuarios del mismo entorno.

Si se interpreta la definición expuesta en el Artículo 2, Apartado a) de la Ley 8/2011 de 28 de abril, por la que se establecen medidas para la Protección de Infraestructuras Críticas [1] ("*Servicio esencial: el servicio necesario para el mantenimiento de las funciones sociales básicas, la salud, la seguridad, el bienestar social y económico de los ciudadanos, o el eficaz funcionamiento de las Instituciones del Estado y las Administraciones Públicas.*"), puede concluirse que los **Servicios Esenciales** son aquellos que permiten, a una sociedad, mantenerse con unas funciones sociales mínimas, así como un correcto funcionamiento de las administraciones públicas.

Por lo tanto, y tras estas definiciones, se entiende por **Protección de Infraestructuras Críticas** (PIC) el conjunto de acciones y actividades destinadas a asegurar la función de las Infraestructuras Críticas, así como la continuidad e integridad de estas y cuyo fin es la prevención, paliación y neutralización del daño que puede ser causado por un ataque deliberado contra este tipo de infraestructuras. Además, se debe garantizar la integración de estas acciones con otras que procedan de otros roles, servicios o sujetos responsables dentro de la competencia que lo atañe.

Los **Operadores Críticos** son las empresas, entidades u organismos responsables del funcionamiento de una instalación, sistema, red, equipo, tecnología de la información, etc. designada como Infraestructura Crítica por proporcionar un servicio esencial e imprescindible para la sociedad.

2.1.2. Evolución de la PIC en España

Hace algo más de 14 años, con la aprobación del Real Decreto 421/2004 [6] e impulsado por las necesidades nacientes, que demandaban unos servicios de inteligencia capaces, especializados, renovados y competentes para afrontar nuevos retos y escenarios, surgió el Centro Criptológico Nacional (CCN), adscrito al Centro Nacional de Inteligencia (CNI). Entre los retos y necesidades de la época, se encuentra el desarrollo de las tecnologías de la información y la seguridad de los sistemas, garantizando la confidencialidad, la disponibilidad y la integridad de la información que estos manejan y de los propios sistemas [5].

En 2006, se crea la Capacidad de Respuesta a Incidentes de Seguridad de la Información por parte del Centro Criptológico Nacional (CCN-CERT), supliendo la ausencia de un CERT (Equipo de Respuesta ante Emergencias Informáticas) gubernamental en España, equivalente al ya existente en otros países del entorno. Cabe destacar que el primer CERT español corresponde con el creado por la Universidad Politécnica de Cataluña (esCERT-UPC), concretamente a finales de 1994. La creación del CCN-CERT se enfocó, en primera instancia, a las distintas administraciones públicas, ampliando esta responsabilidad con el paso de los años sobre empresas pertenecientes a sectores designados como estratégicos, esenciales para la seguridad nacional y para el conjunto de la economía de este [5].

Este organismo, no se enfoca de manera específica en la protección de infraestructuras críticas hasta el año 2007, cuando se publica el PNPIC (Plan Nacional de Protección de Infraestructuras Críticas) y se crea el Centro Nacional para la Protección de las Infraestructuras Críticas (CNPIC), que depende del Ministerio del Interior a través de la Secretaría de Estado de Seguridad. El PNPIC obliga a todas las infraestructuras críticas a designar un responsable de seguridad que hará de enlace con el CNPIC en caso de emergencia, a incentivar el intercambio de información entre las distintas empresas y organizaciones afectados y a definir las medidas que deben poner en marcha las infraestructuras críticas cuando se produzca un ataque. La misión del CNPIC es la de desarrollar el PNPIC y gestionar el Catálogo Nacional de Infraestructuras Estratégicas (que surge más adelante). Esto supuso un paso importante en materia de protección de infraestructuras críticas, pero se echaba de menos la existencia de una legislación robusta que apoyase las iniciativas, estableciera las responsabilidades de los implicados, etc. [7].

A pesar de que en 2008 se aprobó en Europa la Directiva 2008/114/CE del Consejo de 8 de diciembre de 2008 sobre la identificación y designación de infraestructuras críticas europeas y la evaluación de la necesidad de mejorar su protección [8], que marcaba un plazo de dos años para ser adoptada por los países miembros de la Unión, hasta 2011 no llegó ningún

cambio significativo a España, cuando se publicó la Ley de Protección de Infraestructuras Críticas (Ley 8/2011) y el Real Decreto 704/2011, de 20 de mayo, por el que se aprueba el Reglamento de protección de las infraestructuras críticas [4] que establecen medidas para la Protección de Infraestructuras Críticas y desarrolla su reglamento, respectivamente [7]. Con esta Ley, también surgieron las disposiciones 18439 del 15 de noviembre de 2011 [2] y 10060 del 18 de septiembre de 2015 [3], en las que se establecen los contenidos mínimos de los Planes de Seguridad del Operador y los Planes de Protección Específicos conforme a lo dispuesto en el Real Decreto 704/2011.

Dicha Ley, define los servicios principales como los necesarios para mantener las funciones sociales básicas, la salud, seguridad, etc. o el eficaz funcionamiento de las instituciones públicas, catalogando estos servicios en doce sectores: Administración, Espacio, Industria Nuclear, Industria Química, Instalaciones de Investigación, Agua, Energía, Salud, Tecnologías de la Información y las Comunicaciones, Transporte, Alimentación y Sistema Financiero. La Ley 8/2011 no fue implantada hasta el año 2014, cuando, además, se aprobaron los cinco primeros planes estratégicos sectoriales (electricidad, gas, petróleo, nuclear y financiero) [7].

Más adelante, en 2015, se aprobaron dos nuevos planes estratégicos sectoriales correspondientes a los sectores del agua y el transporte (marítimo, aéreo, ferroviario y carretera), en 2016 otros dos para el sector de la Industria Química y del Espacio, en 2017 los planes estratégicos sectoriales de las Tecnologías de la Información y de la Comunicación y en 2018 los del transporte urbano y metropolitano y el de la alimentación [7].

2.1.3. Estado actual en España

Tal y como se ha estudiado en el anterior apartado, el marco normativo asociado a la ciberseguridad en Infraestructuras Críticas en España queda acotado por la Ley PIC y complementado por el Real Decreto 704/2011 y las disposiciones 18439 y 10060 que establecen los contenidos mínimos de los Planes de Seguridad del Operador y los Planes de Protección Específicos.

La Ley PIC, tiene como principales objetivos la catalogación del conjunto de infraestructuras críticas que prestan servicios a la sociedad y el diseño de un planteamiento con medidas de prevención, protección y seguridad que muestren una eficacia real contra las posibles amenazas hacia las infraestructuras críticas (tanto en la seguridad física como en la de las tecnologías de la información y la informática). Además, con esta Ley, se ha designado como prestadores de servicios esenciales a las administraciones, el agua, la alimentación, la

energía, el espacio, la industria nuclear y la química, la salud, el sistema financiero y el tributario, las instalaciones de investigación, las tecnologías de la información y las comunicaciones y el transporte.

El Centro Nacional para la Protección de las Infraestructuras Críticas (CNPIC) y la Secretaría de Estado de Seguridad del Ministerio del Interior son los encargados de determinar y catalogar qué infraestructuras deben nombrarse como críticas y de desarrollar y coordinar acciones y estrategias que permitan garantizar su seguridad, estando obligadas a cumplir con ciertas metodologías de seguridad, separadas en dos protocolos distintos (el Plan de Seguridad del Operador, PSO y el Plan de Protección Específica, PSE, que se verán más adelante) cuyos contenidos mínimos están delimitados por las disposiciones 1849 y la 10060.

Todo esto, ha dado lugar al Plan Nacional de Protección de Infraestructuras Críticas, a partir del cual, están siendo creados los distintos Planes Estratégicos Sectoriales (uno por cada sector o subsector estratégico) y cuya aprobación determina que ciertas empresas u organizaciones serán designadas Operadores Críticos y, por consiguiente, ciertas instalaciones también.

Estos contenidos serán tratados en profundidad en el siguiente apartado.

2.2. Cumplimiento normativo

2.2.1. Ley PIC

El objetivo de la Ley PIC, según la propia Ley (Artículo 1, Apartado 1, Ley 8/2011) es el de "*establecer las estrategias y las estructuras adecuadas que permitan dirigir y coordinar las actuaciones de los distintos órganos de las Administraciones Públicas en materia de protección de infraestructuras críticas, previa identificación y designación de las mismas, para mejorar la prevención, preparación y respuesta de nuestro Estado frente a atentados terroristas u otras amenazas que afecten a infraestructuras críticas. Para ello se impulsará, además, la colaboración e implicación de los organismos gestores y propietarios de dichas infraestructuras, a fin de optimizar el grado de protección de éstas contra ataques deliberados de todo tipo, con el fin de contribuir a la protección de la población.*". Además, dicha Ley, regula las obligaciones de las Administraciones Públicas y los Operadores de Infraestructuras Críticas.

Esta Ley, es aplicable sobre cualquier Infraestructura Crítica ubicada en el territorio español (salvo las dependientes del Ministerio de Defensa y las Fuerzas y Cuerpos de Seguridad, que se regirán por su propia normativa y procedimientos) que esté vinculada a los

sectores estratégicos de la administración, el espacio, la industria nuclear, la industria química, las instalaciones de investigación, el agua, la energía, la salud, las tecnologías de la información y las comunicaciones, el transporte, la alimentación y el sistema financiero y tributario.

La Ley determina que **El Catálogo Nacional de Infraestructuras Estratégicas** (contenedor de toda la información actualizada, completa y contrastada relativa a las características específicas de cada infraestructura estratégica existente en el territorio nacional) es administrado por el Ministerio del Interior, a través de la Secretaría de Estado de Seguridad. Además, considera que para que una infraestructura sea catalogada como estratégica (y en su caso como Infraestructura Crítica) y esta sea incluida dentro del catálogo, el ya mencionado Ministerio debe estimarlo oportuno.

El **Sistema de Protección de Infraestructuras Críticas** (SPIC), también determinado por la Ley PIC, se compone de distintas instituciones, órganos y empresas, procedentes del sector público y del privado: Agentes del Sistema de Protección de Infraestructuras Críticas, la Secretaría de Estado de Seguridad del Ministerio del Interior, El Centro Nacional para la Protección de las Infraestructuras Críticas, Los Ministerios y organismos integrados en el SPIC, Las Comunidades Autónomas y las Ciudades con Estatuto de Autonomía, Las Delegaciones del Gobierno de las Comunidades Autónomas y las Ciudades con Estatuto de Autonomía, Las Corporaciones Locales (a través de la asociación de Entidades Locales de mayor implantación a nivel nacional), La Comisión Nacional para la PIC y los operadores críticos del sector público y privado. Sus responsabilidades son la seguridad de los ciudadanos y el correcto funcionamiento de los servicios básicos y esenciales.

El SPIC comienza con el **Plan Nacional de Protección de Infraestructuras Críticas**, que define la estructura y presta coherencia a todo el sistema. Este documento, elaborado por el Ministerio del Interior, a través de la Secretaría de Estado de Seguridad, permite dirigir y coordinar las actuaciones necesarias para proteger las infraestructuras críticas contra el terrorismo. A partir de este documento, se desarrollan diferentes **Planes Estratégicos Sectoriales** o PES (uno por cada sector estratégico y de carácter confidencial), que incluyen, por sectores, los criterios y medidas a adoptar para hacer frente a situaciones de riesgo. Así mismo, la designación de un Operador Crítico obliga a desarrollar los **Planes de Seguridad del Operador** (PSO) y los **Planes de Protección Específicos** o PPE (instrumentos de planificación mediante los cuales se asume la obligación de colaborar en la identificación de las infraestructuras, especificar las políticas que deben implementarse en materia de seguridad dentro de las mismas, así como implantar las medidas generales de protección para la prevención y protección de posibles ataques) por parte de los operadores críticos respecto a todas sus infraestructuras clasificadas como críticas. Por último, los **Planes de Apoyo**

Operativo (PAO), elaborados por los cuerpos policiales para cada una de las infraestructuras clasificadas como críticas dotadas de un Plan de Protección Específico, que deben contemplar las medidas de vigilancia, prevención, protección o reacción necesarias además de las determinadas por los operadores críticos.

Bajo el SPIC, también se establece cierta seguridad en las comunicaciones, por ejemplo, determinando que la Secretaría de Estado de Seguridad sea la encargada de arbitrar los sistemas de gestión que permitan una continua actualización y revisión de la información disponible en el Catálogo por parte del CNPIC, así como su difusión a los diferentes organismos autorizados. También se expone la necesidad de que las Administraciones Públicas y los sistemas, comunicaciones e información referida a la protección de infraestructuras críticas garanticen la confidencialidad, la integridad y la disponibilidad de los datos de infraestructuras estratégicas a los que tengan acceso según el nivel de clasificación que les sea asignado.

El Grupo de Trabajo Interdepartamental para la Protección de las Infraestructuras Críticas será el encargado de elaborar los diferentes Planes Estratégicos Sectoriales (con la colaboración de los agentes del Sistema de Protección de Infraestructuras Críticas y con asesoramiento técnico), proponer a la Comisión Nacional para la PIC (CNPIC) la designación de los Operadores Críticos por cada sector estratégico definido, proponer a la CNPIC la creación, modificación o supresión de grupos de trabajo sectoriales (informando oportunamente de los resultados obtenidos por estos) y llevar a cabo los estudios y trabajos encomendados por la CNPIC. Este grupo debe estar presidido por el director del CNPIC y compuesto por un representante de:

- El Sistema de Protección de Infraestructuras Críticas.
- La Dirección Adjunta Operativa del Cuerpo Nacional de Policía.
- La Dirección Operativa de la Guardia Civil.
- La Dirección General de Protección Civil y Emergencias del Ministerio del Interior.
- El Estado Mayor Conjunto de la Defensa.
- El Centro Nacional de Inteligencia.
- El Departamento de Infraestructura y Seguimiento para Situaciones de Crisis.
- El Consejo de Seguridad Nuclear.
- El CNPIC.

Además, a las reuniones (que deberán celebrarse al menos dos veces al año con carácter ordinario y tantas veces como sea necesario de forma extraordinaria), deberá asistir un representante de cada Comunidad Autónoma con competencias estatutariamente reconocidas

para la protección de bienes y personas y para el mantenimiento del orden público. Según el Reglamento de protección de las infraestructuras críticas, aprobado mediante el Real Decreto 704/2011, podrán constituirse, igualmente, otros grupos de trabajo sectoriales para los sectores o subsectores expuestos en la Ley 8/2011, en los que, a parte del CNPIC, podrán participar los Operadores Críticos y otros agentes del SPIC.

También se establece la necesidad de que los Operadores Críticos nombren y comuniquen al Ministerio del Interior un Responsable de Seguridad y Enlace (que cuente con la habilitación de Director de Seguridad, expedida por el Ministerio del Interior o una habilitación equivalente), además de comunicar a las Delegaciones del Gobierno (o el órgano competente de la Comunidad Autónoma) la existencia del Delegado de Seguridad asignado a dicha infraestructura. Los Operadores Críticos, deberán, a su vez, garantizar la seguridad de los datos de sus propias infraestructuras, utilizando para ello los medios de protección y los sistemas de información adecuados.

Las explicaciones y definiciones expuestas en párrafos anteriores han sido extraídas y comprendidas a partir de la propia Ley 8/2011 [1] y del Real Decreto 704/2011 de 20 de mayo [9]. De estas explicaciones y definiciones, puede deducirse que los dos grandes objetivos de dicha Ley son la catalogación de las infraestructuras que prestan servicios esenciales a la sociedad y el diseño de un proyecto o programa con medidas de prevención y protección eficaces contra amenazas, tanto en la seguridad física como en la de las tecnologías de la información y las comunicaciones.

Además de estos dos grandes objetivos, la Ley PIC busca la creación del Sistema Nacional de Protección de Infraestructuras Críticas (formado por los Operadores Críticos, el CNPIC, Ministerios, Comunidades Autónomas, etc.) y establecer las bases para el Sistema de Planificación PIC, que se compone de un conjunto de textos normativos que establecen medidas para la Protección de Infraestructuras Críticas y que deben ser llevadas a cabo por los integrantes del Sistema de Protección de Infraestructuras Críticas (PES, PSO, PPE y PAO). Véase la Figura 2.1.

Figura 2.1: Textos normativos del Sistema de Planificación PIC.

- PES o Plan Estratégico Sectorial. Engloba las normativas, tipologías de infraestructuras, interdependencias y niveles de criticidad.
- PSO o Plan de Seguridad del Operador. Deben definir la política general del operador, de manera que garantice la seguridad de todas las instalaciones o sistemas y la gestión de estas.
- PPE o Plan de Protección Específico. En estos documentos deben definirse las medidas concretas que han sido adoptadas, así como las que deban ser adoptadas por los Operadores Críticos para garantizar tanto la seguridad física como la lógica de sus infraestructuras críticas.
- PAO o Plan de Apoyo Operativo: Plan específico para cada una de las Infraestructuras Críticas. Estos planes se elaboran por parte de los cuerpos de seguridad del estado, son supervisados por la Delegación del Gobierno y aprobados por la Secretaría de Estado de Seguridad.

En los siguientes apartados se expondrán, detalladamente, los documentos anteriormente citados, explicando y describiendo su funcionalidad y contenidos.

2.2.2. Planes Estratégicos Sectoriales

Los Planes Estratégicos Sectoriales (PES) son los instrumentos de estudio y planificación que permiten conocer (en todo el territorio nacional), para cada uno de los sectores contemplados en la Ley PIC (administración, espacio, industria nuclear, industria química, instalaciones de investigación, agua, energía, salud, tecnologías de la información y las comunicaciones, transporte, alimentación y el sistema financiero y tributario), los servicios básicos que deben proporcionar a la sociedad, el funcionamiento general de estos, las vulnerabilidades que pueden encontrarse en estos sistemas (basándose en amenazas potenciales

tanto de carácter físico como lógico que afecten al sector o subsector en cuestión), los efectos que podría provocar el paro de estos sistemas y las medidas que deben llevarse a cabo para su correcto mantenimiento [10], [1].

Estos planes, serán elaborados por el Grupo de Trabajo, coordinado por el CNPIC (con la participación y asesoramiento técnico de los operadores afectados) y su contenido se basa en [1]:

- Analizar la normativa sectorial para evitar discrepancias con la Ley PIC.
- Establecer tipologías de Infraestructuras Críticas.
- Identificar a los Operadores Críticos.
- Estructurar y segmentar las Infraestructuras Críticas por actividades.
- Analizar dependencias entre sectores y dentro de los propios sectores.
- Decretar una tabla de criticidad.
- Decretar análisis de riesgos sectorial.
- Decretar mecanismos de coordinación con el Plan Nacional de Protección de las Infraestructuras Críticas.

Para la adaptación completa al Plan Estratégico Sectorial que le corresponda a cada operador, estos, deberán llevar a cabo varias acciones. En primer lugar, deberán elaborar el Plan de Seguridad del Operador y mantenerlo actualizado. También es necesaria la elaboración de un Plan de Protección Específico por cada una de las infraestructuras consideradas como críticas, así como la actualización periódica de este. Por otro lado, es necesario designar a un Responsable de Seguridad y Enlace y a un Delegado de Seguridad por cada infraestructura considerada crítica (comunicando su designación a las Delegaciones del Gobierno o el órgano competente de la Comunidad Autónoma), facilitar las inspecciones que se requiera llevar a cabo por parte de las autoridades competentes para verificar el cumplimiento de la normativa sectorial y ejecutar las medidas de seguridad necesarias, solventando todas las deficiencias descubiertas en el menor tiempo posible. La comunicación con el Ministerio del Interior será a través del CNPIC en cualquier tema relacionado con sus responsabilidades, funciones y obligaciones [10], [1].

La aprobación de estos planes requerirá una reunión previa con las entidades que serán afectadas por el plan en cuestión, consensuando con dichas entidades, los ministerios implicados, etc. el contenido final (contenido de los planes, medidas técnicas y organizativas de estos, etc.). Cuando se hayan aprobado estos planes, se llevará a cabo el nombramiento de los primeros Operadores Críticos de cada uno de estos sectores, que deberán elaborar sus respectivos PSO y PPE apoyados por el CNPIC [1].

A 21 de abril de 2018, se encuentran cubiertos nueve de los principales sectores nacionales de producción, con aproximadamente 150 operadores críticos [11]. Estos sectores, se cubren gracias a los Planes Estratégicos Sectoriales aprobados hasta la fecha, siendo:

- Electricidad (Aprobado en el año 2014)
- Gas (Aprobado en el año 2014).
- Petróleo (Aprobado en el año 2014).
- Nuclear (Aprobado en el año 2014).
- Financiero (Aprobado en el año 2014).
- Agua (Aprobado en el año 2015).
- Transporte marítimo (Aprobado en el año 2015).
- Transporte aéreo (Aprobado en el año 2015).
- Transporte ferroviario (Aprobado en el año 2015).
- Transporte por carretera (Aprobado en el año 2015).
- Industria química (Aprobado en el año 2016).
- Espacio (Aprobado en el año 2016).
- Tecnologías de la Información y la Comunicación (Aprobado en el año 2017).
- Transporte Urbano y Metropolitano (Aprobado en el año 2018).
- Alimentación (Aprobado en el año 2018).

Por lo tanto, los operadores críticos designados deben poner en marcha una serie de Planes de Protección Específicos sobre todas sus infraestructuras, detallados en estos Planes Estratégicos Sectoriales, que serán complementados por los Planes de Apoyo Operativos facilitados por las Fuerzas y Cuerpos de Seguridad y/o las Fuerzas Armadas.

2.2.3. Plan de Seguridad del Operador

Los PSO o Planes de Seguridad del Operador, deben definir la política general del operador para garantizar completamente la seguridad de todas las instalaciones o sistemas de su propiedad o que se encuentren bajo su gestión. Estos planes, deben recoger algunos aspectos básicos, entre los que destacan [12]:

- Objeto. La meta que se pretende conseguir desde la organización con la política y el desarrollo y aplicación de esta.
- Alcance. Podrá ser uno o varios campos, uno o varios aspectos o toda la organización.
- Compromiso de la alta dirección. Aprobando y apoyando el plan propuesto.

- Carácter integral. Incluyendo tanto seguridad física como seguridad lógica.

Entre los contenidos de estos planes, deben incluirse la política general de seguridad del operador y el marco de gobierno, la relación de servicios esenciales prestados por el Operador Crítico, los criterios de aplicación de medidas de seguridad integral y la metodología de análisis de riesgo, tanto para amenazas físicas como lógicas [12], [2], [3].

- La política general de seguridad del operador y el marco de gobierno, que, a su vez, se divide en tres grandes bloques, cuyo contenido se describe a continuación.

    - Organización de la seguridad. Debe designarse tanto un Responsable de Seguridad y Enlace como un Delegado de Seguridad. Siendo necesario el diseño de un organigrama de seguridad y de un organigrama general en el que queden latentes e integradas las distintas funciones de seguridad de la organización, indicando, además, si existe alguna subcontrata (y en caso afirmativo, el tipo de servicios que desempeña y los compromisos acordados con esta).

    - Formación y concienciación. Todo el personal que guarde relación con la protección de los servicios esenciales e Infraestructuras Críticas debe formarse para conseguir capacidad de comprensión de la seguridad integral, de la autoprotección y de la seguridad del medio ambiente, así como habilidades organizativas y de comunicación. Debe reflejarse en este apartado, si existiera el Plan de Formación General, especificando la parte relacionada con la PIC. Además, será necesario reflejar la participación del operador crítico en ejercicios de simulación de incidentes de seguridad (y la periodicidad programada para estos).

    - Modelo de gestión aplicado. Este apartado debe contemplar, como mínimo, la implementación de controles de seguridad acorde con las prioridades y necesidades de la organización, así como una evaluación y monitorización periódica de la seguridad.

    - Comunicación. El Operador Crítico deberá recoger, en este apartado, los procedimientos establecidos para comunicarse e intercambiar información con el CNPIC (sobre los incidentes o situaciones que puedan poner en riesgo o comprometer la seguridad de las Infraestructuras Críticas y de aquellas variaciones de carácter

organizativo, planificación, etc. que se produzcan) y con el CERTSI (a través de la Oficina de Coordinación Cibernética del Ministerio del Interior, acerca de los incidentes que puedan comprometer la seguridad y la disponibilidad de los servicios que se prestan).

- La relación de servicios esenciales prestados por el Operador Crítico, igual que ocurre con la política general de seguridad del operador y el marco de gobierno, puede desglosarse en tres bloques:
    - Datos descriptivos de la organización. Es necesario presentar al Operador Crítico, así como el sector principal bajo el que desarrolla su actividad. También debe exponerse la estructura organizativa, y, cuando se trate de grupos empresariales, la de la sociedad, tal como la presencia geográfica de la organización (incluidas Comunidades Autónomas y países donde presten sus servicios) y las principales actividades que se llevan a cabo (incluidos los servicios o productos ofrecidos).
    - Datos sobre servicios esenciales. Deben identificarse y mantenerse un inventario actualizado de los servicios esenciales. También es preciso exponer las consecuencias que supondría para la sociedad la interrupción del servicio o servicios esenciales ofrecidos.
    - Datos sobre interdependencias. Es necesario identificar y explicar el motivo que origina las interdependencias (entre las propias instalaciones o servicios, con servicios prestados por otros Operadores Críticos o con sus proveedores).
- Las metodologías de análisis de riesgo engloban la descripción de la metodología de análisis, el inventario de activos, la identificación y evaluación de amenazas y la valoración y la gestión del riesgo.
    - Descripción de la metodología de análisis. Debe seleccionarse y establecerse una metodología de análisis de riesgos reconocida internacionalmente (MAGERIT, Mosler, NIST SP 800 30, Mehari, etc.), describiendo y asociando a la metodología elegida las etapas esenciales, el algoritmo de cálculo de empleados, el carácter cuantitativo o cualitativo, el método empleado para valorar los impactos, las métricas utilizadas para la medición de riesgos aceptables, residuales, etc. y las

relaciones entre los análisis de riesgos a distintos niveles (corporación, servicios y nivel de infraestructura crítica).

- Inventario de activos que soportan servicios esenciales. Es esencial exponer la vinculación entre servicios y activos y detallar las instalaciones y sistemas (*software*, *hardware*, comunicaciones, etc.) que los proporcionan, así como las personas involucradas en los distintos procesos.
- Identificación y evaluación de amenazas. En el PSO debe presentarse y evaluarse cualquier amenaza que pueda mostrarse, tanto internas como externas, físicas, lógicas, intencionadas, no intencionadas, etc.
- Valoración y gestión del riesgo. Deben detallarse los criterios utilizados para valorar las categorías en las que se han clasificado los riesgos o amenazas y la metodología de selección de la estrategia (reducción, eliminación, transferencia, etc.). Es necesario presentar, en el PSO, los plazos necesarios para la implementación de las medidas (cuando se elija una estrategia de minimización del riesgo), además del tratamiento que debe dársele a las amenazas de ataques intencionados (en especial a las que supongan una interrupción a la hora de prestar los servicios esenciales) y los mecanismos de seguimiento y actuación periódicos que muestren los niveles de riesgo.

- Los criterios de aplicación de medidas de seguridad integral deben incluir, de forma general, las medidas que han sido implantadas en los activos y los recursos sobre los que se basan los servicios esenciales (recogidos en sus correspondientes Planes de Protección Específicos).

La revisión de estos documentos ha de hacerse cada dos años. Cuando deba realizarse algún tipo de modificación del documento, estas modificaciones han de ser validadas por el CNPIC. Independientemente de la actualización formal del PSO, si ha variado algún tipo de información sustancial de la organización o empresa, estos cambios han de ser trasladados al CNPIC a través de los canales habilitados para ello en un plazo máximo de diez días (contados a partir del día del cambio) [2], [3].

Por lo tanto, de forma muy resumida, puede decirse que el Plan de Seguridad del Operador es una declaración de intenciones, una hoja de ruta en la que se exponen aspectos generales sobre cómo se concibe la seguridad de una empresa u organización, que debe incluir,

como mínimo la política general de seguridad del operador y el marco de gobierno, la relación de servicios esenciales prestados, las metodologías de análisis de riesgo que van a utilizarse y los criterios de aplicación de medidas de seguridad integral.

2.2.4. Plan de Protección Específico

Los Planes de Protección Específicos o PPE, son documentos operativos en los cuales es necesario definir las medidas concretas para garantizar la seguridad tanto física como lógica de las Infraestructuras Críticas por parte de los Operadores Críticos. Estas medidas pueden haber sido ya adoptadas o estar previsto hacerlo [12].

Los PPE deben realizarse siguiendo las pautas establecidas en la política general de seguridad del Operador establecida en el PSO. Los Análisis de Riesgos, vulnerabilidades y amenazas llevados a cabo estarán sujetos, a su vez, a las pautas metodológicas descritas en el mismo documento (el PSO) [12].

Es necesario que el Operador elabore un Plan de Protección Específico por cada una de las Infraestructuras Críticas de las que sea propietario o gestor. Sus contenidos mínimos y procesos a realizar dentro de la organización, establecidos por la Secretaría de Estado de Seguridad a través del CNPIC, deben recoger, de forma práctica, los aspectos y criterios del PSO que afecten específicamente a la instalación. Entre estos contenidos y procesos, debe incluirse cómo va a organizarse la seguridad, la descripción de la infraestructura, el resultado del análisis de riesgo y el plan de acción seccionado por activos [12], [2], [3].

- Organización de la seguridad. En este apartado se expone la forma en la que la seguridad va a estar estructurada dentro de la instalación. Para cumplir con este requisito, es necesario llevar a cabo los siguientes procesos:
    - Asignar e informar del Delegado de la Seguridad de las Infraestructuras Críticas (incluyendo sus datos de contacto, entre los que deben constar su dirección, teléfono y correo electrónico). Esta persona, debe ser el enlace operativo y el canal de información entre la organización y las autoridades competentes en materia de seguridad de sus infraestructuras. Debe ser capaz de orientar las necesidades que surjan (tanto operativas como informativas) y de coordinarse con el Responsable de Seguridad y Enlace (además de con los otros Delegados de Seguridad del Operador Crítico). En este apartado también es necesario incluir los cursos o la formación relacionada con el desempeño del puesto que el Delegado de la Seguridad haya recibido.

- Deben detallarse los Mecanismos de Coordinación que van a seguirse entre el Delegado de Seguridad de la Infraestructura Crítica y otros Delegados de otras infraestructuras y con el Responsable de Seguridad y Enlace del propio Operador Crítico, con autoridades y terceros y con otros planes del Operador (como planes de continuidad de negocio, de evacuación, etc.).
- Mecanismos y Responsables de Aprobación interna. Indicar quienes son los responsables de la aprobación de las acciones, así como el procedimiento seguido para ello y la fecha en la que se produjo la última aprobación.

- Descripción de la infraestructura. Deben indicarse, de forma clara, algunos aspectos y descripciones relacionados con la propia infraestructura, que son:
  - Datos generales. Datos relativos a la denominación, tipo de instalación, propiedad y forma de gestionar la misma, su localización (tanto física como estructural), los sistemas que gestionan la Infraestructura Crítica y su arquitectura (mediante mapas de red, de comunicaciones, de sistemas, etc.). Igualmente, en este apartado, deben incluirse datos estratégicos como pueden ser la descripción del servicio esencial que proporciona y el ámbito geográfico o poblacional que cubre, la relación con otras infraestructuras necesarias para prestar el servicio (en caso de existir dichas relaciones) y la descripción detallada de sus funciones y su relación con los servicios esenciales soportados.
  - Activos y elementos que soportan la Infraestructura Crítica. Estos elementos deben diferenciarse según sean vitales o no, detallando, además, el *hardware* y el *software* utilizado, las redes de comunicaciones para el intercambio de datos (utilizadas en la Infraestructura Crítica), las personas que explotan estos elementos y los proveedores críticos necesarios para que la Infraestructura Crítica funcione. En este apartado, además, es necesario especificar las dependencias entre los diferentes activos sobre los que se sostiene o que componen la infraestructura crítica. El nivel de detalle debe corresponderse con el del PSO, incluyendo tanta información como sea necesario para recoger, de forma explícita, el alcance de la infraestructura que se requiere proteger.

- Interdependencias. Es necesario hacer referencia e indicar las interdependencias que puedan tenerse con otras Infraestructuras Críticas pertenecientes al propio Operador, de otros operadores y/u otras infraestructuras estratégicas que soportan el servicio esencial. Además, estas interdependencias deberán ser consideradas en el Análisis de Riesgos.

- Resultado del Análisis de Riesgos. Es preciso que el Operador Crítico refleje, en el PPE, los resultados obtenidos tras la realización del Análisis de Riesgos (realizado siguiendo las pautas indicadas en el PSO). Los contenidos mínimos de este apartado han de ser:

  - Identificación de las amenazas internas o externas, físicas o lógicas, intencionadas o aleatorias. Estas amenazas han de indicarse de forma clara, siempre que hayan sido consideradas para la realización de los análisis de riesgos y que afecten a alguno de los activos que soportan la Infraestructura Crítica y/o a la propia infraestructura.

  - Definición de medidas permanentes y temporales. Es necesario que el Operador describa las medidas de seguridad (de protección de las instalaciones, los equipos, los datos, aplicaciones, personal, documentación, etc.) implantadas en el momento de la elaboración del PPE (con las que se ha contado para la realización del análisis de riesgos). Estas medidas pueden ser de dos tipos:

    - Permanentes: aquellas medidas concretas que ya han sido adoptadas por el Operador Crítico y que han sido consideradas como necesarias tras la realización del Análisis de Riesgos, en base a los riesgos, amenazas e impacto sobre sus activos.

    - Temporales: las medidas de seguridad extraordinarias, que refuerzan a las permanentes y se deben implementar a raíz de la activación de alguno de los niveles de seguridad del PNPIC, o debido a las comunicaciones que las autoridades competentes puedan efectuar al Operador Crítico en relación con una amenaza concreta y temporal sobre la instalación que gestiona. Estas medidas deben permanecer activas el tiempo estrictamente necesario (mientras permanezca activo el nivel de seguridad) y modificarse paulatinamente según el nivel.

- Identificación de medidas por capas. La identificación de las medidas de protección y prevención debe realizarse por capas, especificando, para cada nivel, la propia medida en concreto y el tiempo de respuesta y de recuperación que estas requieren. Estas capas deben corresponderse con:
    - Medidas organizativas o de gestión. Estas medidas deben centrarse en Análisis de Riesgos, la definición de los roles y las responsabilidades asociadas a estos, las políticas, procedimientos y estándares de seguridad a llevar a cabo, las normas y/o regulaciones que se aplican en la Infraestructura Crítica, así como la identificación del nivel de cumplimiento de estas y la certificación, acreditación y evaluación de seguridad obtenidas para la Infraestructura Crítica.
    - Medidas operacionales o procedimentales. Deben especificarse los procedimientos llevados a cabo para la realización, gestión y mantenimiento de los activos (inventario, identificación, catalogación, gestión continua de activos físicos y lógicos, etc.), los procedimientos operativos para la monitorización, supervisión y evaluación de activos físicos y lógicos y los procedimientos llevados a cabo para formar, concienciar y capacitar a los empleados y operarios. También se engloban los procedimientos de contingencia., los de gestión y respuesta de incidentes, los necesarios para la gestión de acceso de los usuarios, accesos temporales, control de entrada/salida, etc. y los procedimientos operacionales del personal de seguridad (funciones, horarios, dotaciones, etc.).
    - Medidas de protección o técnicas. Estas medidas, en materia de prevención y detección, deben contemplar la seguridad física perimetral y los controles de acceso (zonas de seguridad, detectores de intrusos, cámaras de videovigilancia, arcos de seguridad, etc.), la coordinación y monitorización (los centros de control de seguridad y el control de alarmas, recepción y visionado de imágenes de estos, etc., los equipos de vigilancia con sus turnos, rondas, volúmenes, etc. y los sistemas de comunicación) y la seguridad lógica perimetral y la segmentación de redes (*firewalls*, zonas desmilitarizadas, redes privadas

virtuales, configuración de elementos técnicos, protección frente a Malware, etc.).

- El PPE debe incluir, además, la valoración de riesgos (los riesgos asumidos por la Infraestructura Crítica que tengan un nivel de impacto elevado y una baja probabilidad de perpetrarse). Entre estos valores, deben destacarse las principales conclusiones obtenidas tras el Análisis de Riesgos. Para cada uno de los activos y/o amenazas, ha de incluirse información de quién ha evaluado o aprobado el riesgo y la estrategia de tratamiento asociada, los criterios de valoración de riesgos adoptados, la fecha del último análisis llevado a cabo y el resultado o la conclusión sobre el nivel de riesgo soportado. Estos riesgos deben ser validados por el CNPIC.

- Plan de acción por activos. Cuando han de aplicarse medidas de seguridad adicionales sobre los activos de la Infraestructura Crítica, estas deben especificarse de forma clara, exponiendo el motivo de la necesidad, su ámbito de acción y el resultado buscado. Estas medidas pueden ser de dos tipos:

  - Medidas complementarias. En caso de ser necesaria la implantación de medidas complementarias a las ya existentes (que deben ser implementadas en no más de tres años), se debe enumerar dichas medidas (ya sean físicas o lógicas) y explicar la operación resultante para cada tipo de protección y cada uno de los horarios significativos.

  - Medidas a aplicar para la protección del activo como consecuencia de los resultados obtenidos en el Análisis de Riesgos. En este proceso, deben incluirse la acción propuesta (detallando su ámbito de aplicación), el activo, quién es el responsable de su implantación, los plazos estimados, los mecanismos de coordinación y seguimiento y el carácter (permanente, temporal o gradual) de la medida.

Los PPE, además de ser presentados al CNPIC tras su creación, deberán ser revisados bienalmente. Cuando estos documentos requieran una actualización o modificación, quedarán actualizados tras la validación de dicha modificación por parte del CNPIC [3].

2.2.5. Plan de Apoyo Operativo

Los Planes de Apoyo Operativo (PAO), son documentos operativos en los que deben plasmarse medidas concretas que deben poner en marcha las Infraestructuras Críticas y que sirven como apoyo para mejorar la protección de estas infraestructuras, complementando los Planes de Seguridad Específicos elaborados por los Operadores. Estos planes, son realizados por las Administraciones Públicas a través de las Fuerzas y Cuerpos de Seguridad del Estado, o, en su caso, por las Fuerzas Armadas [1].

En ellos, se contemplan las medidas de vigilancia, prevención, protección y reacción que debe brindarse complementando a las dispuestas por los Operadores Críticos en sus Planes de Seguridad del Operador y los Planes de Protección Específicos, siendo acordes a los cinco niveles de protección establecidos [1].

Además, esos documentos son elaborados por los Cuerpos de Seguridad del Estado, o, en su caso, los autonómicos con competencia territorial en el área de cada una de las Infraestructuras denominadas Críticas y que estén dotadas de un Plan de Protección Específico. Esta elaboración, debe llevarse a cabo en un plazo máximo de cuatro meses desde la recepción del Plan de Seguridad Específico definitivo. Cuando sea labor de la Policía Nacional, la revisión e inspección de los Planes de Protección Específicos y la elaboración de los PAO corresponderá a las Unidades Territoriales de Seguridad Privada de cada una de las Brigadas Provinciales de Seguridad Ciudadana. En las Comunidades Autónomas que dispongan de competencias estatutarias reconocidas para la protección de bienes y personas y el mantenimiento del orden público, estas deben desarrollar, sobre cada una de las infraestructuras críticas ubicadas en su territorio, las facultades de las Delegaciones de Gobierno correspondientes a la coordinación de los cuerpos policiales autonómicos, así como, cuando corresponda, la activación del PAO para responder ante una brecha de seguridad [1].

Como mínimo, los PAO deben contener los datos generales de la infraestructura (denominación, operador asignado, localización, ubicación, geolocalización, extensión, datos del delegado de seguridad y su suplente, etc.) y datos relevantes extraídos del PPE, entre los que deben aparecer [13]:

- Los resultados del Análisis de Riesgo realizado.
- Las medidas permanentes que han sido implantadas por el operador.
    - Medios humanos involucrados en la seguridad de la Infraestructura Crítica (vigilantes, personal del departamento de seguridad, etc.).
    - Medidas de protección activas (zonas de seguridad, detectores de intrusos, cámaras de videovigilancia, etc.).

    - Medidas de protección pasivas (vallas, muros, etc.).
    - Información de la localización de los medios y activos de interés, ordenados en función de su criticidad y capacidad de protección.
- Medidas a implantar gradualmente por el Operador conforme al PPE.
- Medidas específicas previstas por el Operador en función de la infraestructura.
- Medidas a aplicar en caso de materialización de una amenaza (facilitadas por el operador para facilitar la actuación de las Fuerzas de Seguridad).
- Observaciones a los puntos anteriores.

Tras la elaboración de los Planes de Apoyo Operativo, estos deben ser enviados a la Delegación del Gobierno (o, en las Comunidades Autónomas con competencia para ello, al CNPIC), dónde serán validadas y grabadas de forma definitiva. Posteriormente, serán devueltas de nuevo al Cuerpo Policial pertinente para que este las custodie y ponga en funcionamiento en caso de ser necesario [1].

2.2.6. Análisis de Riesgos

Tal y como se menciona en anteriores apartados, la Ley PIC hace necesaria la elaboración de un Análisis de Riesgos a distintos niveles para la creación del Plan de Protección Específico. En este análisis ha de utilizarse, obligatoriamente, una metodología reconocida internacionalmente (MAGERIT, Mosler, NIST SP 800 30, Mehari, etc.). Estos Análisis de Riesgos han de ser elaborados por parte del Grupo de Trabajo Interdepartamental para la Protección de las Infraestructuras Críticas y aprobados por el CNPIC.

MAGERIT es la metodología de análisis y gestión de riesgos más utilizada para la elaboración de los Análisis de Riesgos en entornos PIC. Esta metodología, ha sido confeccionada por el Consejo Superior de Administración Electrónica, como respuesta a la necesidad y apreciación de que toda la sociedad depende, cada vez más, de las tecnologías de la información para cumplir plenamente con su misión [14].

Gracias a la realización de un Análisis de Riesgos con MAGERIT, es posible estudiar y analizar los riesgos soportados por un sistema de información y por su entorno. En este Análisis de Riesgos, se incluye la evaluación del impacto que una brecha o violación de seguridad podría tener en la empresa u organización, señalando, además, los riesgos que pueden existir, identificando las amenazas y determinando las vulnerabilidades del sistema de prevención que pretende mitigar esas amenazas. A partir de esta información, pueden obtenerse unos resultados que posibilitan encontrar, de forma apropiada, las medidas a adoptar para conocer, prevenir,

impedir, reducir o mitigar dichos riesgos, obteniendo una reducción de los posibles daños que estos pueden ocasionar [15].

MAGERIT implementa el Proceso de Gestión de Riesgos dentro de un marco de trabajo de tal forma que los órganos de gobierno puedan tomar decisiones teniendo en cuenta los riesgos que surgen del uso de tecnologías de la información. Esta metodología se compone de dos libros y una guía de técnicas, cuyos contenidos se comentan, de forma breve, en el 0.

Para facilitar la realización de estos Análisis de Riesgos, el Centro Criptológico Nacional (CN-CERT) ha creado algunas herramientas para la realización de estos, basándose en la metodología MAGERIT. Entre estas herramientas cabe destacar:

- PILAR, con la cual pueden analizarse los riesgos en varias dimensiones (confidencialidad, integridad, disponibilidad, autenticidad y trazabilidad). Esta herramienta, propone salvaguardas o contramedidas, normas de seguridad y procedimientos de seguridad para tratar el riesgo, analizándose el riesgo residual a lo largo de diversas etapas de tratamiento [16].

- PILAR Basic, versión sencilla de PILAR destinada, en especial, a PYMES y administraciones locales. Con esta herramienta, pueden analizarse los riesgos en varias dimensiones (confidencialidad, integridad, disponibilidad, autenticidad y trazabilidad) al igual que ocurre con PILAR y se proponen contramedidas, analizándose el riesgo residual a lo largo de las distintas etapas del tratamiento [17].

- µPILAR, es una versión muy reducida de la herramienta PILAR, especialmente desarrollada para realizar Análisis de Riesgos muy rápidos. Los resultados obtenidos con esta herramienta pueden cargarse en PILAR para realizar posteriormente un análisis más detallado. Al igual que ocurre con sus dos hermanas (PILAR y PILAR Basic), con µPILAR pueden analizarse los riesgos en varias dimensiones (confidencialidad, integridad, disponibilidad, autenticidad y trazabilidad). Además, se proponen salvaguardas analizándose el riesgo residual [18].

CAPÍTULO 3. CIBERSEGURIDAD INDUSTRIAL

Anteriormente, los Sistemas de Control Industrial (SCI o ICS, por sus siglas en inglés *Industrial Control Systems*) guardaban poco parecido con los sistemas de información tradicionales, encontrándose prácticamente aislados, ejecutando *software* propietario y utilizando protocolos muy concretos. Con el paso del tiempo, a medida que estos sistemas fueron integrándose cada vez más en los propios sistemas de información convencionales, y para promover la conectividad, la eficiencia y las capacidades de acceso remoto, gran parte de estos ICS comenzó a utilizar otros protocolos y sistemas de comunicación más extendidos, empleando también para su desarrollo componentes *hardware* y *software* que hasta la fecha solo utilizaban los sistemas de información tradicionales. Aunque este cambio introdujo nuevas capacidades a los ICS, también hizo que estos sistemas quedaran al descubierto, introduciendo en ellos un mayor número de vulnerabilidades y requiriendo, por ello, una mayor necesidad de asegurarlos y securizarlos.

Un único elemento de seguridad, configuración o tecnología no puede proteger de forma adecuada un ICS, debiéndose basar esta protección en la combinación de políticas de seguridad efectivas y un conjunto de sistemas y controles de seguridad debidamente configurados.

Detectar qué controles de seguridad son necesarios para mitigar los riesgos hasta un nivel admisible, conocer si dichos controles se han implementado correctamente y de forma realista o percibir el nivel de seguridad requerido para que funcionen según lo previsto y produzcan el resultado deseado, dependerá, casi en su totalidad, del contexto de un proceso de gestión de riesgos efectivo y de una estrategia de seguridad que identifique, mitigue y controle continuamente los riesgos de los ICS. A su vez, estos ICS (y, por ende, los controles de seguridad necesarios asociados al mismo), irán ligados a los requerimientos de la organización, no siendo los mismos, por ejemplo, para una fábrica de refrescos que para una central nuclear.

En este capítulo se proporciona una guía de buenas prácticas para mejorar la seguridad de los ICS, incluidos los sistemas SCADA, los Sistemas de Control Distribuido (*Distributed Control Systems*, DCS) y otras configuraciones en sistemas de control como, por ejemplo, PLCs (*Programmable Logic Controllers*), al mismo tiempo que se abordan sus necesidades de rendimiento, confiabilidad y seguridad. Estos sistemas, son los encargados de administrar, ordenar, dirigir y/o regular toda la maquinaria y elementos que pueden encontrarse en las Infraestructuras Críticas, por lo que es de especial interés su securización, configuración y el diseño de la arquitectura de red en la que van a desplegarse.

A pesar del esfuerzo dedicado a la creación de normativas relativas a la seguridad en los SCI, para incrementar y reforzar la seguridad sobre estos, estas no han llegado a implementarse completamente, encontrándose la gran mayoría de ellas en fases de desarrollo y/o borrador en revisión, por lo que cabe esperar que, en un futuro no muy lejano, queden recogidos en ellas todos los cambios sufridos en los sistemas de control en estos últimos años. Uno de los estándares de seguridad más relevantes para este sector, es el IEC 62443, compuesto de trece documentos (IEC 62443-1-1 "*Models and Concepts*" , IEC TR 62443-1-2 "*Master Glossary of Terms and Abbreviations*", IEC 62443-1-3 "*System Security Compliance Metrics*", IEC TR 62443-1-4 "*Security Life Cycle and Use Cases*", IEC 62443-2-1 "*Requirements for an IACS Security Management System*", IEC TR62443-2-2 "*Operating a Control Systems Security Program*", IEC TR 62443-2-3 "*Patch Management in the IACS Environment*", IEC 62443-2-4 "*Certification of IACS supplier security policies and practices*", IEC TR62443-3-1 "*Security Technologies for IACS*", IEC 62443-3-2 "*Security Risk Assessment and System Design*", IEC 62443-3-3 "*System Security Requirements and Security Levels*", IEC 62443-4-1 "*Product Development Requirements*" e IEC 62443-4-2 "*Technical Security Requirements for IACS Components*"). Este estándar, profundiza en los conceptos planteados por ISA99 (normas que comenzaron a desarrollarse pretendiendo dar un mayor valor a la seguridad de los sistemas de control industrial, formada por quince documentos y centradas, principalmente, en la defensa en profundidad), extendiendo la seguridad a otros ámbitos, desde los fabricantes hasta los operadores [19].

El estudio y análisis para la aplicación de la ciberseguridad en entornos industriales y todos los conocimientos necesarios para el desarrollo de este capítulo han sido adquiridos consultando las fuentes [20], [21], [22], [23], [24] y [25].

3.1. Sistemas de Control Industrial

Los Sistemas de Control Industrial o ICS se forman mediante la combinación de componentes y dispositivos de control (eléctricos, mecánicos, hidráulicos, neumáticos, etc.), entre los que se encuentran los sistemas SCADA, DCS, PLCs, etc., encargados de administrar, ordenar, dirigir y/o regular el comportamiento de otros sistemas y actuando de forma conjunta para lograr un objetivo industrial (fabricación, transporte de materia o energía, etc.). Un ICS típico puede contener numerosos sistemas de control (que constan de sensores, *hardware* de controlador, actuadores, interruptores y mecanismos para la comunicación), interfaces hombre máquina y herramientas de diagnóstico y mantenimiento remotos utilizando una matriz de protocolos de red.

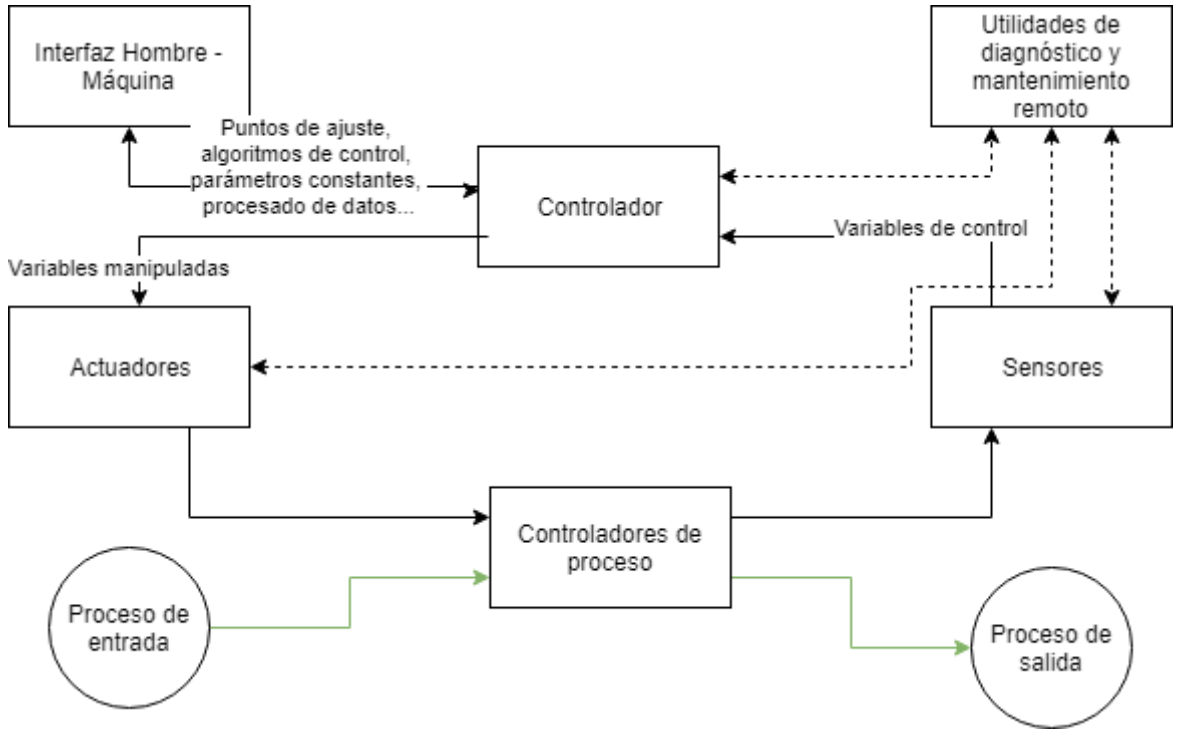


Figura 3.1: Ejemplo de operación básica de un ICS.

Estos sistemas se pueden configurar para operar en modo de circuito abierto (en los que la salida o resultado final está controlado por configuraciones prestablecidas), circuito cerrado (cuya salida tiene un efecto en la entrada) y manual (en los que el sistema es controlado completamente mediante acciones humanas). El control puede ser completamente automatizado o necesitar de una o varias personas.

Los ICS se utilizan en cualquier tipo de industria, como pueden ser las eléctricas, agua, petróleo, gas, química, transporte, farmacéutica, etc. y son elementos decisivos en el funcionamiento de las Infraestructuras Críticas, en las que, a menudo, se encuentran interconectados y dependen los unos de los otros.

En este apartado, se muestra una descripción general de los sistemas SCADA, DCS y PLC, incluidas las tipologías y componentes típicos. Además, se presentan varios diagramas para representar la topología de red, las conexiones, componentes y protocolos que suelen encontrarse en cada sistema para facilitar la comprensión de estos.

3.1.1. Funcionamiento y componentes de los ICS

Un ejemplo de operación básica de un ICS puede observarse en la Figura 3.1. Estos sistemas, típicamente, contienen numerosos sistemas de control, interfaces humanas y herramientas de mantenimiento y diagnóstico remoto creadas utilizando una matriz de

protocolos de red con arquitecturas de red por capas. Los sistemas de control utilizan sensores (dispositivos que producen medidas de alguna propiedad física y la envían como variables al controlador), actuadores (como, por ejemplo, válvulas de control, interruptores, motores, etc.) y controladores (como PLCs) para manipular los procesos controlados. El controlador interpreta las señales y genera las variables correspondientes, basadas en un algoritmo de control y unos puntos de ajuste de destino, que se transmiten a los actuadores, utilizados para manipular directamente el proceso controlado en función de los comandos dictados por el controlador.

Por otro lado, los operadores e ingenieros necesitan interfaces humanas para monitorear y configurar los algoritmos de control y los distintos parámetros del propio controlador. Esta interfaz, también sirve para mostrar información del estado del proceso e históricos. Las utilidades de diagnóstico y mantenimiento se utilizan para prevenir, identificar y recuperar el sistema de fallos u operaciones fuera de lo común.

En algunos casos, estos sistemas se encuentran anidados o en cascada, basando determinados puntos del procedimiento en variables de proceso de otros sistemas.

A continuación, se describen y detallan algunos de los componentes clave en los ICS: los historiadores de datos, los sistemas SCADA, los DCS y los PLCs.

3.1.2. Historiador de datos

Los historiadores de datos suelen ser programas *software* desplegados en servidores que se encargan de registrar y recuperar información de producción y proceso asociándola a un momento determinado. Almacenan la información, que puede ser, por ejemplo, sobre los sistemas de producción (como la temperatura, presión, tasas de flujo, niveles, pesos, etc.), información de los productos fabricados (identificador de los productos, de los lotes, del material, del lote de materia prima), etc. en una base de datos.

Estos sistemas recopilan información que puede provenir de muchas fuentes diferentes, entre las que se encuentran los PLCs, DCS, instrumentos de laboratorio, entradas realizadas de forma manual por los operarios, etc.

Los usos que pueden dársele a los historiadores de datos dependerán, en gran medida, de la industria u organización en la que se encuentren. Algunos de estos usos pueden ser, entre otros, el control de la fabricación (registrando los procesos, el estado de producción, supervisar el rendimiento, el control de calidad, los costes de fabricación, etc.), la observación de centros de datos (chequeando el rendimiento del entorno del servidor, la infraestructura de red, las

aplicaciones, etc.), la monitorización ambiental (clima, nivel del mar, condiciones atmosféricas, contaminación del agua, etc.) y la supervisión de quipos pesados (horas de funcionamiento, lecturas de instrumentos y equipos para el mantenimiento predictivo, etc.).

3.1.3. SCADA

Los sistemas SCADA se utilizan para el control de activos que se encuentran dispersos, en los cuales es importante tanto el control como la adquisición de datos de forma centralizada. Por ejemplo, estos sistemas son utilizados en distribuidoras de agua, servicios eléctricos, oleoductos, gaseoductos, sistemas ferroviarios, sistemas de transporte público y, en general, en cualquier sistema de distribución.

Estos sistemas, están diseñados para la recopilación de información, su transferencia a una instalación central para su procesamiento y el muestreo posterior de los resultados al operador (ya sea de forma gráfica o textual), permitiéndole, de esta forma, monitorizar y/o controlar todo un sistema desde una única ubicación central. Dependiendo de la sofisticación y configuración del sistema, el control, las operaciones y/o las tareas de este pueden ser automáticas o realizarse mediante comandos lanzados por el operador.

Típicamente, existe un servidor de control (ubicado en un centro de control), equipamiento de comunicaciones (radio, línea telefónica, cableado, satélite, etc.) y uno o más elementos que interactúan con el entorno, distribuidos geográficamente, que consisten en RTU (*Remote Terminal Units* o Unidades Terminales Remotas) y/o PLCs, encargados de controlar los actuadores y/o supervisar los sensores. Este servidor de control se encarga de almacenar y procesar la información de las distintas entradas y salidas de las RTU (enviadas a través del *hardware* de comunicaciones), mientras que las mencionadas RTU o los PLC controlan el proceso local. Por otra parte, el *software* será el encargado de comunicarle al sistema qué debe controlar y cuándo debe hacerlo, los rangos de parámetros aceptables y qué acción debe iniciarse cuando los parámetros cambien o se encuentren fuera de lo considerado como aceptable. Los Dispositivos Electrónicos Inteligentes (*Intelligent Electronic Device, IED*), como, por ejemplo, los relés de protección son capaces de comunicarse directamente con el servidor de control. Estos elementos, proporcionan una interfaz directa para poder controlar y monitorizar equipos y sensores, y, en la mayoría de los casos poseen una programación local que les permite actuar sin necesidad de recibir instrucciones directas del centro de control. Los sistemas SCADA, generalmente, están diseñados para ser tolerantes a fallos con redundancia integrada en el propio sistema, pero, en la mayoría de los casos, esta contramedida puede no ser suficiente ante un ataque malicioso.

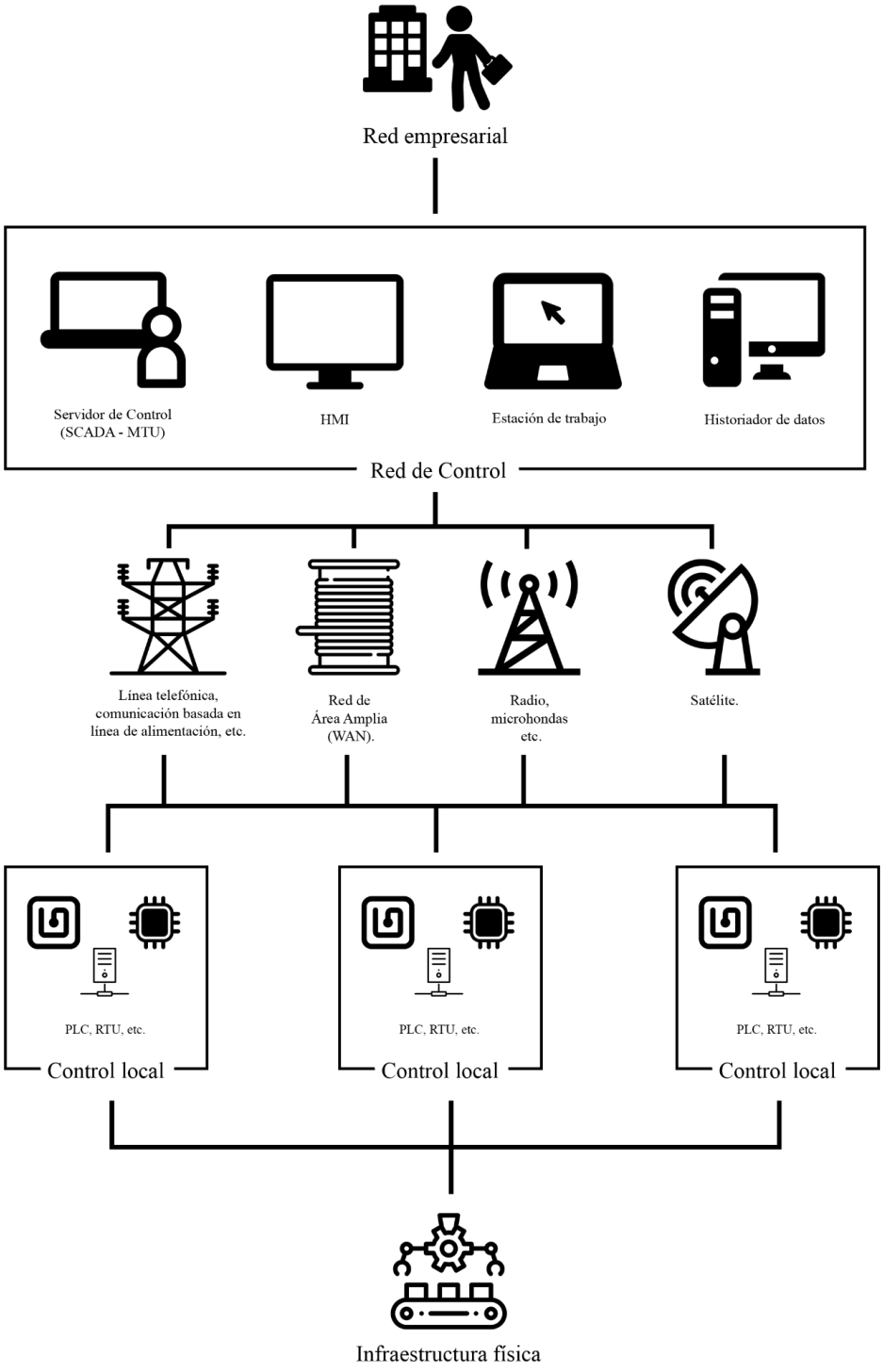


Figura 3.2: Escenario general con SCADA.

En la Figura 3.2 puede observarse un escenario en el que se utiliza un sistema SCADA. El centro de control, formado por un servidor de control, los enrutadores, la interfaz hombre – máquina (*Human-Machine Interface*, HMI), las estaciones de trabajo de los operadores e ingenieros y el historiador de datos, recopila y registra la información adquirida por los elementos que interactúan con el medio para mostrarla en la interfaz, pudiendo generar, además,

acciones en función de los eventos detectados. El centro de control también es responsable de las alarmas centralizadas, los análisis y los informes. Los espacios en los que se realizan los procesos locales (en muchos casos son accesibles remotamente para que los operadores puedan realizar diagnósticos y reparaciones a distancia a través de un módem de acceso telefónico o conexión WAN) realizan el control local de los actuadores y llevan a cabo la monitorización de los sensores. Para transportar la información entre el centro de control y los espacios en los que se realizan los procesos locales, se utilizan línea telefónica, cable, fibra, radio, satélite, etc.

La comunicación SCADA puede realizarse mediante diversas implementaciones, entre las que se encuentran punto a punto (la más simple, pero muy costosa debido a los canales individuales necesarios para cada conexión), serie (reduciendo los canales de conexión necesarios, pero disminuyendo la eficiencia y aumentando la complejidad por ello), estrella (con una menor eficiencia y una mayor complejidad del sistema), etc.

3.1.4. DCS

Los *Distributed Control Systems* o DCS son Sistemas de Control Industrial automatizados, diseñados especialmente para gobernar métodos de producción distribuidos por una misma planta o área de control. Generalmente, se utilizan en procesos o control de piezas en los que es necesario monitorizar y controlar gran cantidad de circuitos y maquinaria, por ejemplo, en refinerías de petróleo, potabilizadoras de agua, plantas eléctricas, plantas de fabricación de productos químicos, etc.

En estos sistemas, a diferencia de los sistemas de control centralizados (en los que un único controlador maneja la función de control al completo), cada una de las máquinas o grupo de máquinas es dirigida por un controlador dedicado, de tal manera que, si uno falla, puede seguirse operando. Además, estos controladores se comunican entre ellos a través de una red de comunicaciones de alta velocidad.

Los DCS se basan en la distribución de varias funciones de control en conjuntos de subsistemas (semiautónomos e interconectados). Algunas de estas funciones incluyen la adquisición de datos, su presentación, el control y la supervisión de procesos, la creación de informes, el almacenamiento y la recuperación de información, etc. Además, gracias a la integración de estrategias de control avanzadas, los DCS consiguen automatizar, por ejemplo, los procesos de fabricación. Estos sistemas también organizan toda la estructura de control como si de un sistema de automatización único se tratara, donde varios subsistemas se unifican a través de una estructura de comando y un flujo de información constante.

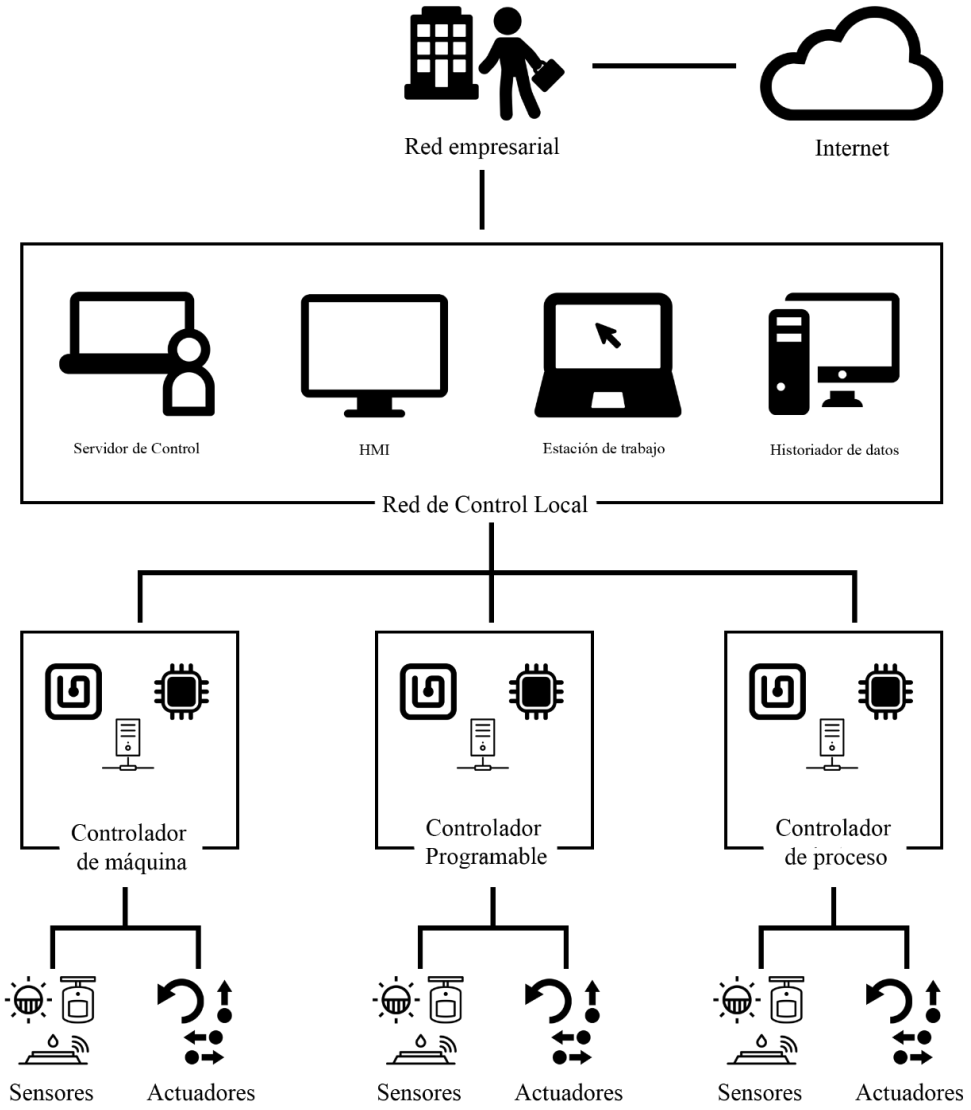


Figura 3.3: Escenario de ejemplo con DCS.

En la Figura 3.3, puede observarse la arquitectura y atributos del DCS. Entre sus elementos, pueden encontrarse la estación de trabajo de ingeniería, el HMI, las unidades de control de proceso o unidades de control local (en el ejemplo: controlador de máquina, programable y de proceso), los dispositivos inteligentes (sensores y actuadores) y los sistemas de comunicación. El funcionamiento de los DCS parte de los sensores, en los que se detecta la información del proceso, la cual es enviada a los módulos de entrada/salida local, a los que, además, están conectados los actuadores que controlan los parámetros del proceso. La información de estos módulos remotos se recopila en la unidad o servidor de control local. Por otro lado, la información recopilada se procesa y analiza, generando los resultados de salida en función de la lógica de control que se haya implementado y llevando los resultados o acciones de control de nuevo a los dispositivos actuadores. La configuración del DCS, su puesta en

marcha y la lógica de control se lleva a cabo en la estación de ingeniería, mientras que el operador puede ver y enviar acciones de control de forma manual desde los HMI.

3.1.5. PLC

Los PLC o *Programmable Logic Controllers* son componentes de control utilizados para proporcionar una gestión local de los procesos de forma automatizada, pudiendo utilizarse tanto en sistemas SCADA como DCS. Cuando se utilizan en sistemas SCADA, estos elementos pueden proporcionar la misma funcionalidad que los RTU, obteniendo señales de los distintos procesos y enviando esta información a la red de control. Si los PLC se emplean en DCS, estos se implementan como controladores locales dentro de un esquema de control de supervisión.

Los PLC, al margen de su uso en SCADA y DCS, pueden utilizarse también como controlador primario en configuraciones de sistemas de control de tamaño reducido, proporcionando control operacional de procesos tales como líneas de ensamblaje o empaquetado. Estas topologías difieren de SCADA o DCS en que, generalmente, carecen de un servidor de control central y una HMI, ofreciendo únicamente un control de circuito cerrado sin participación humana directa. Los PLC tienen una memoria programable por el usuario, en la que pueden almacenarse instrucciones con el fin de realizar acciones específicas (control de entrada y salida, temporización, conteo, comunicación, etc.).

Estos elementos poseen algunas características clave que merecen especial mención. Los PLC tienen módulos de entrada y salida, encargados de proporcionar información a la CPU y desencadenar resultados específicos. Los cuales, pueden ser analógicos o digitales y entre los dispositivos que se conectan a ellos pueden incluirse sensores, interruptores, medidores, relés, luces, válvulas, etc., siendo posible combinarlos de tal forma que se obtenga la configuración correcta para la aplicación buscada. Además, los PLC ofrecen una amplia gama de puertos y protocolos de comunicación para garantizar que estos sistemas puedan comunicarse con otros tales como los SCADA. Para poder interactuar en tiempo real con el PLC, también es necesario una HMI (que pueden ser pantallas simples, paneles táctiles grandes, etc.), permitiendo a los usuarios y empleados revisar e ingresar información en el PLC en tiempo real. En la Figura 3.4, obtenida de [26], pueden observarse las características descritas, además de la estructura interna de los PLC.

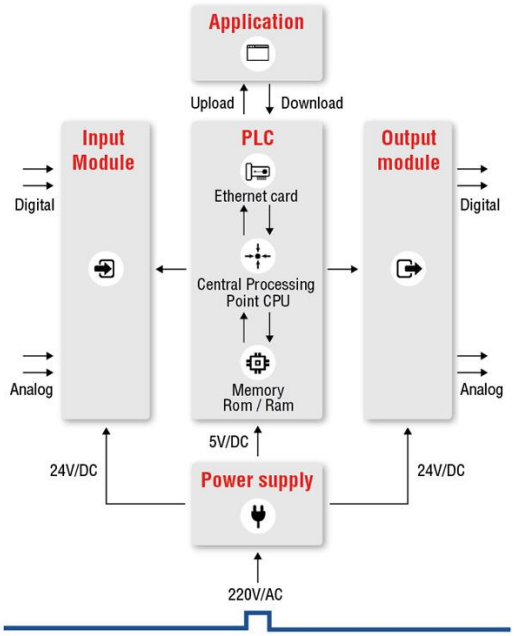


Figura 3.4: Funcionamiento y estructura de un PLC [26].

3.1.6. Diferencia entre SCADA y DCS

A pesar de que ambos sistemas son mecanismos de monitorización y control industrial, los SCADA y los DCS tienen diferentes objetivos. Por un lado, los DCS se orientan al proceso, escaneándolo de forma regular, haciendo un mayor énfasis en el control de este y en el nivel de supervisión, mostrando la información relacionada como parte de ello y utilizándose, generalmente, para procesos de control complejos. Sin embargo, SCADA está orientado a la recopilación de datos, centrando su utilidad en mostrar a los operadores y al centro de control los datos del proceso de adquisición e impulsado por eventos, evitando el análisis del proceso de forma secuencial, esperando un evento que haga que el parámetro del proceso active ciertas acciones. De esta forma, DCS no requiere mantener una base de datos de valores de parámetros de proceso, mientras que para la utilización de SCADA es necesaria para registrar los valores de parámetros que pueden requerirse por parte del operador.

Por otra parte, en DCS los módulos o controladores de adquisición y control de datos generalmente se encuentran dentro de un área más aislada (como una planta o fábrica) y la comunicación entre varias DCS se realiza a través de una red de área local. SCADA, sin embargo, suele cubrir áreas geográficas más grandes (utilizando distintos sistemas de comunicación a lo largo de miles de kilómetros, siendo estos, normalmente, menos confiables que una red de área local) y dado que existen retrasos a la hora de transmitir los datos a la sala de control (por tener que transmitirse vía satélite, radio, etc.), el control en tiempo real se realiza apoyándose en RTU y/o PLC.

3.2. Arquitectura de seguridad de los ICS

A la hora de diseñar una arquitectura de red para una implementación de ICS, generalmente, es recomendable separar la red del ICS de la red corporativa de la empresa, ya que la naturaleza del tráfico de estas dos redes es muy diferente. En la primera, no debería permitirse el acceso a Internet, FTP, correo electrónico, etc., mientras que en la segunda sí. Si el tráfico correspondiente a la red del ICS se propagara o transmitiera por la red corporativa, este podría ser interceptado o sufrir ataques DoS (ataques de denegación de Servicio o *Denial of Service*) o MitM (*Man in the Middle*, en el que un atacante adquiere la capacidad de interceptar mensajes entre dos víctimas, pudiendo leerlos y modificarlos a su antojo). De esta forma, si las redes se mantienen separadas, los problemas de seguridad y rendimiento en la red corporativa no deberían afectar a la del ICS.

En caso de que las dos redes no puedan ser separadas (por ejemplo, por el alto coste de implantar esta arquitectura), deben permitirse las conexiones mínimas necesarias y realizar esta conexión entre ambas redes a través de un cortafuegos y una DMZ (*Demilitarized Zone*, segmento de red separado que se conecta directamente al cortafuegos), a la que se conectarán los servidores que contienen los datos del ICS. Por otra parte, el cortafuegos deberá estar correctamente configurado para permitir las conexiones imprescindibles mencionadas.

En los siguientes apartados, se detallan algunas de las consideraciones en materia de arquitectura que deben tenerse en cuenta a la hora de aplicar y diseñar redes industriales que contengan ICS.

3.2.1. Segmentación y segregación de la red

La segmentación y la segregación son uno de los conceptos más efectivos en materia de arquitectura de red que una organización puede implementar para la protección de sus ICS. Estas técnicas, pueden dificultar el acceso a los atacantes, así como proteger y contener los efectos provocados por errores y accidentes no intencionados.

El objetivo de la segmentación y la segregación de la red es minimizar el acceso a la información a aquellos sistemas y personas que no lo requieren, garantizando, a su vez, que la organización pueda seguir funcionando correctamente y de forma efectiva.

Los entornos ICS, a menudo, tienen múltiples dominios bien definidos (tales como redes operacionales, redes de control, DMZ operacionales, etc.) y pasarelas a otros entornos menos confiables que no son ICS (como Internet, redes corporativas, etc.). La segregación de la red implica el desarrollo y la aplicación de un conjunto de reglas que controle qué comunicaciones

se permiten y a través de qué dominios. Generalmente, estas reglas se basan en la identidad del origen, la del destino y el tipo o contenido de los datos que se van a transferir, por lo que conocer la cantidad de tráfico que cruza de un dominio a otro es un buen indicador para definir los límites de estos dominios.

Para garantizar tanto la segmentación como la segregación de red, pueden utilizarse distintas tecnologías y métodos, que dependerán de la arquitectura y la configuración de la red utilizadas. Algunos ejemplos aplicables son:

- Separar la red de forma lógica mediante encriptación o particionamiento forzado por dispositivos de red, utilizando, entre otras, Redes de Área Local Virtuales (VLANS, *Virtual Local Area Network*), Redes Privadas Virtuales (VPN, *Virtual Private Network*) cifradas (que utilizan mecanismos criptográficos para separar el tráfico de una red a pesar de que, realmente, el tráfico transcurre por la misma red), pasarelas unidireccionales (que realizan la comunicación entre distintas conexiones en una sola dirección, segmentando así la red).
- Separación de la red de forma física para evitar la interconexión del tráfico entre dominios.
- Filtrado del tráfico de red, que, a su vez, puede ser de varios tipos:
    - Filtrado del tráfico en la capa de red. De esta forma, pueden restringirse los sistemas que requieren comunicarse con otros en función de la información de ruta y la dirección IP.
    - Filtrado basado en el estado. Pueden limitar los sistemas que requieren comunicarse con otros en función del estado actual de los mismos y/o el cometido previsto.
    - Filtrado basado en el puerto y/o el protocolo. Restringiendo la cantidad y el tipo de servicios que cada sistema puede utilizar con otros sistemas dentro de la red.
    - Filtrado del tráfico en la capa de aplicaciones. Son capaces de restringir los sistemas y sus comunicaciones según el contenido del tráfico basándose en la capa de aplicación. Este tipo de filtrado puede llevarse a cabo mediante cortafuegos a nivel de aplicación, *proxys*, filtros basados en el contenido, etc.

Para implementar una buena segmentación y segregación de la red, es necesario y recomendable aplicar tecnologías en varias capas de la topología de red (de ser posible, desde la capa de enlace hasta la de aplicación), usar los principios de mínimo privilegio, separar la información y la infraestructura en función de los requisitos de seguridad e implementar listas blancas en lugar de listas negras (las cuales permiten bloquear todo el tráfico por defecto, permitiéndose únicamente lo imprescindible).

3.2.2. Fronteras

Los dispositivos de control de las fronteras se encargan de comprobar los flujos de información que fluyen entre los distintos dominios interconectados, siendo su objetivo principal la protección de los ICS contra atacantes y/o errores o accidentes no intencionados. Entre estos dispositivos, se incluyen las puertas de enlace, los enrutadores, los cortafuegos, los analizadores de *malware* basados en red, los sistemas de detección de intrusos, las pasarelas de correo, las pasarelas unidireccionales (como, por ejemplo, los diodos de datos), etcétera.

Para la implantación de las fronteras, en primer lugar, es necesario decidir qué dominios permitirán una comunicación directa entre ellos, las políticas que regirán la comunicación permitida, los dispositivos a utilizar para aplicar la política y la topología que se requerirá para ello, que, normalmente, se basará en la relación de confianza entre los distintos dominios. Dicha confianza implica el grado de control que la organización tiene sobre cada uno de los dominios (dominios de la organización, proveedores de servicios contratados, Internet, etc.), que no será igual para todos.

Los dispositivos de control de las fronteras se organizan de acuerdo con la arquitectura de seguridad de la organización, estando modelada, comúnmente, por una zona desmilitarizada (DMZ) y/o un *host* o segmento de red formando una “zona neutral” entre los dominios de seguridad. Su objetivo es el de hacer cumplir la política de seguridad del dominio del ICS para poder intercambiar información con el exterior y, a su vez, proporcionar un acceso restringido a dicho dominio desde fuera, protegiéndolo de las amenazas externas.

Las consideraciones arquitectónicas, así como las funciones que deben realizar los dispositivos de control de fronteras para mantener una comunicación segura entre dominios son:

- De forma predeterminada, denegar todo el tráfico y permitir el estrictamente necesario. Esto se conoce como una política de lista blanca.

- Utilizar *proxys* como intermediarios para que los dominios externos le soliciten a este todos los recursos que requieran del dominio del ICS. El *proxy*, se encargará de evaluar y administrar estas peticiones limitando la conectividad.
- Prevenir la filtración de información mediante, por ejemplo, cortafuegos de inspección de paquetes. Estos dispositivos, se encargan de verificar el cumplimiento de los formatos de protocolo y las especificaciones dentro de la capa de aplicación, identificando vulnerabilidades que no pueden ser detectadas por dispositivos de la capa de red o de las capas de transporte.
- Permitir la comunicación únicamente entre pares de direcciones IP origen-destino autorizados y autenticados.
- Utilizar DMZ para aislar los ICS evitando, entre otras, que los atacantes descubran las técnicas de análisis que se emplean en la organización.
- Ocultar las direcciones de red de los componentes del ICS en los servidores DHCP (*Dynamic Host Configuration Protocol*) y deshabilitar los servicios y protocolos de control y solución de problemas, especialmente aquellos que emplean mensajes de difusión. De esta forma se evita la exploración de la red por parte de los atacantes.
- Configurar los dispositivos de control de las fronteras para que fallen e informen cuando se encuentren en determinados estados.
- Configurar los distintos dominios con direcciones de red separadas (como subredes disjuntas).
- Deshabilitar la retroalimentación a los remitentes cuando haya un error en el formato de validación, evitando, de este modo, que los posibles atacantes obtengan información relevante de los sistemas.
- Implementar flujos de datos unidireccionales, especialmente entre los distintos dominios.

Tipo	Funcionamiento	Ventajas / Desventajas
Filtrado de paquetes	Son dispositivos de enrutamiento que incluyen funcionalidad de control de acceso para direcciones de sistema y sesiones de comunicación. El control de acceso se rige por un conjunto de reglas. En su forma más básica, los filtros de paquetes operan en la capa 3 del modelo OSI (*Open Systems Interconnect*). Este tipo de *firewall* verifica la información básica de cada paquete (como las direcciones IP) contra un conjunto de criterios antes de reenviarlo.	Tienen un bajo coste y un pequeño impacto en el rendimiento de la red. Generalmente, sólo examinan uno o unos pocos campos de encabezado en el paquete.
Inspección con estado	Son filtros de paquetes que incorporan conocimiento adicional de los datos del modelo OSI en la capa 4. Filtran paquetes en la capa de red, determinan si los paquetes de sesión son legítimos y evalúan el contenido de los paquetes en la capa de transporte. La inspección con estado realiza un seguimiento de las sesiones activas y utiliza esta información para determinar si los paquetes deben reenviarse o bloquearse.	Ofrece un alto nivel de seguridad y un buen rendimiento. Puede ser costoso y complejo de administrar. Se pueden requerir conjuntos de reglas adicionales para su aplicación en los ICS.
Capa de aplicación	Examinan los paquetes en la capa de aplicación y filtran el tráfico en función de reglas específicas, determinando si puede realizarse la comunicación, por ejemplo, dependiendo de la aplicación *software* que la requiere o los protocolos utilizados en la misma.	Pueden ser muy eficaces para evitar ataques a los servicios de configuración y acceso remoto proporcionados por los componentes de los ICS. Pueden tener cierto impacto en el rendimiento de la red, en ocasiones inaceptable en un entorno de ICS.

Tabla 3.1: Clases generales de cortafuegos.

3.2.3. Cortafuegos

Los cortafuegos o *firewalls* son dispositivos encargados de controlar el tráfico que circula entre distintas redes. Los cortafuegos pueden aplicarse en entornos de red que incluyen o requieren conectividad a Internet, pero también pueden hacerlo en entornos en los que no exista dicha conectividad. Existen tres clases generales de *firewalls*, cuya descripción puede observarse en la Tabla 3.1.

En la mayoría de los casos, en los entornos de ICS, los cortafuegos se despliegan entre la red del ICS y la corporativa. Si se configuran de forma adecuada, estos son capaces de restringir en gran medida el acceso no autorizado hacia y desde los equipos y controladores, mejorando de esta forma la seguridad. También pueden aumentar la capacidad de respuesta de una red de control eliminando el tráfico no esencial en esta. Por lo tanto, puede decirse que cuando se diseñan, configuran y mantienen adecuadamente, los cortafuegos pueden contribuir significativamente a aumentar la seguridad de los entornos de ICS.

Además de lo descrito, los *firewalls* también son capaces de:

- Bloquear todas las comunicaciones, a excepción de las que hayan sido habilitadas específicamente entre los dispositivos de una subred desprotegida y las redes de los ICS, pudiendo basarse, entre otros, en pares de direcciones IP origen-destino, en servicios, puertos, estado de la conexión, las aplicaciones, etc.
- Hacer cumplir la autenticación de todos los usuarios que quieren acceder a la red del ICS mediante el uso de contraseñas, tecnologías de autenticación de múltiples factores, *tokens*, biometría, etc.
- Hacer cumplir la autorización del destino, pudiendo restringir a los usuarios y permitiéndoles el acceso únicamente a los nodos o sistemas de la red de control necesarios para poder desempeñar su trabajo.
- Monitorizar, analizar y detectar el tráfico en busca de intrusos.
- Permitir que el ICS implemente políticas operativas apropiadas que podrían no serlo para una red informática, por ejemplo, prohibir las comunicaciones poco seguras como el correo electrónico.
- Diseñar conexiones documentadas y mínimas, dentro de lo posible, que permitan que la red del ICS se mantenga separada de la red corporativa.

El uso de cortafuegos a nivel de dispositivo puede generar una sobrecarga de administración excesiva, especialmente en la gestión de cambios y configuraciones. Por otro lado, los cortafuegos basados en *hardware* requieren un soporte continuo, un elevado mantenimiento y un alto respaldo para conservar los conjuntos de reglas actualizados, brindando la protección adecuada a la luz de las amenazas de seguridad nacientes.

A la hora de implementar *firewalls* en entornos de ICS, además de las dificultades asociadas a la falta de experiencia en el diseño de conjuntos de reglas adecuadas para aplicaciones industriales que suelen encontrarse, pueden presentarse demoras en las comunicaciones por tenerse que controlar el tráfico de red.

3.2.4. Separación lógica de la red de control

Como requisito mínimo, la red del ICS debe estar separada lógicamente de la red corporativa, en dispositivos de red físicos independientes. En los casos en los que se utilice esta arquitectura, es necesario que esta:

- Contenga puntos de acceso documentados y mínimos entre la red del ICS y la corporativa. Si existen puntos de acceso de respaldo o apoyo, estos también han de estar documentados.

- Incluya un cortafuegos de inspección de estado entre la red del ICS y la corporativa, configurado para denegar todo el tráfico excepto el explícitamente autorizado.

- Tenga reglas de cortafuegos que proporcionen, como mínimo, filtrado de código, por dirección MAC (*Media Access Control*) y por protocolo TCP/UDP e ICMP.

Para permitir la comunicación entre la red del ICS y la corporativa, podría desplegarse una DMZ intermedia, conectada al cortafuegos de manera que pueda existir una comunicación restringida entre la red corporativa y la DMZ y la red del ICS y la DMZ (evitando la comunicación directa entre la red corporativa y la del ICS). Además, la adición de una VPN (*Virtual Private Network*) podría añadir seguridad adicional a la hora de conectar la red del ICS con redes externas. En los próximos apartados se estudiarán estos aspectos.

3.2.5. Segregación de red

La segregación de la red es una de las técnicas más utilizadas a la hora de mejorar la seguridad de los ICS. Para segregar una red, pueden utilizarse diferentes arquitecturas, técnicas y configuraciones, entre las que cabe destacar:

- Los equipos de doble acceso y/o tarjetas de red duales. Estos elementos son capaces de transportar el tráfico de una red a otra (actuando como cortafuegos). Para evitar amenazas adicionales, deben seguirse unos controles de seguridad sobre estas máquinas, además, todo el tráfico y las conexiones entre la red de control y la red corporativa debe realizarse a través de ellos.

- Cortafuegos entre la red corporativa y la de control. Mediante esta técnica, se puede lograr una importante mejora de seguridad, consiguiendo, si el *firewall se* configura correctamente, una significativa reducción de la probabilidad de éxito en un ataque lanzado desde la red de control.

  En caso de que el historiador de datos se encuentre en la red corporativa, será necesario permitir que este se comunique con los dispositivos de la red de control, con lo cual, un *host* o máquina maliciosa (o configurada incorrectamente), haciéndose pasar por el historiador de datos, podría reenviar paquetes a PLCs, DCS, etc.

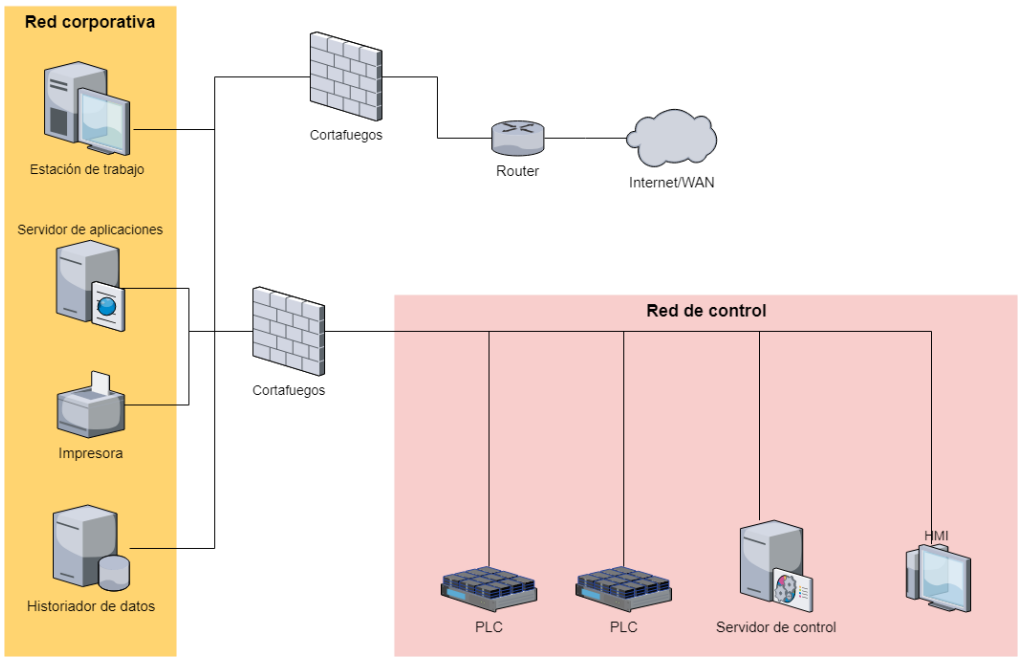


Figura 3.5: Cortafuegos entre la red corporativa y la red de control.

Si el historiador de datos se encuentra en la red de control, es necesaria la existencia de una regla en los cortafuegos que permita que todos los *host* o máquinas de la empresa se comuniquen con este. Normalmente, estas solicitudes o comunicaciones se producen en la capa de aplicación, por lo que un fallo en estas aplicaciones o en su código podría comprometer el historiador, y, tras ello, el resto de los nodos de la red de control pasarían a ser vulnerables a la propagación de un gusano o cualquier otro tipo de ataque.

Por tanto, a pesar de que esta arquitectura mejora considerablemente una red si se compara con una no segregada, requiere el uso de reglas en los cortafuegos que permitan comunicaciones directas entre la red corporativa y los dispositivos de control de red, pudiendo dar lugar a posibles fallos de seguridad si no se diseñan y supervisan correctamente. En la Figura 3.5 puede observarse un ejemplo de este tipo de arquitectura.

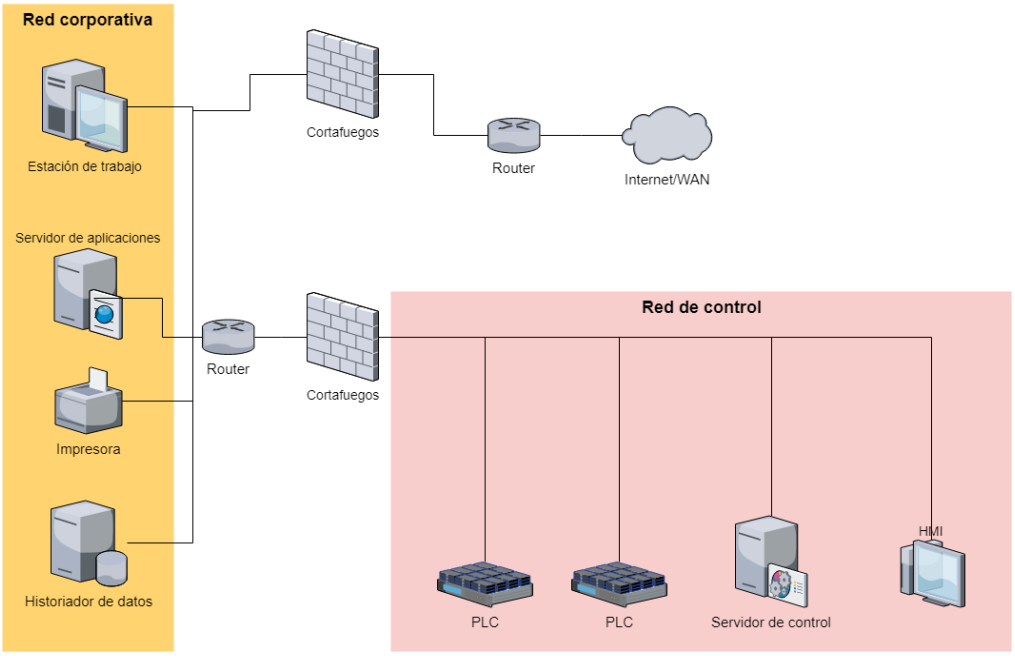


Figura 3.6: Cortafuegos y enrutador entre la red corporativa y la red de control.

- Cortafuegos y enrutador entre la red corporativa y la de control. La combinación de estas dos herramientas, situando el enrutador frente al cortafuegos, y ofreciendo servicios básicos de filtrado de paquetes (mientras que el cortafuegos se encarga de manejar los problemas más complejos mediante inspección de estado o técnicas de *proxy*). Este tipo de arquitectura es habitual en los cortafuegos orientados a Internet, ya que permite que el enrutador maneje, de forma más rápida, la mayor parte de los paquetes entrantes (evitando, por ejemplo, ataques de denegación de servicio), consiguiendo de esta forma una reducción de la carga del cortafuegos y ofreciendo una mejor defensa en profundidad por los dos dispositivos que la conforman. Un ejemplo de arquitectura de red utilizando esta técnica puede observarse en la Figura 3.6.

- Cortafuegos con DMZ entre la red corporativa y la de control. Una mejora significativa sería el uso de cortafuegos con la capacidad de establecer una DMZ entre la red corporativa y la de control, permitiendo la creación de una red intermedia. Se trata de que cada DMZ contenga uno o más componentes críticos, como, por ejemplo: el historiador de datos, el punto de acceso inalámbrico, los sistemas de acceso remoto, etc.

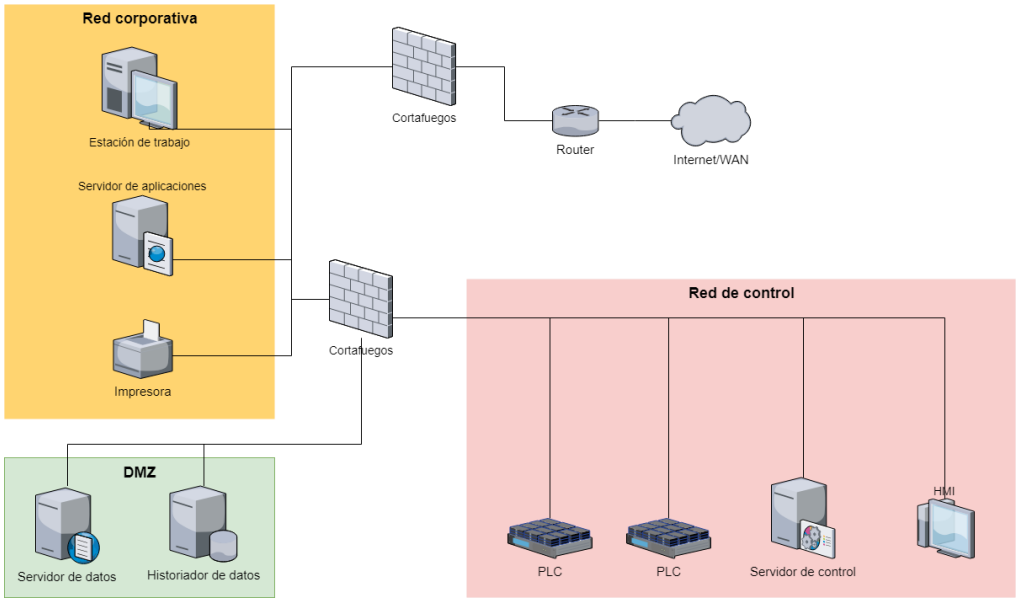


Figura 3.7: Cortafuegos con DMZ entre la red corporativa y la red de control.

Para ello, el cortafuegos debe tener tres o más interfaces de red, la primera, tiene que conectarse a la red corporativa, la segunda a la de control y las interfaces restantes a los dispositivos inseguros de la DMZ. Al colocar los componentes que deben ser accesibles desde la red corporativa en la DMZ, no se requieren rutas de comunicación directas entre la red de control y la red corporativa (pudiendo el cortafuegos bloquear paquetes destinados a la red de control y regular el tráfico de otras zonas de red). Mediante conjuntos de reglas bien planificados, se puede mantener una separación clara entre la red de control y otras redes, con poco o ningún tráfico entrante en esta.

Esta arquitectura presenta el riesgo de que, si un equipo de la DMZ se ve comprometido, puede utilizarse para atacar la red de control (aprovechando el tráfico permitido). Este riesgo, puede reducirse endureciendo y aplicando parches a los servidores de la DMZ. Por otra parte, existe una complejidad añadida a la hora de configurar y desplegar esta arquitectura, además de un incremento en el coste si se compara con arquitecturas de cortafuegos y/o cortafuegos con enrutador. Sin embargo, la seguridad que aporta en sistemas más críticos es algo que debe tenerse en cuenta.

En la Figura 3.7 puede observarse un modelo general de este tipo de arquitectura.

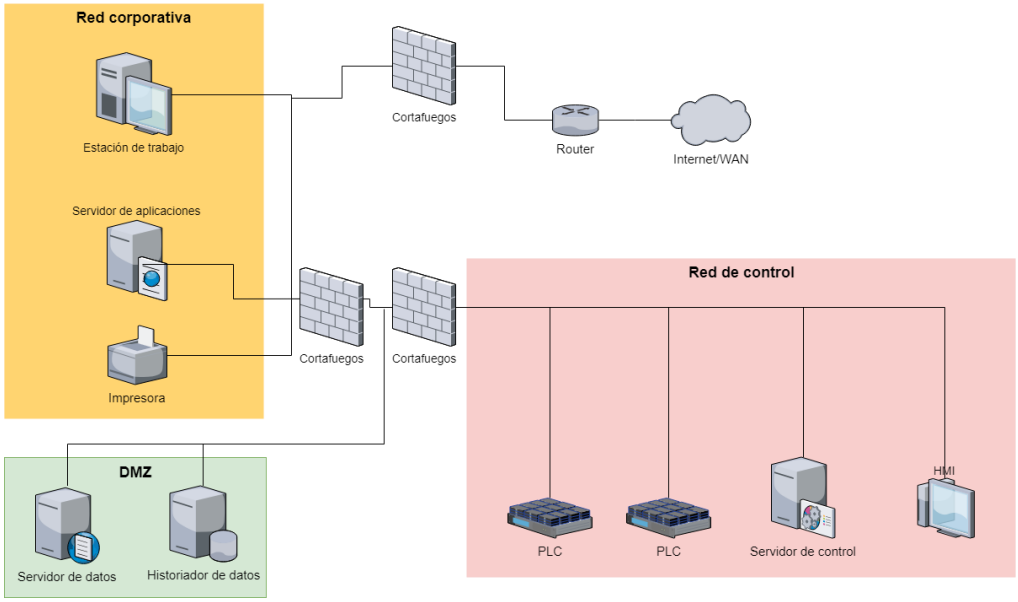


Figura 3.8: Doble cortafuegos con DMZ entre la red corporativa y la red de control.

- Doble cortafuegos entre la red corporativa y la red de control. Pueden utilizarse dos cortafuegos para crear una solución DMZ, situándolos entre la red corporativa y la del ICS, ubicando los servidores o servicios más críticos (tal como el historiador de datos) entre los dos *firewalls*. El primer cortafuegos bloquea los paquetes provenientes de la red de control, permitiendo únicamente el acceso a los servidores estrictamente necesarios situados en la DMZ, mientras que el segundo cortafuegos debe configurarse para evitar el tráfico no deseado de un servidor comprometido ubicado en la red de control, evitando de esta forma que el tráfico de la red de control afecte a los servidores compartidos.

  Esta arquitectura, permite que el departamento encargado del ICS y el de tecnologías de la información tengan una responsabilidad sobre los dispositivos claramente separada, pudiendo administrar cada uno un *firewall*. Sin embargo, su despliegue aumenta el coste final (ya que se requieren dos cortafuegos) y la complejidad de la administración.

  La Figura 3.8 muestra un ejemplo básico de este tipo de arquitectura.

En resumen, las soluciones que no se basan en cortafuegos, generalmente, no proporcionan un aislamiento adecuado entre las redes de control y las corporativas. Las soluciones sin DMZ, son aceptables, pero deben implementarse prestando una considerable atención. Las redes de control más seguras, manejables y escalables son aquellas que se basan en sistemas de al menos tres zonas, incorporando una o más DMZ.

3.2.6. Defensa en profundidad

Una protección adecuada de un ICS requiere una estrategia que cubra varias capas e involucre dos o más mecanismos de seguridad superpuestos (cortafuegos, DMZ, detectores de intrusos, políticas de seguridad efectivas, programas de concienciación del personal, mecanismos de respuesta a incidentes, etc.). Esta técnica se conoce como defensa en profundidad, y minimiza el impacto ante un fallo en cualquiera de los mecanismos.

Para poder implementar una estrategia efectiva de defensa en profundidad, es necesario tener en cuenta todos los posibles vectores de ataque que podría tener un ICS, entre los que se encuentran las puertas traseras y los agujeros en el perímetro de la red, las vulnerabilidades en los protocolos comunes, los posibles ataques a dispositivos y bases de datos, el secuestro de comunicaciones, los ataques de *Man in the Middle*, etc.

En la Figura 3.9, se presenta una estrategia de defensa en profundidad de un entorno ICS propuesta por "*Homeland Security*" en el documento "*Recommended Practice: Improving Industrial Control System Cybersecurity with Defense-in-Depth Strategies*" [27]. En este documento, además, se proporciona cierta orientación para llevar a cabo el desarrollo de estrategias de arquitectura mediante la defensa en profundidad dentro de organizaciones que utilizan redes de sistemas de control, manteniendo una arquitectura de información de múltiples niveles que requiere el mantenimiento de equipos, la recolección de telemetría y/o sistemas de procesos de nivel industrial, acceso a las instalaciones a través de un enlace de datos remoto o módem y servicios públicos para operaciones corporativas o de los clientes.

Esta arquitectura incluye cortafuegos, DMZ y detectores de intrusos en toda la red del ICS. La utilización de varias DMZ brinda la capacidad de separar funcionalidades y privilegios de acceso, además, ha demostrado ser muy eficaz en la protección de grandes arquitecturas compuestas por redes con diferentes mandatos operativos. Los sistemas de detección de intrusos aplican diferentes conjuntos de reglas y firmas para cada uno de los dominios que se supervisan.

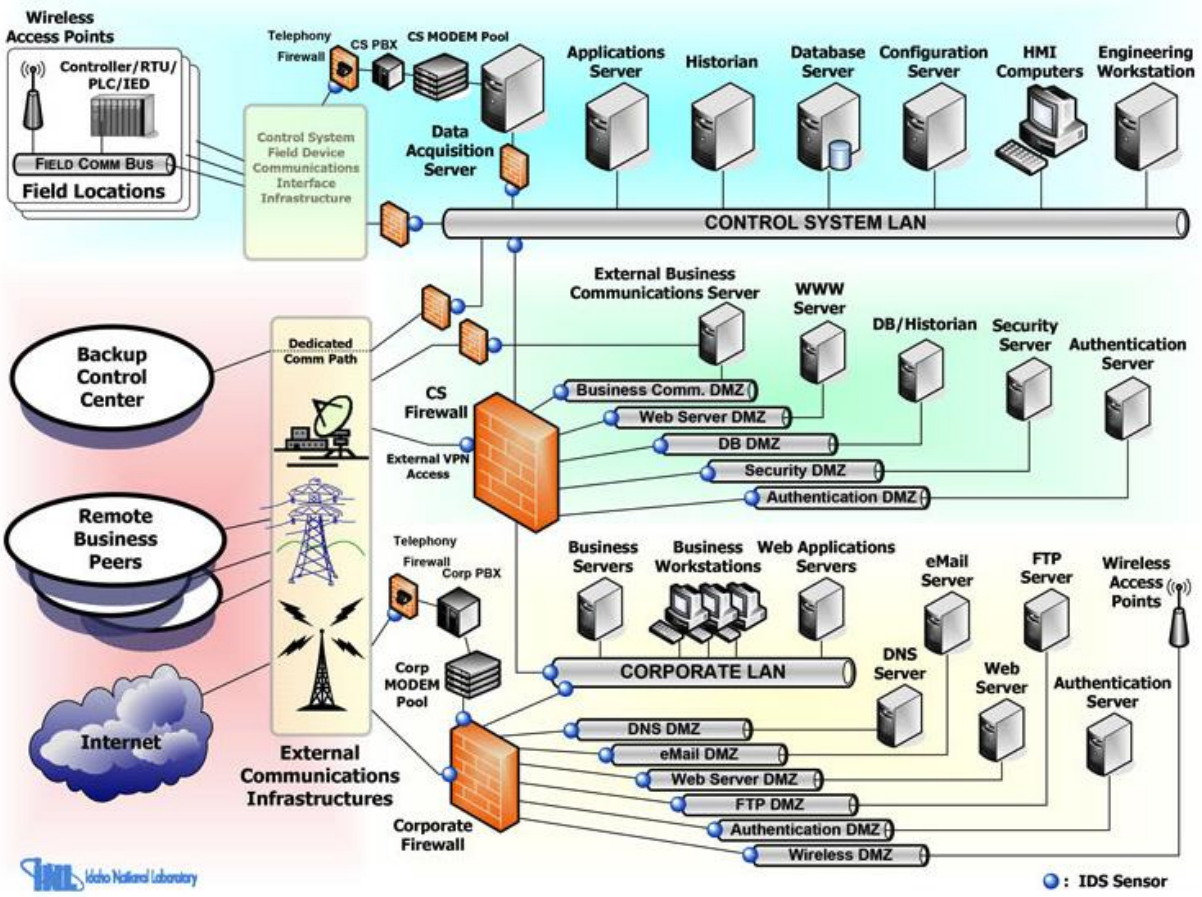


Figura 3.9: Arquitectura recomendada por el ICS-CERT para la defensa en profundidad [27].

3.2.7. Reglas generales para los cortafuegos

Para determinar el tráfico que debe transcurrir y cuál no a través de los cortafuegos, es recomendable, en primera instancia, denegarlo todo y permitir únicamente el tráfico absolutamente necesario para cumplir con las necesidades de la organización.

Cuando se instala un **único cortafuegos** (con dos tarjetas de red) y sin una DMZ, es preciso tener un especial cuidado a la hora de crear las reglas. Como mínimo, estas deben ser con estado, específicas para cada una de las direcciones IP y el puerto, permitiendo el tráfico entrante a la red de control a un conjunto muy reducido de dispositivos (por ejemplo, el historiador de datos) desde la red corporativa. Además, los puertos permitidos deben restringirse cuidadosamente a protocolos relativamente seguros (tales como HTTPS, *Hypertext Transport Protocol Secure*) y no permitir el acceso a otros menos seguros (como HTTP, FTP, etc.). Por último, también ha de considerarse que las reglas de los cortafuegos no permitan iniciar conexiones hacia la red de control desde fuera de esta (únicamente se debería permitir establecer conexiones desde la red de control hacia fuera, no de fuera hacia dentro).

Cuando se utiliza la **arquitectura con DMZ**, debe configurarse el tráfico para que no vaya directamente desde la red corporativa a la red de control (y viceversa), contando con algunas excepciones. Todo el tráfico de cualquiera de las redes (corporativa o de control) podría llegar a los servidores de la DMZ, permitiendo una mayor flexibilidad en los protocolos permitidos a través de los cortafuegos. Por ejemplo, los PLC podrían comunicarse con el historiador de datos mediante TCP y el historiador de datos podría hacerlo con los clientes de la empresa vía HTTP. A pesar de ser ambos protocolos inseguros, ninguno de los dos cruzaría las dos redes, por lo que se estarían utilizando de forma segura. Por lo tanto, no debe permitirse que un mismo protocolo pueda utilizarse entre la red de control y la DMZ y entre la DMZ y la red corporativa, reduciendo gracias a esta restricción, las posibilidades de que un *malware* o gusano llegue a la red de control, ya que el gusano o el *malware* debería usar dos protocolos diferentes.

Tanta importancia tiene el control del tráfico entrante a la red de control, como el saliente de esta, debido a que podría emplearse, por ejemplo, un troyano que utilice el túnel HTTP para explotar reglas de salida mal definidas. Una buena práctica sería el bloqueo del tráfico entrante al sistema de control (teniendo en cuenta que el acceso a los activos que lo componen debe hacerse a través de la DMZ) y la limitación del tráfico de salida desde la red de control a comunicaciones esenciales y estrictamente necesarias (restringidas por origen y destino, servicio y puerto).

A pesar de que cada entorno de control es diferente, y debe ser evaluado individualmente antes de implementar cualquier conjunto de reglas en los cortafuegos, es recomendable considerar las siguientes prácticas a la hora de implementarlas:

- Las reglas, en primer lugar, deben denegar todo para, posteriormente, ir permitiendo lo estrictamente necesario.
- Los puertos y servicios entre la red de control y la red corporativa deben habilitarse y otorgarse uno por uno, debiendo existir una justificación del porqué deben estar disponibles (documentada con un análisis de riesgos).
- Todas las reglas que permitan el acceso deben ser específicas para cada dirección IP, el puerto (TCP y/o UDP), y, si es necesario, el estado.
- Todas las reglas deben restringir el tráfico a una dirección o un rango de direcciones específico, nunca a la red completa.
- Debe evitarse el tráfico directo entre la red de control y la red corporativa.

- Los protocolos permitidos entre la red de control y la DMZ no deben permitirse entre la DMZ y las redes corporativas (y viceversa).
- Los paquetes de salida de la red de control o la DMZ deben permitirse solo si estos tienen una dirección IP origen correcta asignada a la red de control o los dispositivos de la DMZ.
- La red de control no debe tener acceso a Internet.
- La gestión de los cortafuegos debe llevarse a cabo desde una red segura o encriptada con autenticación multifactor, debiendo estar restringido, además, por la dirección IP de las estaciones de administración que vayan a utilizarse para estos menesteres.
- Todas las reglas de los cortafuegos deben revisarse periódicamente.

3.2.8. Reglas de servicios específicos para los cortafuegos

Además de las reglas generales, presentadas en el anterior apartado (3.2.7 Reglas generales para los cortafuegos), deben crearse reglas especiales para los cortafuegos, que variarán dependiendo de la organización, los protocolos y los servicios utilizados en ellas. A continuación, se exponen algunos consejos sobre los protocolos más utilizados en entornos industriales en términos de función, riesgo de seguridad, impacto y medidas sugeridas:

- Sistemas de nombres de dominio (*Domain Name System*, DNS). Este sistema, se utiliza para traducir entre nombres de dominio y direcciones IP. La mayoría de los servicios de Internet dependen del DNS, pero su uso en la red de control no suele ser habitual. Por lo tanto, las solicitudes de DNS desde la red de control a la DMZ deben abordarse caso por caso, y, en la mayoría de las ocasiones, prohibirse y/o utilizar un DNS local o archivos *host*.
- Protocolo de Transferencia de Hipertexto (*Hypertext Transfer Protocol*, HTTP). Es el protocolo más característico de los servicios de navegación web en Internet. Como ocurre con el DNS, es fundamental en la mayoría de los servicios de Internet, aunque, cada vez más, también se utiliza para la comunicación de dispositivos de control. Este protocolo tiene poca seguridad y muchas aplicaciones HTTP contienen vulnerabilidades explotables fácilmente. En general, no debería permitirse que HTTP cruce de la red corporativa a la red de control, pero, si es estrictamente necesario, debe controlarse con una lista blanca, restringirse este acceso por origen-destino, aplicar una autorización de acceso al

servicio en la capa de aplicación, utilizar únicamente las tecnologías necesarias, verificar el servicio de acuerdo con las prácticas de seguridad de aplicaciones conocidas, registrar todos los intentos de uso del servicio y utilizar HTTPS siempre que sea posible.

- Protocolo de Transferencia de Archivos (*File Transfer Protocol*, FTP) y Protocolo de Transferencia de Archivos Trivial (*Trivial File Transfer Protocol*, TFTP). Estos protocolos se utilizan para la transferencia de archivos entre dispositivos. Suelen implementarse en todas las plataformas (incluidos muchos sistemas SCADA, DCS, PLC y RTU), ya que son muy conocidos y utilizan una potencia de procesamiento mínima. En estos protocolos, no se tiene en cuenta la seguridad (en FTP se utiliza una contraseña sin encriptar, mientras que TFTP no requiere inicio de sesión), por lo que las comunicaciones TFTP deben ser bloqueadas, mientras que las FTP deben permitirse, siempre que sea estrictamente necesario, para las comunicaciones salientes y/o implementando autenticación multifactor basada en *token* adicional y túnel encriptado. Cuando sea posible, deben utilizarse protocolos más seguros como *Secure* FTP (SFTP) o *Secure Copy* (SCP).

- Telnet. Este protocolo define una sesión interactiva de comunicaciones basada en texto entre un cliente y un *host*. Se utiliza para el inicio de sesión remoto y servicios de control simples sobre sistemas con recursos limitados. Todo el tráfico de Telnet (incluidas las contraseñas) se transmite en claro, por lo que es un alto riesgo para la seguridad de los ICS. Es recomendable utilizar, en su lugar, SSH (*Secure Shell*) y bloquear, siempre que sea posible, las sesiones Telnet entrantes desde la red corporativa hacia la sesión de control, a no ser que se encuentren protegidas con autenticación multifactor basada en *token* adicional y túnel encriptado. Las sesiones salientes solo deben permitirse a través de *Virtual Private Network* (VPN) a dispositivos específicos.

- Protocolo de Configuración Dinámica de Host (*Dynamic Host Configuration Protocol*, DHCP). El protocolo DHCP se utiliza para distribuir dinámicamente parámetros de configuración de red. No incluye ningún mecanismo de autenticación entre servidores y clientes, pudiéndose proporcionar información incorrecta a los clientes. Además, clientes sin autorización pueden obtener acceso al servidor y provocar el agotamiento de los recursos disponibles. Para evitar estas acciones, se recomienda configurar estáticamente las direcciones IP, y, en caso de ser necesaria la asignación dinámica, habilitar la detección de

intrusos DHCP para defenderse contra servidores fraudulentos, ataques ARP e IP *spoofing*, etc. Estos servidores deben ubicarse en el mismo segmento de red que el equipo que requiere la configuración dinámica de la red.

- Intérprete de Órdenes Seguro (*Secure Shell, SSH*). Permite el acceso remoto a dispositivos. Proporciona autenticación y autorización seguras basadas en criptografía. Este sistema es recomendable como alternativa a Telnet y otras herramientas de acceso remoto inseguras.

- Protocolo Simple de Acceso a Objetos (*Simple Object Access Protocol*, SOAP). SOAP es una sintaxis de formato basada en XML para el intercambio de mensajes. Los flujos de tráfico relacionados con los servicios basados en SOAP deben controlarse en el cortafuegos, concretamente entre los segmentos de red corporativos y del ICS. Es necesario utilizar la inspección profunda de paquetes y/o los cortafuegos de capa de aplicación para restringir el contenido de los mensajes al esperado.

- Protocolo Simple de Transferencia de Correo (*Simple Mail Transfer Protocol*, SMTP). Es el principal protocolo de transferencia de correo electrónico en Internet. No debe permitirse el correo entrante a ningún dispositivo de la red de control ya que puede contener, entre otras, *malware*.

- Protocolo Simple de Administración de Red (*Simple Network Management Protocol*, SNMP). Este protocolo se utiliza para proporcionar servicios de red entre una consola de administración central y dispositivos de red tales como enrutadores, impresoras y PLC. La seguridad de este protocolo, en sus versiones 1 y 2, es muy débil, ya que utilizan contraseñas no cifradas tanto para leer como para configurar los dispositivos, y, en muchos casos, estas contraseñas son públicas y no pueden modificarse. Su versión 3 es algo más segura, pero tiene un uso limitado y aún no está implantada en la mayoría de los dispositivos. Los comandos de SMTP deben prohibirse en la red de control, en especial cuando se opere con las versiones 1 y 2 del protocolo.

- SCADA (*Supervisory Control And Data Acquisition*) y protocolos industriales. Este tipo de protocolos, entre los que también se encuentran MODBUS/TCP, Ethernet/IP, IEC 61850, ICCP (*Inter-Control Center Communications Protocol*) y DNP311, son fundamentales para las comunicaciones con la mayoría de los dispositivos de control. Muchos de estos protocolos, fueron diseñados sin seguridad incorporada, no requiriendo autenticación para poder ejecutar

comandos sobre un dispositivo de control. Por lo tanto, estos protocolos deben permitirse únicamente dentro de la red de control (cuando sea estrictamente necesario), prohibiendo la salida a la red corporativa.

3.2.9. Problemas específicos de los cortafuegos para ICS

Además de lo discutidos en los apartados "3.2.7 Reglas generales para los cortafuegos" y "3.2.8 Reglas de servicios específicos para los cortafuegos", los cortafuegos en entornos de ICS presentan algunos problemas que deben ser considerados durante su despliegue e implantación:

- Historiadores de datos. En las arquitecturas que incluyen DMZ, estos sistemas han de estar contenidos en ella (correctamente configurados, tal y como se ha visto en anteriores apartados), pero en los diseños de dos zonas (red corporativa y red de control), surgen problemas difíciles de resolver. Si se sitúa el historiador en el lado corporativo del cortafuegos, es necesario permitir el tráfico mediante protocolos inseguros (como MODBUS/TCP), ya que se requiere que cada dispositivo de control informe al historiador. Por otra parte, si se posiciona el historiador en el lado de la red de control, deben permitirse protocolos igualmente cuestionables (como HTTP, SQL, etc.) a través del cortafuegos, dejando un servidor dentro en la red de control accesible para casi toda la organización (el propio historiador).

  Para solucionar este problema, lo mejor es evitar los sistemas de dos zonas y utilizar un diseño de tres (red corporativa, DMZ y red de control), colocando el recopilador de datos en la red de control y el historiador en la DMZ. En las situaciones en las que esto no sea posible, pueden instalarse dos servidores (uno en la red de control para recopilar datos de los dispositivos de control y otro en la red corporativa que refleje el primer servidor y respalde las consultas de los clientes). Aunque es asumible, esta arquitectura requiere que se permitan las comunicaciones directas de servidor a servidor (y, por lo tanto, a través del cortafuegos).

- Acceso de soporte remoto. Debe requerirse autenticación mediante mecanismos fuertes (como, por ejemplo, la autenticación basada en *tokens*) a todos los usuarios que accedan a la red de control.

  El personal de soporte remoto conectado a Internet o mediante módems de acceso telefónico debe utilizar un protocolo encriptado (como VPN, servidores

de aplicaciones o acceso HTTP seguro) y autenticarse utilizando mecanismos fuertes (como autenticación multifactor basada en *tokens*). Una vez conectados, lo ideal es que se requiera que se autentiquen una segunda vez en el cortafuegos de la red de control (de nuevo, mediante un mecanismo fuerte) para poder acceder a dicha red. En las organizaciones en las que no se permite ningún tráfico de control desde la red corporativa (sin ninguna excepción), esto podría requerir la implementación de soluciones de túneles para obtener acceso a dicha red (mediante *Secure Sockets Layer* - SSL o *Transport Layer Security* - TLS dentro de una VPN Ipsec).

- Tráfico multidifusión. Si la fuente y los destinos de un paquete de multidifusión están conectados sin enrutadores intermedios o cortafuegos entre ellos, la transmisión de multidifusión (en inglés *multicast*) es fluida. Sin embargo, si esta fuente y los destinos no se encuentran en la misma red, el envío de los mensajes de multidifusión se vuelve complejo. Para resolver el problema del enrutamiento de este tipo de mensajes, además de separar los *hosts* por grupos (asociando un identificador a cada uno de ellos), es necesario indicar al enrutador de multidifusión la existencia de estos grupos mediante el protocolo de administración de grupos de Internet (IGMP). Gracias a esto, los enrutadores de multidifusión conocerán a los miembros de estos grupos y pueden decidir si reenviar o no los mensajes recibido (dependiendo de las reglas que hayan sido configuradas en el cortafuegos).

  Otro problema del cortafuegos relacionado con la multidifusión es el uso de NAT (*Network Address Translation*). Un firewall que realiza traducciones de direcciones de red y que recibe un paquete de multidifusión de un *host* externo no tiene un mapeo inverso para el cual el identificador del grupo interno debe recibir los datos. Si es compatible con IGMP, podría transmitirlo a cada identificador de grupo que conozca, porque una de ellas será correcta, pero esto podría causar serios problemas si un paquete de control incorrecto o malicioso se transmitiera a un nodo crítico. La medida más segura que debe tomar el cortafuegos en estos casos es ignorar el paquete.

  Por lo tanto, la multidifusión generalmente se considera una mala práctica.

3.2.10. Pasarelas unidireccionales

Las pasarelas unidireccionales reforzadas por *hardware* (como, por ejemplo, los Diodos de Datos) se utilizan cada vez más en el límite entre los ICS y otras redes (como, por ejemplo, las redes corporativas). La naturaleza física de estos mecanismos solo permite que los datos pasen de un lado de la conexión de red a otro y no al revés, por lo que es una muy buena práctica a la hora de implementar arquitecturas de seguridad en los ICS, aunque el precio de estos mecanismos suele ser muy elevado.

3.2.11. Puntos de fallo

Como en cualquier sistema informático, en las arquitecturas de los ICS pueden existir puntos de fallo a cualquier nivel o capa. Ya que la seguridad suele ir ligada al entorno del ICS, debe realizarse una evaluación para identificar estas vulnerabilidades, además de una valoración de los riesgos que conllevan estas vulnerabilidades, determinando, de esta forma, la exposición del sistema. Tras descubrirlos, es necesaria la estimación de los posibles métodos para remediarlos, aplicándolos e implementándolos siempre que sea posible.

3.2.12. Redundancia y tolerancia a fallos

La mayoría de los componentes que conforman la red de los ICS se suelen clasificar como elementos críticos para la organización y requieren una alta disponibilidad. Un método para lograrla es utilizando la redundancia, de tal manera que, si un elemento falla, además de no generar tráfico innecesario en el ICS o causar otro problema en otro lugar (como un evento en cascada), existirá otro que responda en su lugar.

El sistema de control debe tener la capacidad de ejecutar procesos de seguridad adecuados ante la pérdida de comunicación con el ICS o la pérdida del propio ICS. Para esto, es necesario, en primer lugar, definir el tiempo transcurrido a partir del cual podría considerarse pérdida de comunicaciones. Posteriormente, basándose en las posibles consecuencias que este hecho podría acarrear, definir el proceso de seguridad adecuado a la organización.

Es necesario realizar copias de seguridad en profundidad, haciéndolas por capas (por ejemplo, copias de seguridad locales, de instalaciones, ante desastres, etc.) y con una secuencia de tiempo, de tal manera que las copias de seguridad locales más recientes estén disponibles para su restauración inmediata. Además, estas copias deben almacenarse en un lugar seguro y realizarse de forma rigurosa, siendo el acceso a ellas rápido en caso de que sea necesaria su restauración.

3.2.13. Prevención de ataques MitM

Un ataque de hombre en el medio (MitM por sus siglas en inglés, *Man in the Middle*) requiere conocer el protocolo que se está manipulando. Esta técnica, en las que un atacante consigue interceptar mensajes entre dos máquinas o *hosts* sin que ninguna de ellas lo sepa y pudiendo leer y manipular los paquetes que van a intercambiarse, es una de las más utilizadas para explotar protocolos inseguros, como los que se encuentran en los sistemas de control. Sin embargo, existen técnicas de mitigación que pueden aplicarse para proteger estos sistemas, por ejemplo, mediante el bloqueo de direcciones MAC, tablas estáticas, cifrado, autenticación y monitorización:

- Bloqueo de direcciones MAC. Los ataques MitM utilizando el protocolo ARP (*Address Resolution Protocol*) requieren que el atacante esté conectado a la red local y/o tenga el control de un equipo en la propia red. El bloqueo de direcciones MAC es un método que sirve para asegurar la conexión física al final de cada puerto en un conmutador de red. Los conmutadores de red de gama alta, generalmente, tienen opciones para asociar direcciones MAC a determinados puertos o conexiones. Este bloqueo, es muy efectivo contra atacantes que buscan conectarse físicamente a la red interna. Sin esta seguridad, cualquier conector de red accesible para el atacante podría utilizarse para entrar en la red corporativa. De esta forma, se asocia un puerto a una dirección MAC específica en un cierto conmutador. Si la dirección MAC no coincide, el enlace de comunicación se desactiva y el atacante no podrá alcanzar su objetivo.

  Aunque este mecanismo no mitiga todos los ataques, agrega una capa de seguridad adicional a la red.

- Tablas estáticas. Para las redes de ICS que permanecen relativamente estáticas, pueden implementarse tablas ARP estáticas, en la que se almacenarían todas las direcciones MAC necesarias. La creación de las tablas ARP estáticas, evita que el adversario pueda modificarlas enviando paquetes de respuesta ARP a la máquina de la víctima.

  A pesar de que esta técnica no es factible en organizaciones de un tamaño elevado y/o dinámicas, la cantidad limitada de *hosts* en una red de ICS podría protegerse de forma efectiva mediante esta técnica.

- Cifrado. Los sistemas den estar diseñados para incluir el tráfico cifrado entre los dispositivos, con el fin de dificultar la ingeniería inversa de los protocolos y

crear paquetes e insertarlos en las redes del sistema de control. Cifrar las comunicaciones entre los dispositivos consigue dificultar (y prácticamente imposibilitar) este tipo de ataques.

- Autenticación. Los protocolos con autenticación fuerte proporcionan resistencia a los ataques MitM, por lo que, cuando sea posible, es muy recomendable su uso en sustitución de otros que no la implementen.
- Monitorización. La monitorización del envenenamiento ARP proporciona una capa adicional de defensa, ya que, mediante esta técnica, puede detectarse el ataque en el momento en el que se está produciendo.

3.2.14. Autenticación y autorización

Realizar una autenticación y una autorización de todos los usuarios que pueden acceder a los sistemas que forman los ICS presenta un gran desafío. Además, la administración de las cuentas de estos usuarios puede ser problemática a medida que se agregan, eliminan y/o cambian sus roles o crece la cantidad de sistemas y usuarios.

Tanto la autenticación como la autorización pueden realizarse de forma distribuida (en la que cada sistema realiza estas acciones por su cuenta, almacenando su propio conjunto de cuentas de usuario, credenciales y roles) o centralizada (cuando se necesita administrar una mayor cantidad de usuarios y cuentas, consultando esta autorización y autenticación a un servidor central, utilizando, por ejemplo, *Lightweight Directory Access Protocol*, Kerberos, *Remote Authentication Dial-In User Service*, etc.).

Cabe destacar que los enfoques centralizados proporcionan una escalabilidad mejorada (no requiriendo el borrado de una cuenta de usuario en cada uno de los sistemas si, por ejemplo, este abandona la organización), pero, a la vez, presenta numerosas preocupaciones que pueden afectar a los entornos de ICS. Por ello, cuando vaya a implantarse, es necesario considerar:

- El servidor de autenticación debe ser robusto, altamente seguro y con una gran disponibilidad, siendo estos los encargados de administrar todas las cuentas del sistema.
- El almacenamiento en caché de las credenciales de usuario solo debe estar disponible y habilitado para usuarios recién autenticados.

- Las redes utilizadas para respaldar el protocolo de autenticación deben ser confiables y seguras, garantizando que los intentos de autenticación no se vean obstaculizados.

En algunos casos, los dispositivos de red del ICS son antiguos y la mayoría no admiten ningún mecanismo o protocolo para integrarse con un sistema de autenticación centralizado, por lo que es necesario utilizar sus propias cuentas específicas y mecanismos de autenticación, con lo que estos hechos conllevan.

3.2.15. Monitorización, registro y auditoría

La arquitectura de seguridad de un ICS también debe incorporar mecanismos para monitorizar, registrar y auditar las actividades que ocurren en cada uno de los sistemas y las redes. Estas acciones, además de ser importantes a la hora de realizar cualquier análisis forense, ayudan a determinar que el sistema está funcionando tal y como se espera y que ninguna violación o incidente de ciberseguridad lo está obstaculizando.

3.2.16. Respuesta a incidentes y recuperación del sistema

Es esencial contar con un plan de respuesta a incidentes, siendo de vital importancia la rapidez con la que puede recuperarse un sistema después de que haya ocurrido un incidente.

Esta respuesta debe abarcar la forma en la que se recuperarán los sistemas del ICS, así como sus redes en caso de desastre. Además, debe incluirse la restauración de las distintas copias de seguridad, el posterior análisis de la causa del incidente, etc.

En el APÉNDICE B se estudian otras recomendaciones de seguridad para los ICS, consideradas de menor relevancia por su encontrarse contenidas en el propio marco normativo que regula la Protección en Infraestructuras Críticas (véase el apartado “2.2 Cumplimiento normativo”).

Además, el APÉNDICE C expone un ejemplo básico de la aplicación, sobre una fábrica de refrescos, de los controles de seguridad a los ICS analizados a lo largo de este capítulo.

CAPÍTULO 4. CONCLUSIONES Y TRABAJO FUTURO

En este capítulo, se detallan las conclusiones y aspectos más destacables encontrados tras la realización de este trabajo. Estas conclusiones engloban tanto el estudio previo, como la investigación exhaustiva y el análisis de la legislación y las normativas españolas en materia de Protección de Infraestructuras Críticas, las recomendaciones y aspectos a tener en cuenta en los Sistemas de Control Industrial y en la arquitectura de red de estos, así como la ejemplificación de estas recomendaciones. En este mismo capítulo, además, se especifican las líneas a seguir en el futuro, que incluyen cuestiones abiertas relativas a la investigación realizada y posibles caminos por los que continuar para completar y ampliar este estudio.

4.1. Conclusiones

En esta investigación, se han descrito y especificado algunos conceptos y definiciones que han de tenerse en cuanta cuando se habla de Protección en Infraestructuras Críticas. Así mismo, se ha expuesto la forma en la que ha evolucionado, en materia legislativa, esta PIC en España, poniendo esto de manifiesto el amplio abanico de tiempo que ha sido necesario hasta que ha podido disponerse de una regulación estable y robusta.

Además, se ha comprobado que, a pesar de que se están haciendo grandes esfuerzos para complementar la Ley PIC, aún quedan algunos aspectos que han quedado sin respaldar y/o se ha de hacer más énfasis en ellos, sobre todo en materia técnica, ya que, si bien es cierto que la Ley obliga a cumplir ciertos requisitos y a documentar algunos detalles de las Infraestructuras Críticas, esta no expone ninguna recomendación ni el obligado cumplimiento o utilización de arquitecturas o topologías concretas para securizarlas, dejando esta decisión en manos de los propietarios o encargados de la organización.

Se sabe que las Infraestructuras Críticas utilizan, para su correcto funcionamiento y la automatización de sus procesos, activos y Sistemas de Control Industrial. A pesar de que existen ciertas recomendaciones, estándares y guías de buenas prácticas para desplegar arquitecturas de seguridad para estos ICS (la forma en la que debe segmentarse y segregarse la red, como desplegar fronteras y cortafuegos, los posibles puntos de fallo, la prevención de ataques MitM, la aplicación de una defensa en profundidad, etc.), estas dependerán, en gran medida, de la propia organización, de sus necesidades, su presupuesto, etc. Estos aspectos, dificultan el obligado cumplimiento de arquitecturas o topologías concretas, pero podría barajarse la

posibilidad de que una entidad gubernamental, como puede ser el CNPIC, se encargara de aconsejar y supervisar los aspectos técnicos en materia de seguridad para el correcto despliegue y la arquitectura de estos ICS.

Por otra parte, el ejemplo típico de topología de red de una industria expuesto en el apartado "C.1 Ejemplo típico de topología de red de una industria", y su posterior modificación para cumplir con una cierta arquitectura de seguridad en "C.2 Ejemplo de arquitectura de seguridad en la red de una industria", ha evidenciado las dificultades a las que se encuentran expuestos los Operadores Críticos, en muchos casos, con pocos conocimientos técnicos y en materia de ciberseguridad.

Es evidente que nos dirigimos a un mundo en el que los ataques informáticos son cada vez más dirigidos a objetivos concretos, no siendo de extrañar que en los próximos años salten a la luz escándalos relacionados con desastres o ataques a Infraestructuras Críticas (como ya ocurrió con Stuxnet, gusano que infectó miles de sistemas SCADA causando un daño sustancial al programa nuclear de Irán) que evidenciarán la necesidad de incrementar, aún más, la protección y supervisión de estas infraestructuras.

A pesar de que no ha sido recogido en ningún apartado de este documento, merece una especial mención la importancia del factor humano a la hora de securizar y proteger este tipo de infraestructuras. Este agente, puede explotarse mediante técnicas de ingeniería social, sobre todo en organizaciones en las que se dispone de una baja capacidad para controlar el acceso a los diferentes Sistemas de Control Industrial. Puede hacerse más robusto este obstáculo humano, mediante el uso de herramientas de concienciación para las personas implicadas en el ciclo de vida de las Infraestructuras Críticas (empleados de la planta, técnicos y personal de mantenimiento, administradores, etc.), capacitándolos mediante, por ejemplo, la simulación de distintos escenarios. También puede fortalecerse el control de acceso a determinados lugares de la propia organización (por ejemplo, la sala de servidores) utilizando medidas compensatorias que pueden mitigar el riesgo, como elementos de seguridad perimetral para ICS.

4.2. Líneas de trabajo futuro

Debido a la constante evolución de las herramientas, sistemas y *software* de prevención y protección ante amenazas, así como a la transformación y actualización de los propios Sistemas de Control Industrial, que incorporan cada vez más funcionalidades e incrementan el uso de estándares populares, y, sin olvidar el crecimiento y la activa actualización de las

distintas normativas y leyes que regulan la Protección en Infraestructuras Críticas, este análisis y las recomendaciones asociadas al mismo no pueden considerarse como definitivas, debiendo evolucionar día a día. Además, es de gran importancia tener en cuenta siempre las nuevas amenazas, que pueden tener un impacto desastroso en las Infraestructuras Críticas.

Para continuar y ampliar este análisis, sería interesante la investigación y el estudio de las normativas que regulan las Infraestructuras Críticas, en materia de seguridad de la información, en otros países, como, por ejemplo, Estados Unidos, en el que se rigen por el "*NIPP 2013: Partnering for Critical Infraestructure Security and Resilience*" [28].

Otro de los posibles temas a tratar, es la ejemplificación de un Análisis de Riesgos en una Infraestructura Crítica, o, incluso, llevar a cabo un ejemplo completo en el que se exponga todos los pasos seguidos para un correcto cumplimiento normativo, incluyendo la realización del Plan de Seguridad del Operador, el Plan de Protección Específico y el Análisis de Riesgos. Además, este ejemplo podría completarse concretando y haciendo más preciso lo expuesto en el APÉNDICE C, incluyendo direcciones IP y MAC reales, protocolos de comunicación utilizados, *software* y *hardware* concreto y sus configuraciones específicas, etc.

APÉNDICE A. CONTENIDOS DE MAGERIT

La metodología de análisis y gestión de riesgos MAGERIT se compone de dos libros y una guía de técnicas, cuyos contenidos se comentan, de forma breve, a continuación [29]:

- **Libro I – Método**. En este documento se describen los conceptos, fases, actividades y obstáculos asociados a la gestión de riesgos. Considera tres elementos clave:
    - Activos. Elementos del sistema de información que soportan la misión de la organización o empresa. Los activos engloban la información, los datos, los servicios, el *software*, el *hardware*, los sistemas de comunicación, los recursos administrativos, los recursos físicos y los recursos humanos.

      Por su parte, los activos pueden tener ciertas dependencias (entre activos superiores y activos inferiores). Estas dependencias son la medida en que un activo superior se vería afectado por un incidente de seguridad en un activo inferior (se dice que un "activo superior" depende de un "activo inferior" cuando las necesidades de seguridad del primero se ven reflejadas en las del segundo).

      Estos activos han de valorarse mediante dos factores, el valor propio (valor nuclear de la información que el sistema maneja y los servicios que se prestan. Activos esenciales) y el valor acumulado (valor que se transfiere a los activos inferiores del sistema a través de las dependencias). La forma de valorar estos activos puede ser cuantitativa (sobre una escala de valores numérica, evitándose que la interpretación de los valores sea motivo de controversia, pero añadiendo un incremento del esfuerzo y la imposibilidad de cuantificar todo) o cualitativa (sobre una escala relativa de valores, obteniéndose una mayor sencillez, pero perdiendo la posibilidad de comparar valores más allá de su orden relativo). Las dimensiones de la valoración se basarán en la disponibilidad, la integridad, la confidencialidad, la autenticidad y la trazabilidad.

- Vulnerabilidades o Amenazas. Posibles situaciones que pueden ocurrirle a los activos ocasionando un perjuicio o problema a la organización o empresa.

  Las amenazas pueden ser de origen natural (como, por ejemplo, accidentes naturales), del entorno (como desastres industriales), defectos de las aplicaciones, causadas por personas de forma accidental o causadas por las personas de forma deliberada.

  No todas las amenazas afectan a todos los activos, así como no todas las amenazas afectan a las dimensiones de seguridad por igual. Estas amenazas han de valorarse bajo dos percepciones distintas, la degradación (cuanto se perjudicaría el valor del activo) y la probabilidad (cuanta probabilidad existe de que se materialice la amenaza).

- Salvaguardas. Medidas de protección desplegadas para minimizar el daño causado por las vulnerabilidades o amenazas. Hay que centrarse y seleccionar aquellas más relevantes para lo que hay que proteger mediante el principio de proporcionalidad, en el que se tiene en cuenta el valor del activo (centrarse en lo más valioso) y la probabilidad de ocurrencia (zonas de riesgo).

  Las salvaguardas ofrecen varios tipos de protección, como son la prevención (autorización previa de los usuarios, gestión de privilegios, pruebas en entornos de preproducción, etc.), la disuasión (guardias de seguridad, códigos de acceso, etc.), la eliminación (borrado de cuentas innecesarias o por defecto, desinstalación de servicios innecesarios, etc.), la minimización (desconexión de redes, equipos o servicios en caso de ataque, etc.), la corrección (líneas de comunicaciones alternativas, SAIs, etc.), la recuperación (copias de seguridad, planes de recuperación, etc.), la monitorización (*logs*, monitorización de sistemas, etc.), la detección (IDSs, detectores de humo, antivirus, etc.), la concienciación (cursos, formación, etc.) y la administración (mantener un inventario de activos, realizar análisis de riesgos, etc.).

  Para que las salvaguardas tengan éxito, es necesario que estas sean idóneas y eficaces. Tras su aplicación, no cambian los activos ni sus

dependencias, se reduce la magnitud de la degradación (baja el riesgo y el impacto).

A partir de estos elementos, se estima el impacto (lo que podría ocurrir) y el riesgo (la probabilidad de que esto ocurra). Por lo tanto, puede decirse que existen unos activos, que están expuestos a amenazas y que estas, a su vez, pueden existir con cierta probabilidad (aumentando el riesgo) y causar degradación sobre dichos activos (provocando un cierto impacto sobre el valor de los activos). Este flujo puede observarse en la Figura A.1.

Para llevar a cabo el método de Análisis de Riesgos con MAGERIT versión 3 (MAGERIT V3), han de detallarse las actividades a realizar y las tareas asociadas a cada una de estas. Las tareas, a su vez, tienen asociados unos objetivos, unos productos de entrada, unos de salida, unas técnicas, prácticas y pautas. Además, de este análisis, surgen unos entregables intermedios (entre los que se encuentran resultados de entrevistas, documentación de otras fuentes como estadísticas, observaciones de expertos y observaciones de los analistas, información existente utilizable como inventario de activos, documentación auxiliar como planos, requisitos, análisis funcionales, manuales de usuario, etc.) e informes y evaluaciones de defectos de productos, procedentes de fabricantes o centros de respuesta a incidentes de seguridad. Como entregables finales, cabe destacar:

- Un modelo de valor. Se trata de un informe en el que se detallan los activos, sus dependencias, las dimensiones de su utilidad y la estimación de su valor en cada dimensión.
- Un mapa de riesgos. En este informe, se detallan las amenazas significativas sobre cada uno de los activos, categorizándolas por frecuencia de ocurrencia y degradación que causaría su materialización.

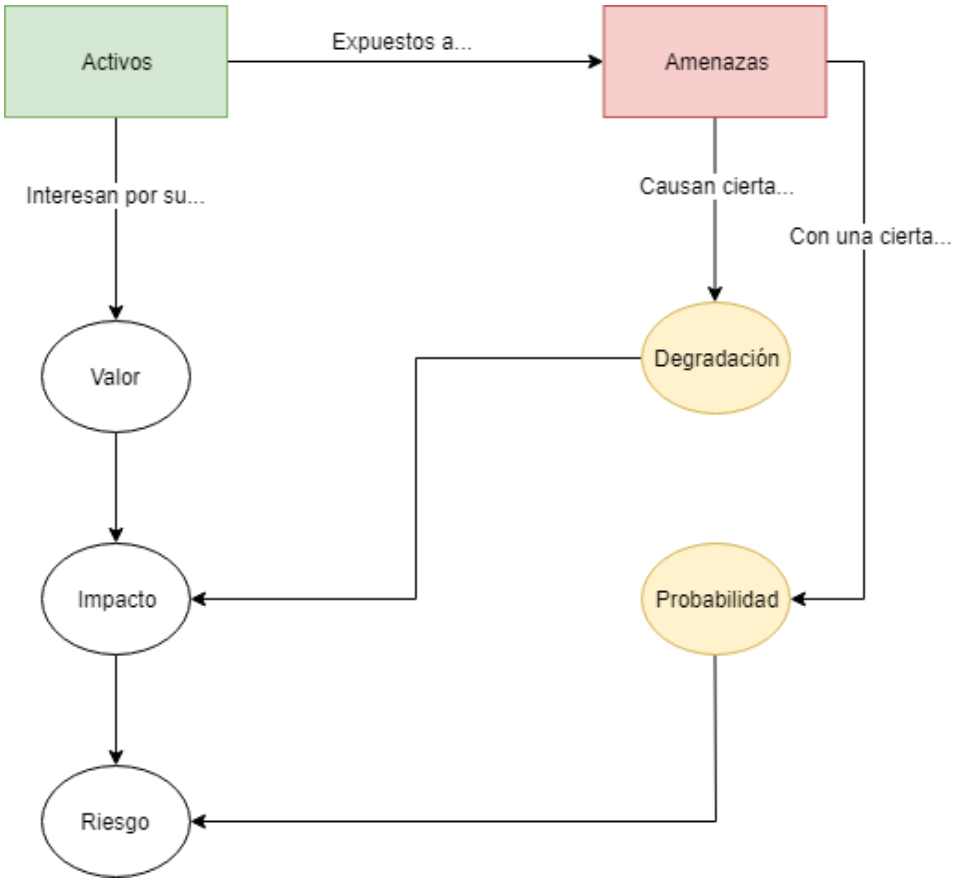


Figura A.1: Flujo seguido en el Libro I - MARGERIT.

- La declaración de aplicabilidad. Un informe que recoge las contramedidas consideradas para la defensa del sistema de información.
- Evaluación de salvaguardas. En él se analizan las salvaguardas, calificando su eficacia para la reducción del riesgo que afrontan.
- Informe de insuficiencias o vulnerabilidades. Se detallan las salvaguardas necesarias pero inexistentes o que no cumplen plenamente.
- Estado de riesgo. Se determinan, para cada uno de los activos, el impacto y el riesgo (potenciales y residuales) frente a las amenazas.

Por otro lado, para el proceso de gestión de riesgos, una vez obtenido el análisis, es necesaria la toma de decisiones basada en la gravedad del impacto y el riesgo obtenido y los requerimientos legales, sectoriales y contractuales. El proceso de gestión de riesgos consiste en corroborar si las salvaguardas implantadas son suficiente y se han implantado de manera eficiente.

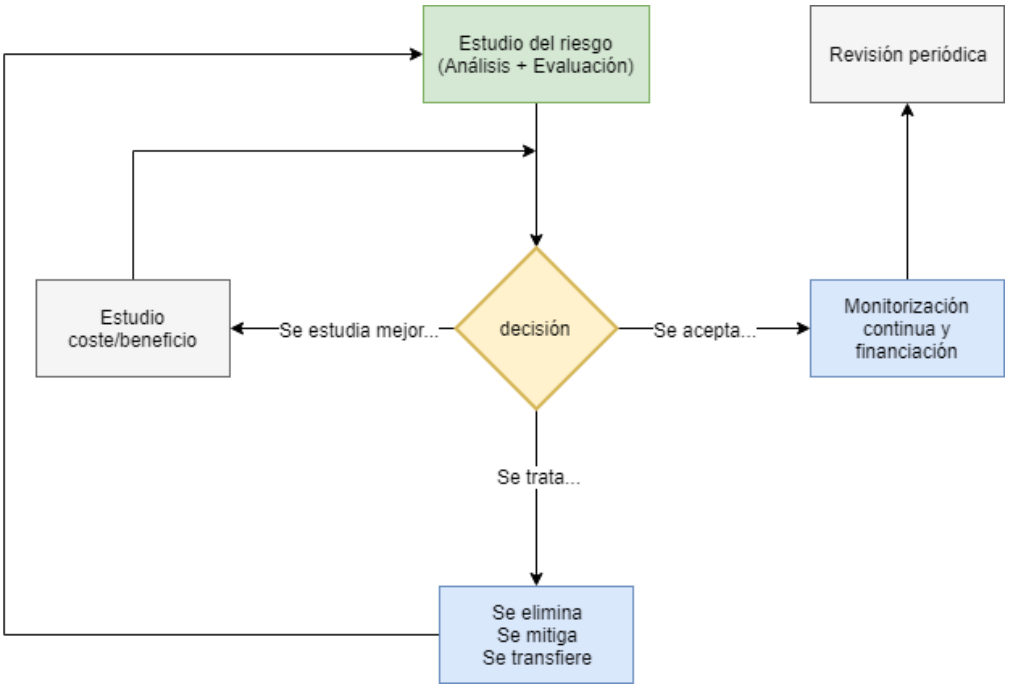


Figura A.2: Flujo de la gestión de riesgos en MARGERIT (Libro I).

Este proceso, comienza con la toma de decisiones basada en la gravedad del impacto y el riesgo obtenido, estos riesgos, pueden aceptarse (en cuyo caso, deberán monitorizarse constantemente y guardarse financiación por si hubiera que responder a sus consecuencias), estudiarse de una forma más exhaustiva (haciendo un estudio cuantitativo de coste/beneficio y tomando una decisión a partir de este) o tratarse (eliminándola, mitigándola o transfiriéndola cualitativamente, externalizando componentes del sistema y/o cuantitativamente, por medio de la contratación de seguros). El flujo seguido puede observar en la Figura A.2.

Cuando se realiza un Análisis de Riesgos partiendo de cero, se consumen gran cantidad de recursos y conviene llevar a cabo una planificación de las actividades necesarias, englobando este análisis dentro de un proyecto, desglosable en varias fases:

- Fase 0. Roles y funciones (equipo de proyecto, comité de seguimiento, grupos de interlocutores, etc.).
- Fase I. Actividades preliminares. Entre las que destacan el estudio de oportunidad (fundamentos para la realización del Análisis de Riesgo y obtener la aprobación de la dirección de la organización para la

realización del proyecto), la determinación del alcance del proyecto (determinar los objetivos del proyecto), la planificación del proyecto (definir los interlocutores, planificar entrevistas de recogida de información, determinar los recursos necesarios, realizar el calendario de actividades y tareas, etc.) y el lanzamiento del proyecto (cuestionarios, catálogo de activos, dimensiones de valoración de los activos, criterios de valoración de los activos, amenazas, informar a los actores afectados, etc.

- Fase II. Análisis de Riesgos.
- Fase III. Comunicación de resultados.

Por último, se lleva a cabo un plan de seguridad, el cual ha de dividirse en tres bloques diferenciados:

- Identificación de proyectos de seguridad. El objetivo de este bloque es la elaboración de un conjunto de programas de seguridad. Deben especificarse los productos de entrada (resultados de las actividades de análisis y tratamiento de riesgos, conocimientos de técnicas y productos de seguridad y catálogos de productos y servicios de seguridad), los productos de salida (la relación de programas de seguridad), las técnicas, prácticas y pautas (planificación de proyectos) y los participantes (equipo de proyecto, especialistas en seguridad y especialistas en áreas específicas de seguridad).
- Plan de ejecución. Su objetivo es ordenar temporalmente los programas de seguridad. En este caso, los productos de entrada serán los resultados de las actividades de análisis y tratamiento de riesgos y los de la anterior tarea (identificación de proyectos de seguridad), los productos de salida se corresponderán con un cronograma de ejecución del plan y un plan de seguridad, las técnicas, prácticas y pautas serán el Análisis de Riesgos y la planificación de proyectos y como participantes colaborarán el departamento de desarrollo y el de compras.
- Ejecución. Se alcanzarán los objetivos previstos en el plan de seguridad para cada proyecto planificado. De nuevo, se cuenta con unos productos

de entrada (los resultados de las dos actividades anteriores y el proyecto de seguridad), unos productos de salida (las salvaguardas implantadas, las normas de uso y procedimientos de operación, el sistema de indicadores de eficacia y eficiencia del desempeño de los objetivos de seguridad perseguidos, un modelo de valor actualizado, el mapa de riesgos actualizado y el estado de riesgo actualizado), unas técnicas, prácticas y pautas (Análisis de Riesgos y planificación de proyectos) y unos participantes (el equipo de proyecto y el personal especializado en la salvaguarda en cuestión).

- **Libro II – Catálogo de elementos**. Se propone un catálogo de activos, dimensiones de valoración de estos activos, sus criterios de valoración, vulnerabilidades o amenazas y salvaguardas relacionados con ellos. Los objetivos de este catálogo son conseguir la estandarización en un proceso de Análisis y Gestión de Riesgos, además de la homogeneización de los resultados y la interpretación de los análisis. Las secciones de este catálogo son las que siguen.
    - Tipos de activos y dependencias. A su vez, formada por:
        - Activos esenciales, que pueden dividirse en información (servicios que la manejan, *software* que la trata, *hardware* que la hospeda, usuarios que acceden) y en servicios (datos que lo sustentan, servicios internos que lo habilitan, *software* que lo sustenta, *hardware* que lo habilita, personal del que depende)
        - Datos/información (*hardware* que lo hospeda, líneas de comunicación por las que se transfieren, soportes de información, personas relacionadas).
        - Claves criptográficas (*hardware* que las hospeda, soportes de información, personas relacionadas).
        - Servicios (*software*, *hardware*, equipos de comunicaciones, soportes de información, personas a cargo del servicio)
        - *Software* (personas relacionadas)
        - *Hardware* (personas relacionadas e instalaciones que lo acogen).

- Redes de comunicaciones (personas relacionadas y personas que lo acogen).
- Equipamiento auxiliar (personas relacionadas, instalaciones que lo acogen).
- Instalaciones y personal de las mismas.

- Valoración y dimensiones. La valoración de los activos debe tener determinadas dimensiones, por ello, es necesario analizar la disponibilidad, la integridad, la confidencialidad, la autenticidad y la trazabilidad.

  Así mismo, debe utilizarse una misma escala de valores para todas las dimensiones (una escala logarítmica centrada en diferencias relativas de valor y no en diferencias absolutas) y utilizar un criterio homogéneo que permita comparar análisis realizados por separado.

- Amenazas. Las amenazas deben desglosarse según su tipo. MAGERIT las clasifica en:
  - Desastres naturales. Fuego, daños por agua, etc.
  - Origen industrial. Fuego, daños por agua, contaminación mecánica, contaminación electromagnética, avería de origen físico, corte del suministro eléctrico, condiciones inadecuadas de temperatura o humedad, fallo de servicios de comunicaciones, interrupción de otros servicios y suministros esenciales, degradación de los soportes de almacenamiento de la información, emanaciones electromagnéticas.
  - Errores y fallos no intencionados. Errores de los usuarios, errores del administrador, errores de monitorización, errores de configuración, deficiencias den la organización, difusión de *software* dañino, errores de encaminamiento, errores de secuencia, escapes de información, alteración accidental de la información, destrucción de información, fugas de información, vulnerabilidades de los programas, errores de mantenimiento/actualización de programas, errores de

mantenimiento/actualización de equipos, caída del sistema por agotamiento de recursos, pérdida de equipos, indisponibilidad del personal.

- Ataques intencionados. Manipulación de los registros de actividad, manipulación de la configuración, suplantación de la identidad del usuario, abuso de privilegios de acceso, uso no previsto, difusión de *software* dañino, encaminamiento de mensajes, alteración de secuencia, acceso no autorizado, análisis de tráfico, repudio, interceptación de información, modificación deliberada de la información, destrucción de información, divulgación de información, manipulación de programas, manipulación de los equipos, denegación de servicio, robo, ataque destructivo, ocupación enemiga, indisponibilidad del personal, extorsión e ingeniería social.

- Salvaguardas. Las salvaguardas, al igual que ocurre con las amenazas, deben clasificarse según el tipo:

  - Protecciones generales. A su vez, estas protecciones, se desglosan en identificación y autenticación, control de acceso lógico, segregación de tareas, gestión de incidencias, herramientas de seguridad, herramientas contra código dañino, herramienta de chequeo de configuración, herramienta de análisis de vulnerabilidades, herramienta de monitorización de tráfico, herramienta de monitorización de contenidos, herramienta para análisis de *logs*, *honey net*/*honey pot*, verificación de las funciones de seguridad, gestión de vulnerabilidades y registro y auditoría.

  - Protección de los datos. Entre las que se encuentran las copias de seguridad, el aseguramiento de la integridad, el cifrado de la información, el uso de firmas electrónicas y el uso de servicios de fechado electrónico.

  - Protección de las claves criptográficas. Gestión de claves de cifra de información, gestión de claves de firma de información,

gestión de claves para contenedores criptográficos, gestión de claves de comunicaciones y gestión de certificados.

- Protección de los servicios. Clasificadas en aseguramiento de la disponibilidad, aceptación y puesta en operación, se aplican perfiles de seguridad, explotación, gestión de cambios (mejoras y sustituciones), terminación, protección de servicios y aplicaciones web, protección del correo electrónico, protección del directorio, protección del servidor de nombres de dominio (DNS), teletrabajo y voz sobre IP.

- Protección de las aplicaciones (*software*). Copias de seguridad (*backup*), puesta en producción, se aplican perfiles de seguridad, explotación/producción, cambios (actualizaciones y mantenimiento) y terminación.

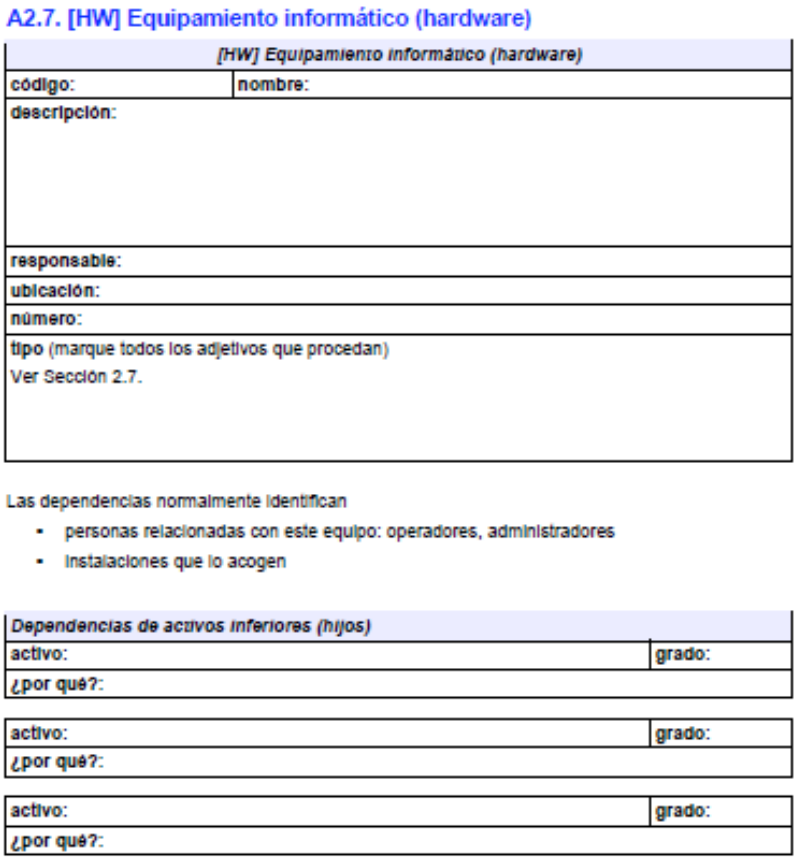
- Protección de los equipos (*hardware*). Puesta en producción, aplicación de perfiles de seguridad, aseguramiento de la disponibilidad, operación, cambios (actualizaciones y mantenimiento), terminación, informática móvil, reproducción de documentos y protección de la centralita telefónica (PABX).

- Protección de las comunicaciones. Desglosadas en protección de las comunicaciones, entrada en servicio, se aplican perfiles de seguridad, aseguramiento de la disponibilidad, autenticación del canal, protección de la integridad de los datos intercambiados, protección criptográfica de la confidencialidad de los datos intercambiados, operación, cambios (actualizaciones y mantenimiento), terminación, Internet, seguridad *Wireless* (Wifi), telefonía móvil, y segregación de las redes en dominios.

- Protección de los puntos de interconexión. Como, por ejemplo, las conexiones entre zonas de confianza, los sistemas de protección perimetral y la protección de los equipos de frontera.

- Protección de los soportes de información. Se desglosan en el aseguramiento de la disponibilidad, protección criptográfica del contenido, limpieza de contenidos y destrucción de soportes.
- Protección de los elementos auxiliares. Aseguramiento de la disponibilidad, instalación, suministro eléctrico, climatización y protección del cableado.
- Protección de las instalaciones (seguridad física). Desglosable en el diseño, defensa en profundidad, control de los accesos físicos, aseguramiento de la disponibilidad y terminación.
- Protección del personal. A su vez, puede dividirse en formación y concienciación y en un aseguramiento de la disponibilidad.
- Medidas organizativas. Organización, gestión de riesgos, planificación de la seguridad e inspecciones de seguridad.
- Continuidad de operaciones. Continuidad del negocio y análisis de impacto (BIA).
- Externalización. Relaciones externas, acuerdos para intercambio de información y *software*, acceso externo y servicios proporcionados por otras organizaciones.
- Adquisición y desarrollo. Pueden dividirse en servicios, aplicaciones, equipos, comunicaciones, soportes de información y productos certificados o acreditados.

Puede observarse un ejemplo de ficha estándar para la captura de datos en un proyecto de Análisis y Gestión de Requisitos en la Figura A.3.



A2.7. [HW] Equipamiento informático (hardware)

[HW] Equipamiento informático (hardware)	
código:	**nombre:**
descripción:	
responsable:	
ubicación:	
número:	
tipo (marque todos los adjetivos que procedan) Ver Sección 2.7.	

Las dependencias normalmente identifican

- personas relacionadas con este equipo: operadores, administradores
- instalaciones que lo acogen

Dependencias de activos inferiores (hijos)	
activo:	**grado:**
¿por qué?:	

activo:	**grado:**
¿por qué?:	

activo:	**grado:**
¿por qué?:	

Figura A.3: Ejemplo de ficha estándar para la captura de datos en un proyecto de Análisis y Gestión de Requisitos.

- **Guía de Técnicas** – En este documento se recopilan distintas técnicas que pueden ser útiles para la aplicación de este método. El objetivo de esta guía es facilitar un conjunto de heurísticos y procedimientos que ayuden a alcanzar los objetivos del proceso de Análisis y Gestión de Requisitos. Esta guía es específica para el Análisis de Riesgos (análisis mediante tablas, algorítmico, arboles de ataque) y sus técnicas generales se basan en técnicas gráficas, sesiones de trabajo como entrevistas, reuniones y presentaciones, valoración Delphi, etc.

APÉNDICE B. AMPLIACIÓN DE LA CIBERSEGURIDAD INDUSTRIAL

A continuación, se exponen algunas recomendaciones para mejorar la seguridad de los ICS, que complementan las presentadas en el Capítulo 3 de este mismo trabajo.

B.1. Gestión y evaluación de riesgos en los ICS

Las distintas organizaciones y empresas se enfrentan, prácticamente a diario, a numerosos riesgos para poder cumplir con sus objetivos comerciales. Estos riesgos, además de financieros, pueden ser causados, por ejemplo, por un fallo en un equipo o por un fallo de seguridad propiciado por el personal de la propia empresa. De esta forma, y para evitar parte de estos problemas, las organizaciones deben desarrollar procesos de evaluación de riesgos acordes a sus propios negocios, decidiendo como enfrentarse a ellos en función de sus prioridades y limitaciones, llevándose a cabo como un proceso interactivo y continuo. Las organizaciones que utilizan ICS, históricamente, han manejado el riesgo mediante las buenas prácticas en seguridad e ingeniería. Así mismo, las evaluaciones de seguridad se encuentran establecidas correctamente en la mayoría de los sectores, incorporándose, a menudo, en los distintos requisitos reglamentarios y las leyes.

En toda organización debe aplicarse un proceso de gestión de riesgos, con el objetivo de mejorar continuamente las actividades relacionadas con el riesgo dentro de la organización, utilizando un enfoque de tres niveles para abordarlo en el nivel organizativo, en el de ocupación y en el de sistema de información (engloba tanto las tecnologías de la información como los sistemas de control industrial).

En este apartado, se estudian, principalmente, las consideraciones de los ICS, sin embargo, merece la pena mencionar que cada una de las actividades de gestión de riesgos puede afectar y causar un determinado impacto en otros niveles de la propia gestión.

B.1.1. Introducción al proceso de gestión de riesgos

El proceso de gestión de riesgos es un proceso continuo y está compuesto por el enmarcado, la evaluación, la respuesta y la monitorización. Estas actividades son interdependientes y en la mayoría de los casos ocurren de forma simultánea dentro de la organización.

El enmarcado o encuadre, consiste en el desarrollo de un marco que englobará las decisiones dentro de la gestión de riesgos. Por otro lado, la evaluación del riesgo conlleva a que las organizaciones identifiquen sus amenazas y vulnerabilidades, el daño que estas podrían causar a la organización y la probabilidad de que ocurran. La respuesta a la identificación del riesgo requiere que las organizaciones identifiquen posibles acciones para abordar y minimizar dicho riesgo, se evalúen estas acciones teniendo en cuenta la tolerancia al riesgo que la organización podría permitirse y elijan la mejor alternativa. Por último, la monitorización del riesgo ha de ser continua, incluyendo la implementación de las estrategias de gestión de riesgos elegidas, los cambios en el entorno que puedan afectar al cálculo del riesgo y la efectividad y eficacia de las acciones de reducción de riesgos.

B.1.2. Consideraciones en las evaluaciones de riesgos de los ICS

En las evaluaciones de riesgos de los ICS, es necesario considerar determinados elementos y estados que pueden darse debido a la propia naturaleza de estos sistemas, considerando el fuerte impacto que puede acarrear un incidente de ciberseguridad en ellos, incluyendo y teniendo repercusión tanto en elementos físicos como digitales. Entre estas consideraciones son destacables los impactos en la seguridad y el uso de evaluaciones de seguridad, el impacto físico de un incidente de ciberseguridad en un ICS y las evaluaciones de riesgos o impacto de los componentes de control no digitales dentro de un ICS.

Las **evaluaciones de riesgos de la seguridad de la información** deben considerarse un complemento a las evaluaciones de seguridad y protección. Dichas evaluaciones de seguridad se refieren, principalmente, al mundo físico, mientras que las evaluaciones de riesgos de seguridad de la información recaen sobre el mundo digital. Sin embargo, en los entornos ICS ambos mundos (el físico y el digital) se encuentran muy ligados, pudiendo producirse una superposición entre ellos. Por lo tanto, es importante tener en cuenta este aspecto, debiendo ser capaz el personal responsable de la evaluación de riesgos de seguridad de la información de identificar y comunicar aquellos riesgos que podrían tener implicaciones de seguridad (así como el personal encargado de las evaluaciones de seguridad debería tener en cuenta los posibles impactos físicos y su probabilidad).

La **evaluación del impacto físico de un incidente de ICS** debe incluir cómo un incidente podría causar cambios en los sensores y actuadores provocando un impacto en el entorno físico, qué controles existen en el ICS para evitar este impacto y cómo podría surgir un incidente físico basado en estas condiciones. Este tipo de evaluaciones deben centrarse en el daño potencial a la seguridad de las personas (en función de si es posible que se produzcan lesiones, enfermedades o la muerte por un mal funcionamiento del ICS), al medio ambiente

(cómo un incidente podría afectar a los recursos naturales y la vida silvestre a corto, medio o largo plazo) y a otras Infraestructuras Críticas (un incidente podría dañar otras Infraestructuras Críticas, por ejemplo, dejándolas sin electricidad).

Deben tenerse en cuenta las **evaluaciones de aspectos no digitales de los ICS en las evaluaciones de impacto**, ya que, a menudo, hay mecanismos y elementos no digitales que presentan fallos y conllevan a que los ICS no funcionen correctamente. Por lo tanto, debe considerarse para estas evaluaciones cualquier mecanismo de control no digital y las medidas que pueden aplicarse para mitigar el posible impacto negativo que puede acarrear al correcto funcionamiento del ICS.

El impacto de los controles de seguridad implementados en el sistema de seguridad también debe evaluarse, determinando de esta forma que estos controles no generen ningún impacto negativo en el sistema. Además, deben incorporarse en estas evaluaciones la manera en la que el impacto sobre un ICS podría propagarse a otro ICS o sistema físico conectado.

B.2. Programas de seguridad de los ICS

Los planes de seguridad de ICS deben guardar cierta coherencia e integrarse con la experiencia, los programas y las prácticas de seguridad de las tecnologías de la información ya conocidas, pero teniendo en cuenta los requisitos y características específicos de las tecnologías y entornos de los ICS. En este apartado se aborda cómo las organizaciones deben desarrollar e implementar los programas de seguridad para los ICS.

Este tipo de programas, deben incluir el desarrollo de un modelo de negocio para la seguridad de los ICS, la creación y entreno de un equipo multifuncional, la definición del alcance, políticas y procedimientos de los ICS, la implementación de un marco de gestión de riesgos de seguridad de estos y proporcionar capacitación aumentando la concienciación del personal que opera con el ICS en materia de seguridad.

B.2.1. Modelo de negocio para la seguridad

La implementación de un programa de seguridad para los ICS parte del desarrollo de un modelo de negocio que cubra las necesidades específicas de la organización. Este modelo, debe reflejar las inquietudes comerciales de la empresa, basándose en la experiencia de otras que ya hayan tenido que lidiar con riesgos similares. En este proceso, debe incluirse información detallada sobre los beneficios que le aportaría a la organización la creación de un programa de seguridad integrado, los posibles escenarios que podrían darse si no se implementa dicho

programa de seguridad para el ICS (con sus costes asociados, daños, etc.) y los costes y recursos necesarios para el desarrollo, implementación y mantenimiento del programa de seguridad.

B.2.2. Creación y entreno de un equipo multifuncional

Para poder compartir conocimientos y experiencias a la hora de evaluar y mitigar los riesgos de los ICS, es esencial la creación y entreno de un equipo multifuncional. Idealmente, este equipo debería estar formado por algún operador de sistemas de control, uno o varios miembros del personal de tecnologías de la información de la organización, algún ingeniero de control, expertos en seguridad informática y uno o varios miembros del personal de gestión de riesgos de la empresa. A pesar de que los ingenieros de control juegan un papel muy importante en la protección de los ICS, estos no podrían desempeñar sus funciones correctamente sin la colaboración y el apoyo del departamento de tecnologías de la información, el cual aporta otro punto de vista al proyecto. Por lo tanto, la integración y colaboración entre todos los roles es esencial para el desarrollo de un buen diseño y para poder llevar a cabo las operaciones de seguridad pertinentes.

Este equipo multifuncional, cuyo compromiso es responder ante el gerente de seguridad de la información del ICS, debe poseer conocimientos y habilidades sobre seguridad informática, incluidos aspectos relacionados con la arquitectura y el diseño de la red, los procesos y prácticas de seguridad, el diseño y las operaciones en infraestructuras seguras, etc.

B.2.3. Definición del alcance

El gerente de seguridad de la información del ICS debe ser el encargado de definir una política que abarque tanto la orientación de la organización en materia de seguridad de la información, como su alcance, los roles y las responsabilidades asociadas a cada uno de ellos.

Es necesario que el objetivo del programa de seguridad quede documentado, manifestándose en él tanto las organizaciones afectadas, como los sistemas informáticos y las redes involucradas, el presupuesto y los recursos necesarios, así como la división de responsabilidades.

B.2.4. Definición de políticas y procedimientos

Cuando sea posible, las políticas y procedimientos de seguridad de los ICS deben integrarse con los ya existentes en materia operativa. Estas políticas y procedimientos ayudan

a garantizar que la protección de seguridad sea constante y actual, protegiendo de esta forma la organización contra las amenazas en evolución.

Es preciso examinar las políticas con las que cuenta la organización, comprobando que se adapten a la misma y aborden de forma adecuada los riesgos emergentes de los ICS, modificándose, adaptándose y/o creándose nuevas políticas cuando sea necesario. La falta de política de seguridad puede considerarse una vulnerabilidad de gran envergadura.

Teniendo en cuenta el nivel de riesgo que la organización está dispuesta a asumir, se deben determinar las mitigaciones a aplicar, buscando una reducción del riesgo residual a niveles aceptables. Las políticas y procedimientos han de basarse en una evaluación de riesgos que establecerá las prioridades y objetivos de seguridad para la organización. Los procedimientos de seguridad deben documentarse, probarse y actualizarse periódicamente, respondiendo a cambios en políticas, tecnologías y amenazas.

B.2.5. Implementación de un marco de gestión de riesgos de seguridad

El proceso de implementación del marco de gestión de riesgos incluye un conjunto de tareas relacionadas con los riesgos emergentes de los ICS, que deben llevarse a cabo por parte de determinados roles dentro de la organización. Las tareas englobadas en este marco, en la mayoría de los casos, se ejecutan al mismo tiempo o como parte de los procesos de ciclo de vida de desarrollo del sistema, por lo que han de tenerse en cuenta las dependencias correspondientes.

En este marco de gestión, han de considerarse y especificarse las categorías de los ICS, los activos que componen las redes y los controles de seguridad aplicables a estos ICS. Además, debe realizarse una evaluación de riesgos e implementar los controles de seguridad que corresponda.

La **categorización e inventariado de los activos** (aplicaciones, sistemas informáticos, etc.) de los ICS, así como las redes dentro del mismo y que interactúan con él, debe ser un proceso constante, debiendo revisarse y actualizarse este listado anualmente. Entre los elementos a inventariar y categorizar deben incluirse los PLC, DCS, SCADA y los sistemas basados en instrumentos que usen un dispositivo de monitorización como HMI, al igual que aquellos activos que utilicen un protocolo enrutable y/o que sean accesibles por vía telefónica. Para este menester, existen sistemas de gestión automatizada para el inventariado, como son los *Computerized Maintenance Management System*, los *Computer Aided Facility Management System*, los *Building Information Model*, etc. que permiten a las organizaciones mantener un inventario preciso sin necesidad de realizar los recuentos y la documentación de forma manual.

La selección de los **controles de seguridad** ha de hacerse en base a la categorización e inventariado de los activos. Estos controles deben aplicarse según los requisitos de seguridad de los ICS y las características organizacionales de la entidad: tamaño, complejidad, tipo de negocio, expectativas, etc. Una exitosa ejecución de estos controles depende de su implementación en toda la organización y de una correcta elección de estos.

Debido a los diferentes recursos que posee cada una de las organizaciones, es necesario **realizar una evaluación de los riesgos e impactos** que pueden acarrear las distintas operaciones que lleva a cabo la entidad (misión, funciones, reputación, etc.), sus activos, los empleados de la propia organización, etc. Ha de tenerse en cuenta, a la hora de realizar esta evaluación, que un evento adverso puede tener infinidad de consecuencias e impactos, en diferentes niveles y marcos de tiempo. Puede realizarse una evaluación de riesgos detallada y más exhaustiva para los sistemas y escenarios que causarían un mayor impacto, debiéndose realizar varias veces durante el ciclo de vida de un sistema. Esta evaluación ayudará a identificar las debilidades que puedan contribuir a los riesgos de seguridad de la información, así como a descubrir los enfoques que pueden amenizar y mitigar estos riesgos.

Para **implementar los controles de seguridad**, las organizaciones deben analizar tanto la evaluación de riesgos como los impactos que pueden manifestarse (en las operaciones que lleva a cabo la organización, los activos, el personal, etc.) y priorizar la implantación de los controles de seguridad, eligiendo, en primera instancia, aquellos que pueden aplicarse de forma rápida y con un bajo coste, aportando, a su vez, un alto valor y reduciendo significativamente el riesgo. Este tipo de controles y su resultado puede variar entre los distintos tipos de sistemas, llegando a perjudicar en algunos casos lo que para otros es una solución eficaz.

APÉNDICE C. APLICACIÓN DE CONTROLES DE SEGURIDAD A LOS ICS

Como se ha analizado en el de este documento, los ICS poseen características únicas, entre las que deben incluirse la necesidad de aplicar un especial énfasis en la seguridad, la exigencia de respuesta en tiempo real, la alta disponibilidad, la previsibilidad de las ocurrencias futuras y los requisitos de confiabilidad.

Para poder contextualizar la arquitectura de seguridad de los ICS, se presenta, en los siguientes apartados, un ejemplo de topología de red típica de una industria y la forma, aspectos y buenas prácticas que deben tenerse en cuenta para su securización aplicando una correcta arquitectura de red. A pesar de que este ejemplo no profundiza en materia de protocolos, reglas de cortafuegos, direcciones IP/MAC concretas, puertos utilizados, etc., puede servir para familiarizarse y comprender de una forma más realista las recomendaciones en materia de arquitectura expuestas en el apartado “3.2 Arquitectura de seguridad de los ICS” de este trabajo.

C.1. Ejemplo típico de topología de red de una industria

En esta sección se presenta un ejemplo representativo de topología de red de una industria, en este caso, de fabricación y envasado de refrescos. Aunque parece un modelo poco realista y desmesurado, hoy en día, la mayoría de las industrias aún no se han preocupado por aspectos tan importantes como la ciberseguridad, desconociendo por completo los problemas que una mala protección de sus sistemas, redes y maquinaria podría acarrear y/o el incremento de la producción, entre otros, que una correcta arquitectura de seguridad de los ICS podría proporcionarles.

En dicha fábrica, se presentan tres grandes áreas de proceso. La primera, el área de fabricación, en la que se llevan a cabo tareas como el tratamiento del agua, la mezcla, etc. Una segunda área, la de envasado, que engloba procesos como el lavado y enjuague de botellas, su inspección, el llenado y cierre, la pasteurización, el etiquetado, etc. Y, por último, una tercera área, la de almacenamiento, en la que se paletiza el producto, se fleja el palé, se traslada al almacén, etc.

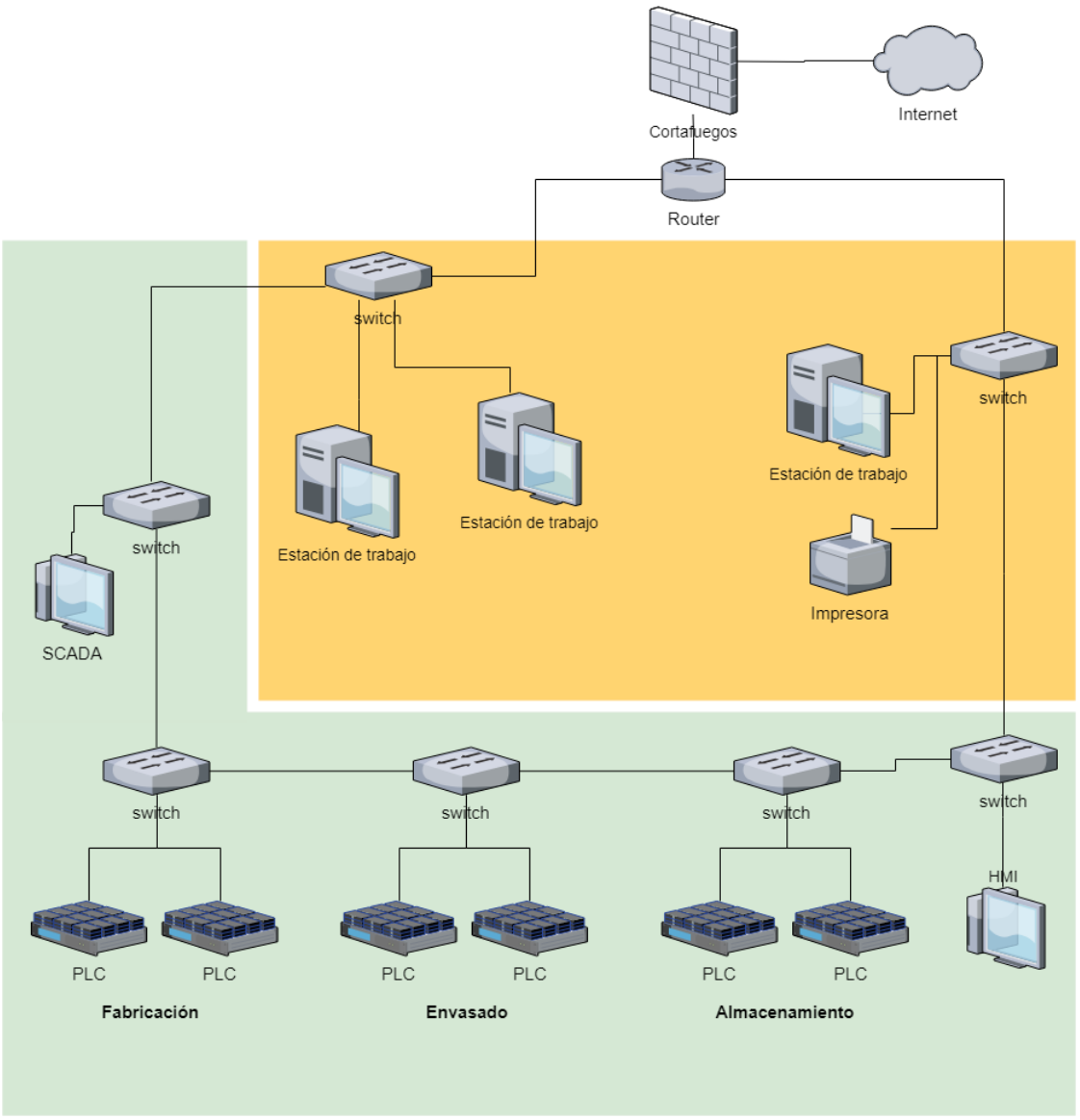


Figura C.1: Ejemplo típico de topología de red de una fábrica de refrescos.

En esta fábrica, existe una única red que da servicio a todos los procesos y sistemas de fabricación (ver Figura C.1), en forma de anillo, y utilizando un enrutador para poder dirigir el tráfico de red a los distintos sistemas que conforman la misma. Esta red, a su vez, y utilizando *switches*, se encuentra segmentada de forma lógica (mediante VLAN). Por otro lado, en las distintas áreas de proceso, existen diferentes PLCs asociados a cada una de las fases y sistemas HMI que permiten la supervisión y el control de dichos procesos. Esta arquitectura también incluye un SCADA para supervisar y controlar el proceso de fabricación.

El cortafuegos, por su parte, mantiene activadas las firmas para la detección de intrusos, consiguiendo de esta forma reducir el riesgo de infección por *malware* y/o la denegación de servicios, entre otras. A pesar de ser esto una buena práctica, en caso de producirse una infección de la red (por ejemplo, mediante *phishing* como vector de ataque o con un USB), su

propagación sería inmediata, afectando gravemente a toda la red (ya que no existe segmentación física), por lo que se considera una medida insuficiente.

En el siguiente apartado (C.2 Ejemplo de arquitectura de seguridad en la red de una industria) se presenta una posible solución para esta arquitectura, siguiendo las buenas prácticas descritas en el apartado "3.2 Arquitectura de seguridad de los ICS" de este mismo documento y manteniendo siempre un cierto equilibrio entre protección y coste de la implementación de esta nueva arquitectura.

C.2. Ejemplo de arquitectura de seguridad en la red de una industria

En la sección anterior, se ha expuesto un ejemplo típico de topología de red de una industria dedicada a la fabricación y envasado de refrescos. A continuación, se presenta una arquitectura de seguridad de la red (y en especial de los ICS) de esa misma organización, prestando una especial atención en la seguridad, la exigencia de respuesta en tiempo real de este tipo de organizaciones, la alta disponibilidad, la previsibilidad de las ocurrencias futuras y los requisitos de confiabilidad. Aprovechando la reestructuración de la arquitectura, se insertan también nuevas tecnologías que sirven para evolucionar la fábrica e incrementar su producción. Un diagrama representativo de este ejemplo puede encontrarse en la Figura C.2.

En un entorno real, en primera instancia, deberían llevarse a cabo diferentes actividades de recogida de información de la organización y sus sistemas, un análisis de riesgo operativo, etc. que, por extensión, para este ejemplo han sido omitidos. A continuación, se presentan los aspectos más relevantes de los puntos estudiados en este capítulo mediante la aplicación a este caso de uso.

En cuanto a las nuevas tecnologías a incorporar, cabe destacar el despliegue de una red wifi para poder comunicar de forma inalámbrica los HMI. Además, para que los fabricantes y técnicos de las máquinas puedan acceder a ellas para su mantenimiento y reparación, se despliega un acceso remoto (para el cual se ha incluido un servidor en el que se encuentran instaladas máquinas virtuales de todos los entornos de desarrollo de los PLCs). También se ha creado un historiador de datos en la nube, para que usuarios y altos directivos puedan tener acceso remoto y seguro a los datos del proceso, que contiene una réplica del historiador de datos local.

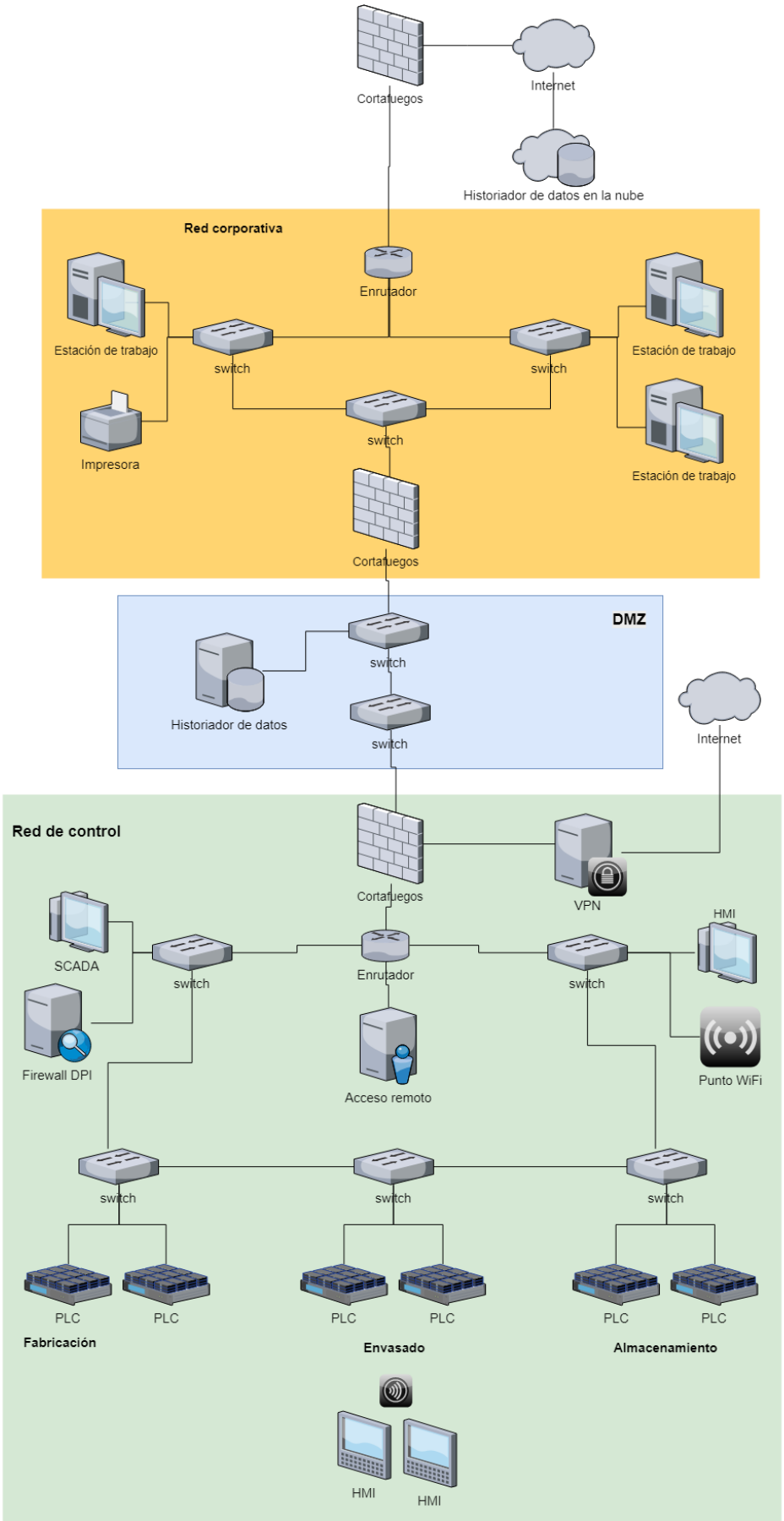


Figura C.2: Ejemplo de arquitectura de seguridad en la red de una fábrica de refrescos.

Teniendo en cuenta el contexto, puede considerarse que, bajo esta nueva arquitectura, en la fábrica existen tres zonas: la red corporativa (que incluye las estaciones de trabajo, impresoras, el centro de datos corporativo, el DNS, etc.), la DMZ (en la que se encuentra el historiador de datos local) y la red de control (que incorpora todos los mecanismos y sistemas del proceso de fabricación, envasado y almacenamiento, además de los HMI, el SCADA y el acceso remoto para los técnicos).

La separación de la primera zona (la red corporativa) se ha llevado a cabo mediante una segmentación física de la red, concretamente mediante un cortafuegos. La tercera zona (la red de control), por su parte, también ha sido separada del resto mediante segmentación física, utilizando un segundo cortafuegos que, a su vez, consigue crear una segunda zona (la DMZ), independiente gracias a los cortafuegos de la red corporativa y el de la red de control.

Dentro de la DMZ se encuentran dos *switches* gestionables de capa de enlace. El primero (situado entre la red corporativa y la DMZ), se encarga de comunicar y restringir el acceso al historiador de datos (desde la red corporativa y únicamente cuyo origen coincida con las direcciones de las máquinas autorizadas para ello). El segundo (situado entre la DMZ y la red de control) es el encargado de permitir al historiador recibir los datos e información de los ICS (desde la red de control y únicamente desde las máquinas autorizadas). Así mismo, estos controles de acceso a la DMZ se refuerzan con las reglas de los cortafuegos, que permiten únicamente el tráfico que proviene de los sistemas de control autorizados y que utiliza el protocolo correspondiente (estas reglas están incluidas en el cortafuegos de la red de control) y el acceso a las máquinas autorizadas (y a través del protocolo correspondiente) desde la red corporativa a la DMZ (habiendo sido aplicadas estas reglas en el cortafuegos de la red corporativa).

A su vez, en la red de control, pueden apreciarse tres subzonas: fabricación, envasado y almacenamiento. Los procesos de fabricación, envasado y almacenamiento pueden considerarse críticos, ya que una interrupción y/o alteración en sus sistemas podría generar grandes pérdidas económicas a la empresa. Por ello, se ha incluido un cortafuegos de inspección de paquetes (DPI, *Deep Packet Inspection*) para asegurar que la comunicación entre los PLCs de cada una de las tres subzonas y el sistema SCADA se hace sobre el protocolo correspondiente, autenticando además la dirección IP y la MAC de cada uno de los dispositivos en las comunicaciones. Los *switches* también han sido configurados para permitir únicamente el intercambio de datos entre los activos de las subzonas y el SCADA, restringiendo la comunicación únicamente a las direcciones de las máquinas y sistemas que deben poder intercambiar paquetes.

También ha sido necesaria la creación de una cuarta subzona para incluir en ella el servidor de máquinas virtuales de todos los entornos de desarrollo de los PLCs asociados al proceso de fabricación, envasado y almacenamiento. El acceso a este servidor se realiza a través de un servidor VPN desplegado para ello, controlándose este acceso mediante una autenticación fuerte en el propio VPN y una segunda autenticación en el cortafuegos de la red de control. Además, el cortafuegos se encuentra correctamente configurado (mediante reglas que controlan tanto las direcciones origen-destino como el puerto utilizado y el protocolo) para permitir únicamente el acceso a este servidor de máquinas virtuales desde el servidor de VPN (y viceversa).

Por último, se incluye una subzona que reúne todos los sistemas HMI, incluidos los que se conectan vía wifi y el punto de acceso para comunicar estos últimos. El *switch* que disgrega esta zona, se encuentra correctamente configurado para permitir únicamente las comunicaciones desde/a las subzonas de fabricación, envasado y almacenamiento (los *switches* de estas tres subzonas mencionadas, a su vez, han sido configurados para hacer lo mismo con la subzona de los HMI).

BIBLIOGRAFÍA

[1] Jefatura del Estado, «Ley 8/2011, de 28 de abril, por la que se establecen medidas para la protección de las infraestructuras críticas,» 28 Abril 2011. [En línea]. Available: https://www.boe.es/boe/dias/2011/04/29/pdfs/BOE-A-2011-7630.pdf. [Último acceso: 21 Abril 2018].

[2] Gobierno de España, «BOE - Disposición 18439,» 2011.

[3] Gobierno de España, «BOE - Disposición 10060,» 2015.

[4] Ministerio del Interior, «Real Decreto 704/2011, de 20 de mayo, por el que se aprueba el Reglamento de protección de las infraestructuras críticas,» 20 Mayo 2011. [En línea]. Available: https://www.boe.es/buscar/pdf/2011/BOE-A-2011-8849-consolidado.pdf. [Último acceso: 21 Abril 2018].

[5] CCI, «La protección de infraestructuras críticas y la ciberseguridad industrial,» 2013.

[6] Ministerio de Defensa, «REAL DECRETO 421/2004, de 12 de marzo, por el que se regula el Centro Criptológico,» 12 Marzo 2004. [En línea]. Available: https://www.boe.es/boe/dias/2004/03/19/pdfs/A12203-12204.pdf. [Último acceso: 21 Abril 2018].

[7] CCI, «Estado de Cibersegurdiad en los Operadores de Infraestructuras Críticas Españolas.,» Check Point, Edición 2017.

[8] Consejo Europeo, «Directiva 2008/114/CE del Consejo de 8 de diciembre de 2008 sobre la identificación y designación de infraestructuras críticas europeas y la evaluación de la necesidad de mejorar su protección,» 08 Diciembre 2008. [En línea]. Available: https://www.boe.es/doue/2008/345/L00075-00082.pdf. [Último acceso: 21 Abril 2018].

[9] Gobierno de España, «Real Decreto 704/2011, de 20 de mayo, por el que se aprueba el Reglamento de protección de las infraestructuras críticas.».

[10] F. S. Jaén, «La Ley PIC y su aplicación en los Operadores Críticos».

[11] Gobierno de España, «La Comisión Nacional para la Protección de las Infraestructuras Críticas aprueba los Planes del Transporte Urbano y Metropolitano y de la Alimentación,» 01 Febrero 2018. [En línea]. Available: http://www.lamoncloa.gob.es/serviciosdeprensa/notasprensa/mir/Paginas/2018/010218-comision.aspx. [Último acceso: 28 Marzo 2018].

[12] F. S. Jaén, «Detalle de los contenidos de los PSO y los PPE».

[13] ADSI, J. Fernández Garrido y E. Landín López, «Infraestructuras Críticas e implantación del Sistema PIC en España,» *NEWS ADSI FLASH,* nº 429, 2017.

[14] PAe - Portal Administración electrónica, «MAGERIT v.3 : Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información,» [En línea]. Available: https://administracionelectronica.gob.es/pae_Home/pae_Documentacion/pae_Metodolog/pae_Magerit.html. [Último acceso: 02 Abril 2018].

[15] PAe - Portal Administración electrónica, «Centro de transferencia de Tecnología - MAGERIT versión 3,» [En línea]. Available: https://administracionelectronica.gob.es/ctt/magerit. [Último acceso: 02 Abril 2018].

[16] CN-CERT, «PILAR,» [En línea]. Available: https://www.ccn-cert.cni.es/herramientas-ciberseguridad/ear-pilar/pilar.html. [Último acceso: 21 Abril 2018].

[17] CN-CERT, «PILAR Basic,» [En línea]. Available: https://www.ccn-cert.cni.es/herramientas-ciberseguridad/ear-pilar/pilar-basic.html. [Último acceso: 21 Abril 2018].

[18] CN-CERT, «μPILAR,» [En línea]. Available: https://www.ccn-cert.cni.es/herramientas-ciberseguridad/ear-pilar/upilar.html. [Último acceso: 21 Abril 2018].

[19] certsi, «IEC 62443: Evolución de la ISA 99,» [En línea]. Available: https://www.certsi.es/blog/iec62443-evolucion-isa99. [Último acceso: 11 Mayo 2018].

[20] ISA, «Setting the Standard for Automation,» [En línea]. Available: https://www.isa.org/. [Último acceso: 11 Mayo 2018].

[21] NIST, «Guide to Industrial Control Systems (ICS) Security,» Washington, 2015.

[22] Washington University in St.Louis (Computer Science & Engineering), «Survey of Industrial Control Systems Security,» [En línea]. Available: http://www.cse.wustl.edu/~jain/cse571-11/ftp/ics/index.html. [Último acceso: 05 Mayo 2018].

[23] Quora, «What is the difference between PLC, DCS, and SCADA?,» [En línea]. Available: https://www.quora.com/What-is-the-difference-between-PLC-DCS-and-SCADA. [Último acceso: 05 Mayo 2018].

[24] iaona, «The IAONA Handbook for Network Security - Draft / RFC 0.4».

[25] F. Sevillano y M. Beltrán, «Diseño de zonas, conductos y canales según la normativa IEC 62443 (ISA99) en una Industria 4.0,» 2016. [En línea]. Available: http://ucys.ugr.es/jnic2016/docs/ActasJNIC2016.pdf. [Último acceso: 12 Mayo 2018].

[26] unitronicsplc, «What is the definition of "PLC"?,» [En línea]. Available: https://unitronicsplc.com/what-is-plc-programmable-logic-controller/. [Último acceso: 05 Mayo 2018].

[27] ICS-CERT, «Secure Architecture Design,» [En línea]. Available: https://ics-cert.us-cert.gov/Secure-Architecture-Design#nogo. [Último acceso: 09 Mayo 2018].

[28] Homeland Security, «NIPP 2013: Partnering for Critical Infrastructure Security and Resilience,» 2013.

[29] F. S. Jaén, «MAGERITv3 - Metodología de Análisis y Gestión de Riesgos Tecnológicos».