GUÍA SOBRE CONTROLES DE SEGURIDAD EN SISTEMAS OT

MINISTERIO DEL INTERIOR

SECRETARÍA de ESTADO de SEGURIDAD

GOBIERNO DE ESPAÑA
MINISTERIO DEL INTERIOR

En el mes de julio de 2020 se solicitó la colaboración de organismos públicos, empresas privadas y del sector académico con la finalidad de identificar las carencias de seguridad en los sistemas de operación, así como la definición de las medidas compensatorias que podrían subsanar dichas carencias.

En concreto, las entidades que han colaborado con sus respuestas son las siguientes:

ASOCIACIONES/FUNDACIONES	CCI
	Fundación Borredá
	Instituto El Cano
	ISACA
CONSULTORAS	Deloitte
	EY
	GMV
	Grupo SIA-INDRA
	Ecix
	Capgemini
EMPRESAS	Enigmedia
	Aiuken Solutions
	NextVision
	Agbar
	Ingenia
	Entelgy Innotec Security
FABRICANTES	Check Point Software Technologies
	Tecnalia/PESI
	Siemens
UNIVERSIDADES	Universidad Pontificia Comillas
	Universidad de Málaga
COORDINACIÓN	ISMS Forum
	Oficina de Coordinación de Ciberseguridad

CONTENIDO

1. INTRODUCCIÓN Y CONTEXTO ACTUAL

1.1 Introducción.

Sin lugar a dudas las tecnologías de la información y las comunicaciones (TIC) hoy soportan la gran mayoría de los servicios que se prestan a nivel mundial. Persisten muy pocos servicios esenciales para el ser humano cuyo correcto funcionamiento no dependa de las tecnologías de la información.

Esto se está produciendo a gran velocidad de cambio y es consecuencia de la búsqueda de la eficiencia en todos los sectores. En los últimos años estos procesos de cambio tienen como vehículo conductor los programas de transformación digital, en los que prácticamente toda institución está inmersa. El actual escenario hará que esa dependencia de la Tecnologías de la información sea aún mayor en el futuro.

La digitalización de los procesos industriales incorpora grandes oportunidades, quizás algunas muy necesarias para la humanidad. Seguramente las tecnologías y la digitalización de los sectores industriales ayudarán, entre otras cosas, a la reducción de las emisiones de CO2.

Frente a estas oportunidades que nos brindan las tecnologías disponibles, tales como c*loud, big data, machine learning, inteligencia artificial, IoT, 5G*, etc., se encuentran también las amenazas a las que dichas tecnologías están sometidas.

Hasta hace poco tiempo, en el entorno Industrial se tenía una falsa sensación de seguridad debido a la creencia de no existencia de riesgo. Esa sensación estaba basada principalmente en cinco ideas preconcebidas:

- La planta está aislada, no está conectada a internet.
- Tenemos un *firewall* que nos protege.
- Los hackers no saben de sistemas/procesos industriales.
- Mi planta no es objetivo de nadie.
- Los sistemas de *safety* de planta nos protegen de los ciberataques.

El riesgo que se debe gestionar está asociado a la probabilidad de que nuestros activos sufran una indisponibilidad o pérdida de integridad para prestar servicio o daños (impacto).

La visibilidad o superficie de exposición, que en las redes de entornos industriales, en adelante ***OT (Operation Technology)***, se ha visto incrementada en los últimos años y que por tanto, aumenta la probabilidad de un incidente de ciberseguridad.

En la actualidad, los sistemas *OT* padecen de los mismos males tradicionales que los sistemas ***IT (Information Technology)*** debido a la convergencia y la conectividad que estamos viviendo.

Las consecuencias de un mundo convergente, donde cada vez crece más la necesidad de mantener todo conectado, hacen que las redes industriales, históricamente aisladas, comiencen a tener la necesidad de conectarse, utilizando protocolos como *TCP/IP*, inseguros en su definición, encapsulando paquetes tradicionales de protocolos propietarios, como *MODBUS*.

Aunque una organización decida mantener el sistema *OT* desconectado de sus redes corporativas o de internet, los dispositivos que se utilizan para configurar y mantener estos, son portátiles, *pendrives*, tabletas y *smartphones*, que han tenido contacto previo con internet,

y con sistemas operativos *Microsoft Windows*, por lo que sigue existiendo riesgo si no se aplican políticas de seguridad.

Los sistemas de automatización y control industrial o ***ICS (Industrial Control Systems)***, y los sistemas ***SCADA (Supervisor Control and Data Acquisition)***, ampliamente conocidos estos últimos en el sector, estaban aislados de la red pública internet, incluso de la *LAN* privada de la organización. Disponían de sus propias redes *OT*, pero, poco a poco, sus protocolos propietarios y cerrados, convergieron hacia protocolos de red abiertos, buscando en ocasiones una reducción de costes en la programación y la gestión, que se decide hacer de forma remota aprovechando la infraestructura *IT* existente.

A nadie se le escapa el que existan instalaciones industriales, soportadas actualmente por sistemas operativos o *hardware*, cuyos fabricantes dejaron de dar soporte hace varios años o cuya incorporación de perfiles de ciberseguridad y por ende, cultura de ciberseguridad en los entornos industriales, es aún incipiente.

Seamos o no conscientes de lo que implica el párrafo anterior, el problema introducido es mayor de lo que parece, debido a que estamos juntando dos entornos *IT* y *OT*, con **necesidades de conocimiento específico y ciclos de vida diferentes**, que complicarán el establecimiento de **prioridades**, a la hora de disminuir el riesgo de ciberataque en la organización.

Se debe tener en cuenta también, que un incidente de ciberseguridad en un entorno industrial, puede tener **un impacto más allá del mundo digital**, donde un ciberataque *IT* tradicional podrá disminuir el valor de la organización, dañar su imagen de marca, etc., un entorno industrial es capaz de poner en marcha de forma automática actuadores y mecanismos que **modifican nuestro mundo físico** pudiendo provocar:

- Daños medioambientales.
- Afectación a la salud pública y a las vidas humanas.
- Interrupción de servicios esenciales para la ciudadanía.

Nos enfrentamos pues a grandes retos debido a la convergencia, la adopción de las *IT* en las *OT*, y la fuerte demanda de conectividad, donde han salido a la luz debilidades tradicionales en los sistemas *IT*, ahora en instalaciones críticas, y en ocasiones sin tener en cuenta que:

- En muchas ocasiones, el personal de planta o terceras personas, que hacen uso de estas tecnologías, no están **debidamente formados**.
- Derivado de lo anterior, se **desconocen los riesgos** que supone la utilización de ciertas tecnologías *IT* sobre entornos *OT*, no aplicando medidas de control.
- También sucede, que el personal de *IT*, *OT* y ciberseguridad no aúnan esfuerzos y conocimientos para aplicar medidas y controles de seguridad.

El caso más sonado, sin duda, ha sido ***Stuxnet***, pero cada vez son más las infraestructuras críticas que sufren alguna intrusión: plantas de energía, gas, metalúrgicas, *PLC* aislados en internet y un largo etcétera. Basta hacer una búsqueda en **shodan.io** o visitar su apartado dedicado a *ICS* para ver el número de equipos conectados a internet sin ningún tipo de salvaguarda. Igualmente, una consulta a la *MITRE ATT&CK for ICS*[1] permite valorar la cantidad de amenazas a las que estos sistemas están expuestas.

La automatización industrial no es algo novedoso, los *ICS* existen desde hace mucho tiempo y funcionan correctamente, sin embargo, la integración con las redes *TCP/IP* les hacen ser foco de atención, y ya no se les puede considerar entornos aislados. Organizaciones crimi-

[1] https://collaborate.mitre.org/attackics/index.php/Main_Page

nales o grupos patrocinados por estados, tienen capacidades y conocimiento para acceder a los controles de un sistema industrial/instalación por la vía del *malware* especializado y otras técnicas.

Por todo esto, aquellos que tienen la responsabilidad de brindar servicios esenciales, mantener negocios sostenibles, asegurar con éxito el desarrollo de la I+D nacional, o quienes tienen la responsabilidad de velar por la seguridad de la ciudadanía, tienen el gran desafío de hacerlo acompañando a los negocios de forma que sean competitivos, pero bajo unos niveles de riesgo conocidos, aceptados y gestionables.

Afortunadamente, la preocupación está, y en mayor o menor medida, todos los *stakeholders* (empresas del sector industrial, proveedores de servicios, universidades, reguladores, asociaciones) tienen planes para hacer frente a estos nuevos desafíos.

1.2 *Safety & Security*.

Sin lugar a duda, quienes diseñaron o diseñan instalaciones industriales, han tenido siempre muy en cuenta los aspectos de *safety*, pero quizás en el pasado no tuvieron en cuenta los aspectos de *security*, especialmente los de *cybersecurity*. El lenguaje español no distingue las acepciones de las palabras *SAFETY* y *SECURITY*, en inglés. Pero estas palabras sí que tienen conceptos diferenciales. De una forma muy resumida podría decirse:

"***Safety***" suele aplicarse a la protección contra riesgos más o menos fortuitos, tales como accidentales, desastres naturales, etc.

"***Security***" suele aplicarse a la seguridad ante actos de naturaleza intencionada (robos, intrusiones, vandalismo, agresiones. La ciberseguridad (*cybersecurity*) está dentro de este concepto, pero circunscrito al contexto de la seguridad de la información y los sistemas.

Cabe destacar que la ciberseguridad en el mundo *OT* no puede basarse en los mismos criterios y enfoques que se utilizan para el mundo *IT*. Por resumirlo se podría decir que en el mundo *IT* la ciberseguridad está gestionada con la información como punto central (***Information Centric***), mientras que en el mundo *OT* la ciberseguridad debe focalizarse con los procesos como punto central (***Process Centric***). De esta forma se consigue un mejor entendimiento entre los ingenieros de plantas y los expertos de ciberseguridad, tema que se hace fundamental en proyectos de mejora de la ciberseguridad industrial.

1.3 Redes de tecnologías de la operación (*OT) y* sistemas de control industrial (*ICS)*.

Los *ICS* se basan en 3 etapas:

- Medición de los datos del proceso (monitorización).
- Evaluación de la información obtenida en cuanto a parámetros estándar.
- Control del proceso en base a la información medida y evaluada.

Estos sistemas de control pueden ser completamente manuales, automatizados en su totalidad, o ambas formas (híbridos).

Los sistemas conocidos como *SCADA* permiten evaluar desde una consola la información de múltiples puntos de un proceso y tomar decisiones de control.

Esto nos lleva a la necesidad describir cuáles son los componentes habituales de una red *OT*:

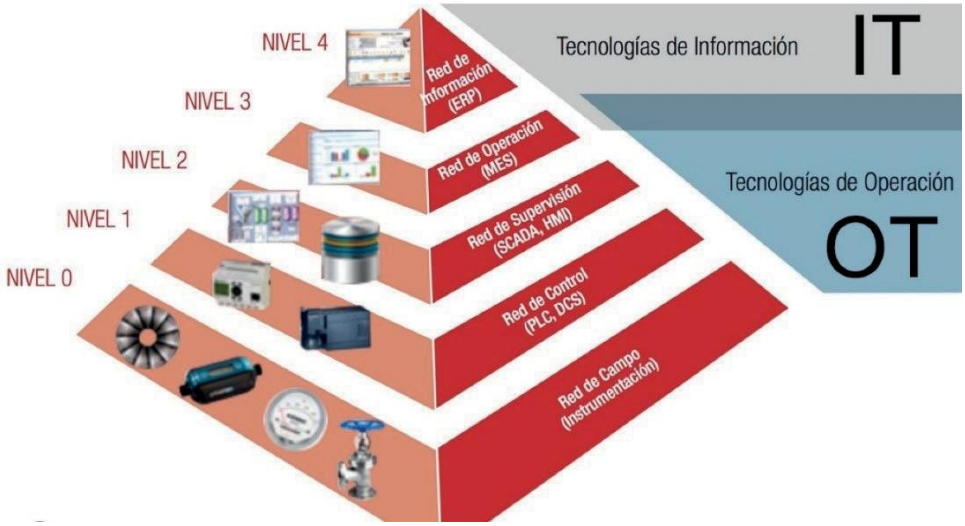


Ilustración1 https://www.cci-es.org/Guia_Piramide

Capa inferior (0). Capa de los Sensores y Actuadores, sería como la capa física, donde lo que importa es el medio o los dispositivos de campo y se transmiten señales, que pueden ser tanto analógicas como digitales, con las particularidades que ello implica.

Entrarían aquí, por ejemplo: sensores de movimiento, sensores de temperatura, sensores de niveles, sensores magnéticos, actuadores, etc.

Capa (1). Se puede encontrar:

- ***PLC*** (*Programmable Logic Controller)*, dispositivo que permite la automatización de un proceso electromecánico, controlando el funcionamiento de las máquinas empleadas en la producción.

- ***RTU*** (*Remote Terminal Unit*) un microprocesador capaz de adquirir señales de campo y actuar en consecuencia en base a una programación existente.

- ***DCS***[2] (*Distributed Control System*), se comunica con los dispositivos de campo y presenta los datos a un ***HMI*** (*Human-Machine Interface*), obteniendo información de los *PLC* o de las *RTU*.

Capa (2). Nivel de los ***HMI/SCADA***, que recolecta toda la información de los *PLC* y/o *RTU* distribuidos de manera automática, y empezamos a encontrarnos con un protocolo conocido: *TCP/IP*. Es el interfaz que utilizan, por ejemplo, los operadores de planta.

Capa (3). Nivel de los ***MES*** (*Manufacturing Execution System*) cuyo objetivo no es la evaluación del proceso en sí mismo, sino la de su eficiencia a partir de la información recibida.

Capa (4). Aquí tendrían cabida los ***ERP*** (*Enterprise Resource Planning*), donde básicamente se decide qué tipo de controles se ejecutarán, con qué frecuencia y con qué esfuerzo, con el objetivo de disponer de una planificación coherente.

[2] Los términos y conceptos de DCS y SCADA son muy similares entre sí, y en ocasiones se utilizan indistintamente, dependiendo del sector.

1.4 Seguridad en la cadena de suministro.

Las infraestructuras *OT* están muy vinculadas a servicios y tecnologías muy específicas, que necesitan ser provistos por especialistas, que en la mayoría de las veces son terceras partes y para ello requieren con frecuencia un importante nivel de interconexión con ellas. Asimismo, muchas de las organizaciones que proveen este tipo de servicios y que provienen del ámbito industrial, no poseen una cultura de ciberseguridad, ni cuentan en muchos casos con áreas expertas en esta materia. Esto implica que los sistemas del cliente sean accedidos por personal externo, expertos en los servicios que proveen, pero pertenecientes a organizaciones donde la seguridad está mucho menos desarrollada que en aquellas provenientes del campo de *IT*. Esto puede traer como consecuencia, prácticas inseguras que pongan en riesgo la infraestructura *OT*, ya de por sí más vulnerable por los puntos vistos anteriormente.

A través de los proveedores se pueden materializar infinidad de riesgos, siendo algunos de los más destacables, la explotación de vulnerabilidades de sistemas *OT* al exponerse a los equipos o redes de los proveedores, la infección de *malware* existente en los equipos o redes del proveedor, la exfiltración de información, al existir, en general, un bajo control de datos y tráfico intercambiado, la indisponibilidad de sistemas debido a acciones del proveedor que podría suponer un enorme impacto por la frecuente ausencia de copias de seguridad en estos entornos, etc. En general, los mismos riesgos que en el entorno *IT* pero agravados por la propia naturaleza de los entornos *OT* que se ha visto antes.

1.5 *IoT* & Privacidad.

Cabe destacar, que muchas redes *OT* en la actualidad están gestionando procesos industriales, pero los procesos de digitalización de la industria, con la incursión de soluciones *IoT* en entornos industriales, hace necesario que se tengan en cuenta aspectos relacionados con la privacidad, cuyo ámbito está fuertemente regulado por *GDPR*.

En este nuevo escenario de los entornos industriales que se fundamentan en la interconexión de múltiples dispositivos inteligentes que automatizan procesos y generan gran cantidad de información, plantean nuevas oportunidades que exigen una revisión del concepto de privacidad que se tenía tradicionalmente en los entornos industriales.

La recolección de datos personales de los usuarios es inherente al funcionamiento de estos dispositivos, con independencia del nivel de consciencia del empresario, profesionales técnicos y usuario en cuanto a la información personal que está revelando con el uso de este nuevo paradigma digital integrado en los entornos industriales.

Todo lo anteriormente expuesto, obliga a quienes estén inmersos en este tipo de proyectos a que deben realizar un análisis pormenorizado de los diferentes riesgos y amenazas a tener en cuenta en sus sistemas de operación, y de los diferentes tratamientos de datos personales que se puedan efectuar con los datos almacenados.

Por tanto, habrá que contemplar controles orientados a preservar la privacidad en los entornos industriales, donde la aplicación de los principios rectores de la normativa de protección de datos aplicable en Europa, como la privacidad por defecto y por diseño (*PbD*) es la mejor evidencia para demostrar la debida diligencia en el ejercicio de "responsabilidad proactiva" exigida en la misma.

Incluyendo los conceptos de *PbD*, se incorporan los principios de privacidad dentro de los procesos de diseño, operación y gestión de los sistemas de una organización para alcanzar un marco de protección integral en lo que a protección de datos se refiere.

Durante el desarrollo de la guía se verán distintos controles específicos para garantizar la privacidad de los datos de carácter personal que puedan almacenarse y tratar en los entornos industriales.

2. MARCO REGULATORIO

La Estrategia de Ciberseguridad Nacional.

La Orden PCI/487/2019, de 26 de abril, es la norma a través de la cual se publica la Estrategia Nacional de Ciberseguridad (en adelante, ENCS).

La ENCS es el marco de referencia de un modelo integrado cuyas bases son la implicación, coordinación y armonización de todos los actores y recursos del Estado, la colaboración público-privada, y la participación de la ciudadanía.

La Estrategia, para el logro de sus objetivos, crea una estructura orgánica, integrada en el marco del Sistema de Seguridad Nacional, que debe servir para articular la acción única del Estado conforme a unos principios compartidos por los actores en un marco institucional adecuado.

Los objetivos para la ciberseguridad, bajo los principios unidad de acción, anticipación, eficiencia y resiliencia por los que se rige la Estrategia, dedican un objetivo específico (Objetivo I) a la "Seguridad y resiliencia de las redes y los sistemas de información y comunicaciones del sector público y de los servicios esenciales".

En dicho objetivo se destaca la necesidad de que estos operadores se involucren activamente en un proceso de mejora continua respecto de la protección de sus sistemas, y se conviertan en modelo de buenas prácticas en la gestión de la ciberseguridad.

Además, se recoge el principio de responsabilidad compartida, en virtud del cual el sector público debe mantener estrechas relaciones con las empresas estratégicas e intercambiar conocimiento para garantizar la adecuada coordinación y cooperación en el entorno de la ciberseguridad.

La Estrategia desarrolla, por último, el marco estratégico e institucional compuesto por los *CSIRT* de referencia o equipos de respuesta a incidentes que analizan los riesgos y que, como puerta de entrada, supervisan los incidentes, difunden alertas y aportan soluciones para mitigar sus efectos, remitiendo las notificaciones oportunas a las Autoridades competentes.

Ley de Protección de las Infraestructuras Críticas

La Ley 8/2011, de 28 de abril, por la que se establecen medidas para la protección de las infraestructuras críticas ("Ley PIC"), traspone 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.

Por infraestructura crítica se entiende aquel elemento, sistema o parte de este cuyo funcionamiento resulta indispensable para el mantenimiento de las funciones sociales vitales, la salud, la integridad física, la seguridad y el bienestar social y económico, y cuya perturbación o destrucción tendría graves consecuencias.

La Ley concibe la seguridad al servicio del ciudadano y del Estado, estableciendo objetivos y líneas de acción para la protección de infraestructuras críticas, y tiene por objeto "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 estas contra ataques deliberados de todo tipo, con el fin de contribuir a la protección de la población".

Derivado de la Ley y de su Reglamento de desarrollo, en 2012 se constituyó el Sistema Nacional de Protección de Infraestructuras Críticas (Sistema PIC) que consiste en un conjunto de agentes del sector público y privado con competencias y responsabilidades en esta materia.

La Ley PIC aporta, asimismo, la creación del Catálogo Nacional de Infraestructuras Estratégicas como instrumento con toda la información y valoración de las infraestructuras estratégicas, y crea el Centro Nacional de Protección de Infraestructuras Críticas (CNPIC), que es el órgano encargado del impulso, coordinación y supervisión de las actividades encomendadas al Ministerio del Interior en relación con la protección de infraestructuras críticas en España.

Por último, de la Ley PIC emana el Plan Nacional de Protección de Infraestructuras Críticas, con el fin de dirigir y coordinar las actuaciones para proteger las infraestructuras críticas, y los Planes Estratégicos Sectoriales, que recogen los criterios definidores de las medidas a adoptar para hacer frente a una situación de riesgo partiendo de las características propias de cada uno de los sectores.

Reglamento de protección de las infraestructuras críticas

La Ley PIC se desarrolla a través del Real Decreto 704/2011, de 20 de mayo, por el que se aprueba el Reglamento de protección de las infraestructuras críticas.

Su finalidad es la de desarrollar, concretar y ampliar los aspectos contemplados en la citada Ley, teniendo en cuenta la necesaria articulación de los órganos y entidades, tanto de las Administraciones Públicas como del sector privado, así como el diseño de un planeamiento orientado a la prevención y protección de las infraestructuras críticas frente a las amenazas o actos terroristas que eventualmente puedan utilizar como canal a las tecnologías de la información y las comunicaciones.

El Reglamento prevé que los operadores de infraestructuras críticas designen a un Responsable de Seguridad y Enlace, así como un Delegado de Seguridad por cada una de las infraestructuras críticas identificadas, que tendrán las competencias recogidas en la propia norma.

El Reglamento contempla los Planes de Seguridad del Operador, como documentos estratégicos definidores de las políticas para garantizar la seguridad del conjunto de instalaciones o sistemas de su propiedad o gestión. Asimismo, se prevén los Planes de Protección Específicos, como documentos operativos donde se deben definir las medidas adoptadas y las que se vayan a adoptar por los operadores para garantizar la seguridad integral, ya sea física o lógica, de las infraestructuras de su propiedad o gestión.

Sus artículos 23 y 26 (Aprobación, registro y clasificación) prevén la aprobación de los Planes de Seguridad del Operador y Planes de Protección Específicos o las propuestas de mejora de los mismos, para lo que se promueve el desarrollo de un esquema de acreditación que podrá estar basado en un estándar internacional (*NIST, ISO/IEC*), o en una normativa específica (en el caso de España, el Esquema Nacional de Seguridad aprobado mediante el Real Decreto 3/2010, de 8 de enero).

Esquema Nacional de Seguridad

El Real Decreto 3/2010, de 8 de enero, regula el Esquema Nacional de Seguridad en el ámbito de la Administración Electrónica (en adelante ENS).

El ENS tiene por objeto "establecer la política de seguridad en la utilización de medios electrónicos en el ámbito de la presente Ley, y está constituido por los principios básicos y requisitos mínimos que garanticen adecuadamente la seguridad de la información tratada".

El ámbito de aplicación del ENS es el Sector Público, que se compone por las instituciones cuyo funcionamiento se rige por los artículos 2º de las leyes 39/2015 y 40/2015, respectivamente, y lo indicado sobre el sector público institucional.

El mandato principal del ENS viene establecido en su artículo 11, según el cual "todos los órganos superiores de las Administraciones públicas deberán disponer formalmente de su política de seguridad que articule la gestión continuada de la seguridad, que será aprobada por el titular del órgano superior correspondiente". Esta política de seguridad se establecerá en base a unos principios básicos y se desarrollará aplicando los requisitos mínimos previstos en el propio Esquema.

Desde su aprobación, el ENS ha sido, primero modificado por el Real Decreto 951/2015, al objeto de actualizarlo a las nuevas necesidades tecnológicas, así como al contexto regulatorio internacional y europeo.

Posteriormente, por la Resolución de 13 de octubre de 2016, de la Secretaría de Estado de Administraciones Públicas, por la que se aprueba la Instrucción Técnica de Seguridad de conformidad con el Esquema Nacional de Seguridad, que en su apartado VII (Soluciones y servicios prestados por el sector privado) indica: "Cuando los operadores del sector privado presten servicios o provean soluciones a las entidades públicas, a los que resulte exigible el cumplimiento del Esquema Nacional de Seguridad, deberán estar en condiciones de exhibir la correspondiente Declaración de Conformidad con el Esquema Nacional de Seguridad, cuando se trate de sistemas de categoría BÁSICA, o la Certificación de Conformidad con el Esquema Nacional de Seguridad, cuando se trate de sistemas de categorías MEDIA o ALTA, utilizando los mismos procedimientos que los exigidos en esta Instrucción Técnica de Seguridad para las entidades públicas.".

Esta última referencia normativa va alineada con lo dispuesto en la Disposición Adicional primera de la Ley Orgánica de Protección de datos y garantía de derechos digitales, Ley 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales.

Ley de seguridad de las redes y sistemas de información

Mediante el Real Decreto-ley 12/2018, de 7 de septiembre, de seguridad de las redes y sistemas de información, se transpuso al ordenamiento jurídico español la Directiva europea 2016/1148 (conocida como Directiva *NIS*) relativa a las medidas destinadas a garantizar un elevado nivel común de seguridad de las redes y sistemas de información en la Unión Europea.

El Real Decreto-ley tiene por objeto regular la seguridad de las redes y sistemas de información utilizados para la provisión de los servicios esenciales y de los servicios digitales, y establecer un sistema de notificación de incidentes en nuestro país.

Dicha norma determina, asimismo, la forma y criterios de identificación de los servicios esenciales y de los operadores que los presten. Además, recoge el marco estratégico e insti-

tucional de la seguridad de las redes y sistemas de información en España haciendo énfasis en la cooperación entre autoridades públicas.

También se disponen las potestades de inspección y control de las autoridades competentes y la cooperación con las autoridades nacionales de otros Estados miembros, se tipifican una serie de infracciones y sanciones, y se establecen las obligaciones de seguridad de los operadores.

Finalmente regula la notificación de incidentes, con especial atención a los incidentes con impacto transfronterizo y a la información y coordinación con otros Estados de la Unión Europea para su gestión.

Desarrollo de la Ley de seguridad de las redes y sistemas de información

El Real Decreto-ley 12/2018 ha sido desarrollada a través del Real Decreto 43/2021, de 26 de enero, que transpone de manera definitiva la Directiva (UE) 2016/1148 del Parlamento Europeo y del Consejo, de 6 de julio de 2016, relativa a las medidas destinadas a garantizar un elevado nivel común de seguridad de las redes y sistemas de información en la Unión.

En este Real Decreto se desarrollan cuestiones como la figura del Responsable de Seguridad de la Información, se establecen las medidas de seguridad mínimas que se han de adoptar, relaciona las Autoridades sectoriales competentes, establece una plataforma única de notificación de incidentes y relaciona los incidentes que han de ser comunicados, entre otras cuestiones.

ISA 99/IEC62443, ISO 27001, ISO 27002, NIST 800-82

Existen diferentes estándares internacionales que abordan de alguna manera la ciberseguridad de los sistemas industriales.

Entre otros, cabe destacar el estándar *ISA 99/IEC62443* que constituye un marco de referencia internacional para la ciberseguridad de sistemas *OT*.

Este estándar pone el foco en la disponibilidad y la integridad de los elementos más importantes, estableciendo un ciclo de vida para la ciberseguridad industrial consistente en tres pasos: evaluación, desarrollo e implementación y mantenimiento.

Podemos considerar además otros estándares como las *ISO 27001 y 27002* en cuanto a la seguridad de la información, o la *SP NIST 800-82*, que aborda la seguridad en los sistemas de control industrial, proporcionando una visión general de los *ICS* y las topologías típicas de los sistemas, identificando amenazas y vulnerabilidades, así como las correspondientes contramedidas de seguridad.

3. RECOMENDACIÓN DE MEDIDAS BÁSICAS DE SEGURIDAD

Antes de comenzar a desarrollar el presente capítulo, es muy importante señalar que tanto el Real Decreto-ley de seguridad de las redes y sistemas de información, como la LPIC o el ENS, establecen como punto de partida para la elección de las salvaguardas el análisis de riesgos.

Alineados con ese pilar básico, el objetivo de este apartado es sugerir un marco de medidas a modo de guía orientativa para los Operadores de servicios Esenciales (OSE) que presten servicios basados en infraestructura *OT*, de forma que permita disponer de mecanismos de prevención, detección, respuesta y recuperación ante incidentes de ciberseguridad en los sistemas de control industrial del operador. Dicho marco de medidas aportará información relevante para el análisis de riesgo, ayudando a verificar que los controles seleccionados cubren al menos el conjunto de medidas que identificamos en este capítulo. Finalmente, pretende minimizar los impactos que pueden afectar a la operación de las instalaciones, evitando pérdidas económicas, daños físicos, medioambientales y reputacionales.

3.1 Gestión de la ciberseguridad en Sistemas de Control Industrial (SCI).

La ciberseguridad de los SCI de los OSE se podrá gestionar mediante procesos globales y/o locales dependiendo del tamaño y tipo de operador.

Con el objetivo de establecer las prácticas con el mayor nivel de detalle posible de acuerdo a la realidad de cada entorno, se recomienda establecer o adaptar estas medidas en diferentes niveles operacionales, tomando como referencia los diferentes niveles del modelo de arquitectura *PERA* (por sus siglas en inglés, *Purdue Enterprise Reference Architecture*).

3.2 Medidas básicas recomendadas.

1- Asignación de roles y responsabilidades. Esta es una de las medidas más relevantes, no solo por su importancia, sino porque es la base para poder asegurar que las siguientes puedan implantarse y mantenerse, de forma que se cumplan con el objetivo marcado. En la medida de lo posible y basado en el modelo general de gobierno de compañía, debería asegurarse una segregación de funciones, de forma que se puedan identificar claramente las responsabilidades y las capacidades ejecutivas y técnicas que debe de tener cada rol.

- **Gobierno de la ciberseguridad en SCI**. Debe existir un rol de gobierno de la ciberseguridad en SCI y asignarse dentro de la estructura organizativa de la compañía.
- **Responsable de seguridad de la instalación**. Es el máximo responsable de la seguridad de la instalación.
- **Propietarios del SCI.** Es el responsable del sistema de control industrial.

2- Estrategia de Seguridad. Disponer de una estrategia de seguridad en las redes *OT* ayuda a garantizar el cumplimiento del resto de medidas indicadas a continuación. Esta estrategia debe estar formada, al menos por los siguientes puntos:

a. Marco normativo interno de seguridad integrando *IT* y *OT* (políticas, normas y procedimientos).

b. Necesidad de aplicar la gestión de riesgos para aplicar las medidas de seguridad adecuadas.

c. Necesidad de llevar a cabo la gestión de vulnerabilidades tecnológicas de los activos que constituyen las redes *OT*.

d. Gestión de incidentes de ciberseguridad.

3- Inventario actualizado de los SCI de la instalación. Disponer de un inventario completo de equipos SCI que se mantenga actualizado mediante la incorporación de los cambios resulta fundamental para la gestión de la seguridad en los SCI. Este inventario se puede utilizar en los análisis de riesgos y vulnerabilidades, así como en la respuesta ante incidentes. Los diferentes SCI de cada instalación deben de ser clasificados según criticidad para la prestación del servicio. Siendo esta la base del documento de aplicabilidad de los sistemas para la instalación.

En relación con el inventario, disponer de una guía de bastionado de los SCI actualizada en la que se recojan las buenas prácticas de configuración. Este guía recogerá las configuraciones generales de todos los SCI clasificadas por fabricante y será mantenida por los propietarios de los activos con el apoyo de los custodios.

4- Control de acceso lógico de los SCI. Disponer de medidas de control de acceso lógico a los SCI garantiza que una determinada entidad, usuario o proceso pueda, o no, acceder a un recurso del sistema para realizar una determinada acción. Para garantizar que los SCI cuentan con medidas de control de acceso adecuadas se debe tener en cuenta:

a. Que todo acceso esté prohibido, salvo concesión expresa.

b. Que la entidad quede identificada singularmente.

c. Que la utilización de los recursos esté protegida.

d. Que se definan para cada entidad los siguientes parámetros: a qué se necesita acceder, con qué derechos y bajo qué autorización.

e. Serán diferentes las personas que autorizan, usan y controlan el uso.

f. Que la identidad de la entidad quede suficientemente autenticada.

g. Que se controle tanto el acceso local como el acceso remoto (ver apartado “Control y supervisión de acceso remoto” incluido posteriormente).

5- Se configurarán los equipos SCI previamente a su entrada en operación, de forma que:

a. Se retiren cuentas y contraseñas estándar.

b. Se aplique la regla de "mínima funcionalidad":

1. El sistema debe proporcionar la funcionalidad requerida para que la organización alcance sus objetivos y ninguna otra funcionalidad.

2. El sistema no proporcionará funciones de operación, ni de administración, ni de auditoría, reduciendo de esta forma su perímetro al mínimo imprescindible.

3. Se debe desactivar mediante el control de la configuración, aquellas funciones que no sean de interés, no sean necesarias, e incluso aquellas que sean inadecuadas al fin que se persigue.

c. Se aplique la regla de "seguridad por defecto".

6- Arquitectura de Seguridad de redes *OT*. La seguridad de los SCI debe ser objeto de un planteamiento integral detallando, al menos, los siguientes aspectos:

a. Documentación de las instalaciones:

1. Áreas.

2. Puntos de acceso.

b. Documentación del sistema:

1. Equipos.

2. Redes internas y conexiones al exterior.

3. Puntos de acceso al sistema (puestos de trabajo y consolas de administración).

c. Esquema de líneas de defensa:

1. Puntos de interconexión a otros sistemas o a otras redes.

2. Cortafuegos y *DMZ*.

3. Utilización de tecnologías diferentes para prevenir vulnerabilidades que pudieran perforar simultáneamente varias líneas de defensa.

7- Segregación entre las redes de control y corporativas. La segregación entre la red del SCI y la corporativa garantiza una comunicación controlada y segura entre ambas, lo que proporciona protección recíproca frente a ataques cibernéticos provenientes de la otra red.

Desde el punto de vista de seguridad, se puede ver cada una de las distintas subredes como zonas con distintos requisitos de seguridad. La seguridad se consigue restringiendo los flujos de información entre esas zonas mediante soluciones de *SW* o *HW*. De esta manera se evita la propagación de ataques entre dichas subredes. Como ejemplo, las normas *IEC-62443-1-1 e IEC-62443-3-3* proporcionan definiciones y medidas de seguridad para las zonas y conductos; o la norma *IEC-62351*, que aborda medidas de seguridad para sistemas de control aplicados a entornos de energía, muchas de las cuales se pueden generalizar para cualquier sistema industrial.

La segmentación entre la red del SCI y la corporativa se debe segmentar garantizando que haya:

a. Control de entrada de los usuarios que llegan a cada segmento.

b. Control de salida de la información disponible en cada segmento.

c. Las redes se pueden segmentar por dispositivos físicos o lógicos. El punto de interconexión estará particularmente asegurado, mantenido y monitorizado.

8- Trazabilidad. Se deben registrar las actividades de los usuarios en los sistemas SCI, de forma que:

a. El registro indique quién realiza la actividad, cuándo la realiza y sobre qué información.

b. El registro incluya la actividad de los usuarios y, especialmente, la de los operadores *OT* y administradores en cuanto puedan acceder a la configuración y actuar en el mantenimiento del sistema.

c. El registro de las actividades realizadas con éxito y los intentos fracasados.

9- Gestión de incidentes. Se debe disponer de un procedimiento de gestión de incidentes de seguridad que garantice la adecuada gestión de mismo. Este procedimiento debe garantizar el tratamiento de incidentes de seguridad que puedan tener un impacto en la seguridad de los SCI, incluyendo:

a. Procedimiento de reporte de incidentes reales o sospechosos, detallando el escalado de la notificación.

b. Procedimiento de toma de medidas urgentes, incluyendo la detención de servicios, el aislamiento del sistema afectado, la recogida de evidencias y protección de los registros, según convenga al caso.

c. Procedimiento de asignación de recursos para investigar las causas, analizar las consecuencias y resolver el incidente.

d. Procedimientos para informar a las partes interesadas, internas y externas.

e. Procedimientos para:

1. Prevenir que se repita el incidente.

2. Incluir en los procedimientos de usuario la identificación y forma de tratar el incidente.

3. Actualizar, extender, mejorar u optimizar los procedimientos de resolución de incidentes.

10- Gestión de vulnerabilidades. Con el objetivo de prevenir los riesgos tecnológicos asociados a los SCI se debe llevar a cabo un plan de gestión de vulnerabilidades de estos, el cual debe de considerar los siguientes aspectos:

a. Contar con un mapa de activos actualizado de la red *OT*.

b. Contar con una herramienta automática de escaneo de vulnerabilidades.

c. Establecer escaneos periódicos de los activos de la red *OT* priorizando los activos críticos.

d. Subsanar las vulnerabilidades identificadas.

e. Creación de métricas e indicadores para potenciar el seguimiento de los resultados obtenidos.

11- Medidas *anti-malware* actualizadas. Las medidas destinadas a prevenir que los SCI puedan infectarse con *malware* y evitar su propagación, lo que garantiza la operación segura y fiable de los SCI. Estas medidas incluyen controles a nivel procedimental y técnico, destinados a detectar *malware* y prevenir infecciones. Asimismo, se debe contar con herramientas de detección o de prevención de intrusión (sondas análisis de tráfico).

12- Medidas preventivas y reactivas frente a ataques de denegación de servicio. Para ello se dotará a los SCI de estas medidas, para lo cual:

a. Se establecerá un sistema de detección de ataques de denegación de servicio.

b. Se establecerán procedimientos de reacción a los ataques, incluyendo la comunicación con el proveedor de comunicaciones.

c. Se impedirá el lanzamiento de ataques desde las propias instalaciones perjudicando a terceros.

13- Medidas de seguridad en relación con el uso de redes *WIFI* corporativas. En el caso en que los SCI hagan uso de redes *WIFI* corporativas, estas deberán contar con las siguientes medidas de seguridad:

a. Contar con un inventario de dispositivos haciendo una revisión periódica de este y de las posibles vulnerabilidades.

b. Crear una red de gestión exclusiva, que solo transporte tráfico de gestión y administración, en la que se empleen protocolos seguros.

c. Utilizar sistemas de autenticación centralizada como servidores *RADIUS* utilizando canales seguros.

d. Realizar una asignación mediante *DHCP* de dirección *IP* fija para cada cliente/dispositivo en cada una de las distintas redes.

e. Configurar los clientes para utilizar el protocolo *802.1X-EAP-TLS*, agente *NAC* y túnel *VPN* cifrado según lo recomendado.

f. Limitar el acceso físico a los equipos, así como el acceso lógico en función de los roles definidos y desactivar el servicio cuando no se esté utilizando.

g. Implementar sistemas de Detección de Intrusiones (*IDS*) para la detección de posibles anomalías que generen alarmas.

h. Monitorizar el tráfico de la red y realizar una búsqueda periódica de anomalías.

14- Procedimiento de parcheo para aplicaciones, sistemas operativos y *firmware*. Los parches de seguridad los publican los proveedores de sistemas operativos, *software* de aplicaciones y equipos para solucionar posibles vulnerabilidades en sus productos que pueden ser aprovechadas por atacantes potenciales. Los parches de seguridad deben ser aplicados según los procedimientos internos y siempre que estén validados por los fabricantes para la instalación en cuestión. Los contratos con proveedores de *software* deben contemplar los servicios parches de seguridad y la validación de los mismos en cada una de las instalaciones industriales.

15- Los equipos portátiles y dispositivos móviles que tengan acceso a redes *OT*, deberán cumplir con las siguientes medidas de seguridad:

a. Contar con un inventario de equipos portátiles junto con una identificación de la persona responsable del mismo y un control regular de que está positivamente bajo su control.

b. Establecer un canal de comunicación para informar, al servicio de gestión de incidentes, de pérdidas o sustracciones.

c. Limitar la información y los servicios accesibles a los mínimos imprescindibles, requiriendo autorización previa de los responsables del SCI y los servicios afectados.

d. Evitar en la medida de lo posible, que el equipo contenga claves de acceso remoto a la organización. Considerar claves de acceso remoto aquellas que sean capaces de habilitar un acceso a otros equipos de la organización, u otras de naturaleza análoga.

16- Protocolos seguros. Para garantizar la confidencialidad del tráfico generado por los SCI, estos deberán emplear protocolos considerados como seguros y soluciones específicas destinadas a tal efecto.

17- Controles para dispositivos extraíbles. Los medios extraíbles (ej.: memorias *USB*, discos duros externos, unidades *CD-ROM/DVD*) son una de las vías más habituales de infección por *malware*. Eliminar, o al menos, reducir el uso de medios extraíbles siempre que sea técnicamente posible y controlar su utilización cuando lo anterior no sea posible, reduce de manera notable el riesgo de infección por *malware*.

18- Control y supervisión de acceso remoto. Deberá implementarse mediante métodos seguros. El acceso remoto a los SCI presenta mecanismos potencialmente dañinos por *malware* y acceso no autorizado a los SCI, que pueden incidir en la operación segura y fiable. El acceso remoto ha de contar con una justificación de negocio e implementarse de forma que esté garantizada su seguridad y que únicamente personas autorizadas puedan hacer uso de esta funcionalidad.

Es recomendable que las comunicaciones de los dispositivos SCI con el exterior sean canalizadas a través de un *firewall*, que preferiblemente se defina una *DMZ* donde se alojen los servicios a los que se puedan conectar los dispositivos SCI y sean los servicios alojados en esta, los que se puedan conectar al exterior. De esta manera se limita mejor el perímetro y es más sencillo de proteger.

Asimismo, se aconseja implementar mecanismos que permitan limitar o bloquear los flujos de información para evitar la propagación de amenazas. En ese sentido, se recomienda bloquear cualquier protocolo de comunicación que no sea necesario para el teleservicio/acceso remoto, con el fin de reducir la superficie de ataque.

Finalmente, los accesos remotos a la infraestructura deben de ser monitorizados y registrados, de manera que puedan ser auditados en un futuro.

19- Plan de respuesta ante incidentes. Resulta esencial que los activos/instalaciones estén preparados ante tal eventualidad, a fin de minimizar su impacto y recuperar el nivel habitual de funcionamiento en el menor tiempo posible. Dada la imposibilidad de prever cada posible tipo de incidente, los planes se centran en la gestión del mismo, garantizando que el personal esté concienciado sobre la problemática de la ciberseguridad, formado para identificar fallos en planta como consecuencia de posibles fallos y/o sabotajes en los SCI. El personal se involucra activamente en el diseño, elaboración y pruebas de los ciberincidentes, estableciendo comunicaciones fluidas y la asignación clara de responsabilidades. Resulta fundamental ensayar los planes para someterlos a prueba y que todo el personal involucrado se familiarice con ellos.

20- Capacidades de copia de seguridad y restauración. La recuperación tras un incidente de seguridad, un fallo de *hardware* o *software* o un problema de corrupción de datos, pueden requerir la restauración total o parcial de uno o varios dispositivos o del sistema en su conjunto.

21- Control estricto sobre roles de administración y la Gestión del Cambio sobre los SCI. Los roles de administración, disponen de privilegios para realizar cambios en los SCI que pueden repercutir en la operación segura y fiable de los SCI, así como de la instalación controlada por estos. Los cambios en los SCI fuera de las operaciones rutinarias (ej.: cambio de *setpoints*, arranque/parada de equipos, apertura/cierre de válvulas) deben someterse a un estricto control, empleando los procesos de gestión del trabajo (ej.: permiso de trabajo) y gestión del cambio existentes en el activo o instalación, a fin de garantizar que los cambios se apliquen únicamente tras pasar por el proceso pertinente de diseño, revisión, pruebas y aprobación.

22- Gestión de archivos de registro y pistas de auditoria. Los archivos de registro y pistas de auditoría son necesarios tanto para la monitorización de eventos de seguridad y detección de anomalías como para la realización de análisis forenses tras cualquier incidente de seguridad.

23- Seguridad de la cadena de suministro. Para establecer un mecanismo seguro en la cadena de suministro, se relacionan las siguientes recomendaciones:

- Establecer un marco para gestionar el ciclo de vida del sistema de control industrial, centrándonos en seguridad por diseño, para minimizar las vulnerabilidades y así reducir la superficie de ataque (ver gestión de riesgos de ciberseguridad).

- Establecer alianzas duraderas en el ámbito de la ciberseguridad con todos los socios. Redactar contratos con acuerdos contractuales específicos sobre Ciberseguridad. Unificar políticas, normas y procedimientos.

- Elevar el nivel de formación y concienciación en ciberseguridad, tanto del personal interno *IT* y *OT*, como externo (proveedores, socios, etc), que estén involucrados en la operación de los sistemas de control industrial. Crear grupos de trabajo transversales *IT/OT* para que la cultura de ciberseguridad definida por la empresa se difunda en todos los niveles. Revisar periódicamente que el personal tiene el nivel requerido de competencia y habilidades (test, píldoras informativas, etc.).

- Análisis e intercambio de inteligencia sobre amenazas cibernéticas dentro del sector, como con los proveedores tecnológicos. Especial atención a los fabricantes de SCI. Establecer la obligatoriedad de notificación de vulnerabilidades, tan pronto se tenga conocimiento de ellas (diligencia especial dentro del mismo sector).

- Realizar revisiones periódicas de la estrategia de gestión de riesgos tecnológicos incluyendo a los socios de la cadena de suministro. Evaluación conjunta de vulnerabilidades, garantizando que el riesgo que surja de las deficiencias se aborda con una adecuada gestión de remediciónintegral.

- **Formación y concienciación del personal de** *OT***.** Se formará regularmente al personal técnico y de operación *OT* en aquellas materias que requieran para el desempeño de sus funciones, en particular en lo relativo a:

  a. Configuración de sistemas.

  b. Detección y reacción a incidentes.

  c. Gestión de la información en cualquier soporte en el que se encuentre. Se cubrirán al menos las siguientes actividades: almacenamiento, transferencia, copias, distribución y destrucción.

Se realizarán las acciones necesarias para concienciar regularmente al personal técnico y de operación *OT* acerca de su papel y responsabilidad para que la seguridad del sistema alcance los niveles exigidos.

En particular, se recordará regularmente:

  a. La normativa de seguridad relativa al buen uso de los sistemas.

  b. La identificación de incidentes, actividades o comportamientos sospechosos que deban ser reportados para su tratamiento por personal especializado.

  c. El procedimiento de reporte de incidentes de seguridad, sean reales o falsas alarmas.

- **Seguridad Física.** Las instalaciones donde se ubiquen los SCI dispondrán de elementos adecuados para el eficaz funcionamiento del equipamiento allí instalado. Y, en especial:

  a. Condiciones de temperatura y humedad.

  b. Protección del cableado frente a incidentes fortuitos o deliberados.

  c. Medidas de protección contra incendios.

  d. Medidas de protección contra inundaciones.

4. RESULTADOS OBTENIDOS

Las 116 carencias detectadas y las medidas compensatorias propuestas para su subsanación por las entidades colaboradoras se adjuntan en el **ANEXO I** del presente documento, agrupadas en 15 ámbitos para una mejor comprensión y facilidad de análisis.

Sobre este punto conviene incidir que muchas de las medidas recogidas en este Anexo I podrían ser también aplicadas a las subcontratas/proveedores.

Adicionalmente se incluye en el **ANEXO II** el estudio estadístico sobre las brechas de seguridad detectadas, así como el origen de la información.

En el **ANEXO III** se realiza una adaptación del catálogo de amenazas propuesto en la metodología MAGERIT, la cual está inicialmente destinada a sistemas de información. Este anexo proporciona algunos detalles que deben ser tenidos en cuenta en el tratamiento de redes en entornos *OT*.

Finalmente, en el **ANEXO IV** se incluye el glosario de términos.

ANEXO I – RESULTADOS DE LA CONSULTA

	ACCESOS LÓGICOS LOCALES	
	CARENCIA DE SEGURIDAD	**MEDIDAS COMPENSATORIAS**
1	Necesidad de permanencia de sesiones abierta en sistemas de supervisión impide la trazabilidad y auditoría.	Aumentar las medidas de control físico y a nivel de las redes. Sistema paralelo de registro de operador. Dispositivos adicionales en red que permitan establecer mecanismos de control de sesiones y bloqueo.
2	Control de sesiones y bloqueo en caso de ser necesario.	Aumentar las medidas de control físico y a nivel de las redes. Sistema paralelo de registro de operador. Dispositivos adicionales en red que permitan establecer mecanismos de control de sesiones y bloqueo. Integración de los intentos de sesión, tanto exitosos como fallidos, en *SIEM*.
3	Contraseñas "*hardcodeadas*". En muchos sistemas industriales existen contraseñas *hardcodeadas* de administración que, además, se encuentran publicadas en foros por internet.	Establecer controles a nivel de red sobre quién se conecta al equipamiento. Estos controles se pueden realizar con un *NGFW* industrial obligando al usuario, antes de conectarse al equipo afectado, a realizar una primera validación contra el *FW* y securizando la conexión entre el *FW* y el dispositivo fina en el caso de que el *FW* esté dotado de esta tecnología.
4	Existencia de un único usuario para todos los operadores. Permisos de administración para todos los usuarios. Política de contraseña débil, inexistente o la imposibilidad del software *OT* de adecuarse a una política de contraseñas robusta.	Creación de una política de credenciales y administración de usuarios que incluya, al menos: Creación de usuarios personalizados. Perfilado *RBAC (Role Based AccessControl)*. Políticas de contraseñas robustas. Registrar e identificar a las personas que hagan uso del usuario genérico compartido en caso de que no se pueda definir uno específico. Habilitar los *logs* de acceso y actividad en los sistemas a gestionar. Asegurar una identificación horaria de los usuarios que han accedido a la consola de operación. Puede ser con identificación con huella, con videovigilancia de la sala de operación, consola central de control de cuentas.

ANEXO I – RESULTADOS DE LA CONSULTA

5	Ciclo de vida de los usuarios	Implantación de políticas de gestión de privilegios asociada al ciclo de vida de los usuarios (p.e. asignación y revocación de accesos).
6	Usuarios con privilegios elevados con accesos a los sistemas.	Creación de cuentas nominales con los mínimos permisos funcionales.
7	Uso compartido de las cuentas locales administradoras.	Monitorización del uso de las cuentas compartidas mediante un registro independiente de entrada y salida al sistema.
8	Contraseñas embebidas en texto plano para aplicaciones.	Rotado de contraseñas embebidas en aplicaciones para evitar el conocimiento de las mismas.
9	Ausencia de doble factor de autenticación.	Integración de dobles factores de autenticación para el acceso a los sistemas.
10	Ausencia de flujos de trabajo de aprobación para cuentas críticas.	Creación de flujos de aprobación para cuentas con criticidad.
11	Ausencia de sistemas de monitorización y control de accesos.	Integración de sistemas de auditoria para el control de cuentas y accesos. Grabación de sesiones.
12	Ausencia sobre el control de políticas de contraseñas.	Integración de políticas de rotado eficientes, controladas y supervisadas de contraseñas.
13	Falta de control de las altas de usuarios en la consola de operación.	Implantar un proceso de autorización con segregación de funciones.
14	Federación segura en determinados escenarios *OT* como puede ser los sistemas de *Smart Grids*, en el que es necesario aplicar procedimientos de autenticación y de autorización estandarizados y siguiendo modelos distribuidos o descentralizados.	Estandarización de entornos federados *OT*, y siguiendo modelos de autenticación y autorización estandarizados, como por ejemplo el *RBAC* (IEC-62351-8), y bajo construcciones de red siguiendo los modelos de interconexión estándar. Estos puntos de interconexión normalmente deben/pueden recaer en g*ateways*, *proxies* o servidores de *Cloud*, *Fog o Edge*.

ANEXO I – RESULTADOS DE LA CONSULTA

	ACCESOS REMOTOS (USUARIO, MANTENIMIENTO, ETC.)	
	CARENCIA DE SEGURIDAD	**MEDIDAS COMPENSATORIAS**
1	Tele mantenimientos inseguros	Utilización de *VPN*. Creación de políticas de mantenimiento. Registro de todas las acciones de administración y mantenimiento llevadas a cabo de forma remota. Se puede reforzar mediante el empleo de un servidor de salto virtualizado que permita grabar entradas de teclado y las propias sesiones. Mención especial a los *softwares* de acceso remoto.
2	Interconexión del *OT* a la nube en la externalización de servicios.	Evaluar la posibilidad de centralizar la información en un único punto de gestión para la parte *OT* e *IT/Cloud*, simplificando las labores de los administradores de seguridad.
3	Uso de dispositivos móviles en el mundo *OT*.	Proteger estos nuevos mecanismos de conectividad con una solución de control de acceso que se pueda instalar en la línea de producción. Es deseable, para evitar introducir distintos elementos en la línea, que la solución cuente con la capacidad de facilitar el acceso a la red móvil. En el caso de dispositivos móviles corporativos, debe procederse al enrolamiento de los mismos en soluciones *MDM*. Definición de una lista blanca de dispositivos y/o implementación de soluciones que permitan llevar a cabo control o restricciones de los dispositivos móviles que accedan a la red *OT*.
4	Excesiva delegación a terceros en labores de mantenimiento.	Renegociación de contratos más favorable al cliente y con un control más exhaustivo sobre los contratos.
5	Accesos remotos a planta (parte *OT*) descontrolados o no auditables, por parte de terceras personas o subcontratas de partes de las instalaciones.	Gestión de accesos remotos seguros a planta y desde un único punto centralizado pasando por ambos *NGFW* que realizan la segregación *IT/OT*.
6	Gestión/administración de los sistemas industriales desde *PC* con salida a internet.	*Whitelisting* de equipos que permiten tener acceso a los sistemas *OT*.

ANEXO I – RESULTADOS DE LA CONSULTA

	PROTECCIÓN FRENTE A ATAQUES	
	CARENCIA DE SEGURIDAD	**MEDIDAS COMPENSATORIAS**
1	Inexistencia de seguridad proactiva. No existen mecanismos de seguridad proactiva en las redes industriales. Falta de sistemas de detección de ataques avanzados.	Contar con sistemas de protección reactiva como cortafuegos, sistemas *IPS*, sistemas de análisis de comportamiento, etc. Los cuales bloqueen los intentos de explotación de las vulnerabilidades de los sistemas industriales. Estos sistemas deben de contar también con capacidades antivirus, *Antibot*, control de ficheros y al menos *IPS* para la realización de *Virtual Patching* de las vulnerabilidades conocidas. Establecer procesos formales y herramientas a de Gestión de software malicioso / antivirus. Incluir funcionalidades *EDR* para la monitorización del comportamiento en los dispositivos que lo permitan.
2	Ataques de Denegación de Servicio.	Implementación de capacidades de detección de ataques *DOS* y *DDOS*. Implementación de capacidades de bloqueo y/o limitación del origen del ataque. Definición de planes de continuidad de negocio y minimización de riesgos asociados.
3	Protección ante ataques complejos.	Progresar en los sistemas de detección de intrusiones basados en anomalías (y, por tanto, en IA y *machine-learning*), e investigar en detección distribuida con soporte en técnicas de aprendizaje automático, *Big Data*, *NDR*, etc..
4	Falta de resiliencia en sistemas *OT*	Investigación en medidas correctivas basadas en métodos o mecanismos de restauración funcionando en tiempos óptimos (a ser posible en tiempo aproximadamente real). En caso de no poder retornar a un estado operativo similar al anterior a la manifestación del fallo, los sistemas deben permanecer en un estado seguro en el que no afecten a otros dispositivos empleados o servicios.

ANEXO I – RESULTADOS DE LA CONSULTA

	INVENTARIO	
	CARENCIA DE SEGURIDAD	**MEDIDAS COMPENSATORIAS**
1	Inexistencia de Inventarios.	Es necesario contar con herramientas de inventariado en tiempo real. Son especialmente interesantes los *BAD* descritos en la NISTIR 800-82r2 e incluidos en el modelo de referencia NIST1800-23 ya que, mediante la utilización de mecanismos pasivos, es decir, no intrusivos con el tráfico productivo, son capaces de realizar un inventariado de activos automático y en tiempo real. Estos sistemas además son capaces de identificar fabricante, *firmware*, número de serie, vulnerabilidades asociadas a la versión de *firmware* y sistemas operativos. Implantación de herramientas de auditoría automatizadas o semi-automatizadas que además se integren con herramientas de inventariado. De esta forma se dispondrá siempre de un inventariado actualizado de todos los activos existentes. Es recomendable, en la medida de lo posible, el mecanismo de inventariado se pueda obtener a partir del tráfico de red existente en la instalación. Realizar auditorías, para conocimiento de activos (Fabricante, Sistema Operativo, versión de hardware, versión de *firmware*, dirección *IP*, protocolo con el que se comunica, etc.). Todos estos datos se podrían obtener mediante *softwares* de mercado denominados *Industrial Anomaly Detection*. No se puede proteger aquello que se desconoce que se tiene.
2	Falta de control de instalación de dispositivos *IoT*.	Establecer un procedimiento de búsqueda de dispositivos a través del inventario exhaustivo de direcciones *IP*. Implantar procedimientos de control para la instalación de nuevos dispositivos. Vigilar los modelos de comunicación y asegurar los canales.

ANEXO I – RESULTADOS DE LA CONSULTA

	ARQUITECTURA DE RED	
	CARENCIA DE SEGURIDAD	**MEDIDAS COMPENSATORIAS**
1	Ausencia de definición de un diseño de arquitectura de seguridad de red para entornos *OT*.	Definición e implantación de un procedimiento que permita definir y regular un modelo de arquitectura base incluyendo la red *OT* y su relación con los entornos *IT*/corporativos. Aumentar las medidas de control físico y de acceso a redes. Reducir en la medida de lo posible las conexiones de equipos a más de una red. Incorporar sistemas de monitorización de red que permitan detectar intentos de acceso indebidos y cortafuegos donde sea posible. Concienciar y formar a operadores, ingenieros, desarrolladores y personal de mantenimiento. Establecimiento de procedimientos de acceso y uso de dispositivos de forma segura. En caso de que aplique/ establecer los accesos en la *DMZ*.
2	Falta de segmentación.	Realizar una segmentación, en la medida de lo posible teniendo en cuenta la norma de zonas de seguridad y conductos que propone la norma ISA99/IEC62443, con separación con cortafuegos de distintos fabricantes y respetando niveles Purdue. Además se deberá de crear una barrera *IT/OT* que incluyan varias *DMZ* donde se ubicarán los servidores de actualizaciones de firmas de los sistemas de seguridad *OT* y servidores de parches para los sistemas operativos generalistas existentes en la red *OT*. Una segunda *DMZ* se utilizará para crear máquinas de salto para dar acceso de forma segura a los telemantenedores. Uso de herramientas: Diodo de Datos, Cortafuegos, Control de acceso a red (*NAC*), *IDS/IPS* que soporten protocolos industriales. Uso estrictamente necesario de redes inalámbricas y solo si son seguras. Uso de mecanismos para la identificación de los dispositivos desplegados en el entorno para evitar la conexión de elementos no autorizados a la red. Implementar la segmentación de cada uno de las células de automatización en base a *switches* y *firewalls* industriales, ya que estos equipos están localizados en los armarios de fábrica, con sus correspondientes interferencias electromagnéticas, polvo, suciedad, etc.

ANEXO I – RESULTADOS DE LA CONSULTA

3	Inexistencia de una *DMZ IT/OT* En la arquitectura *OT* no existe una *DMZ IT/OT* en las plantas.	Esta *DMZ* es imprescindible ya que cumple con dos funciones: *1)* Albergar los sistemas de actualización de SO y *firmware* de los sistemas industriales 2) Red de acceso remoto seguro, donde se ubicarán máquinas de salto para realizar un telemantenimiento seguro.
4	Convergencia entre sistemas *IT* y *OT* Cada vez más se establecen relaciones y comunicaciones directas entre el mundo *IT* y el mundo *OT*. La diferencia de madurez a nivel de ciberseguridad de ambos mundos es abismal.	Deben de dotarse en los sistemas *IT* de soluciones que permitan protegerse contra ataques avanzados como *ransomware, antiphising, zero-days*, tanto a nivel de puesto de trabajo como a nivel de red, siendo deseable una gestión unificada y sencilla de los mismo. Gobierno de la Seguridad: Estructura, Roles, Funciones, Responsabilidades y procesos de gestión comunes o integrados, para el mundo *IT* y *OT*. Instalación de gestores de dominio *IT/OT* diferenciados que eviten en caso de la vulnerabilidad de uno de ellos, que el otro se vea vulnerado también. Abordar la integración de componentes de seguridad a nivel perimetral y a nivel de red, como *firewalls, IDS/IPS, VPN* y comunicación diodo. Establecer *VLANs* en *switches* de capa 3 y establecer *ACLs* entre diferentes segmentos de red. Aislar los puestos de control *OT* de salida internet y acceso a correo electrónico.
5	Falta de implementación de zonas y conductos en red *OT*.	Definición e implementación de segmentación de red *OT*.
6	Debilidades en los conductos entre capas de red.	Desarrollar una política de acceso que limite y controle los conductos habilitados entre capas. Vigilar especialmente los conductos que publican información del estado de variables y puntos de consigna.
7	Deficiencias de control de elementos activos de la red de operación.	Eliminar los administradores externos de *routers, switches* y *hubs* en la red de operación. Deshabilitar todos aquellos protocolos de red innecesarios en el sistema y limitar el uso de los mismos al mínimo (*hardening*).
8	Deficiencias de control de elementos de red, de uso corporativo.	Los subsistemas de control de acceso y videovigilancia, existentes en prácticamente todas las instalaciones industriales, suelen utilizar accesos a la red que pueden comprometer la seguridad de la misma, y por lo tanto se deberían establecer *VLANs* en *switches* de capa 3 y establecer *ACLs* entre el segmento de red de estos subsistemas de control de acceso y videovigilancia con el resto de redes.

ANEXO I – RESULTADOS DE LA CONSULTA

9	Deficiencias de control de elementos de comunicaciones inalámbricas.	Los subsistemas de conexión digital inalámbrica (*VHF*, satelital, *WIFI*, etc.) deben de contar con los mismos esquemas de control y de arquitectura que el resto de la red, para que no puedan comprometer la seguridad de la red.
10	Falta de documentación respecto a la topología de la red y protocolos de la misma.	Realizar auditoría para conocer cada uno de los componentes de red instalados en la fábrica y hacer una configuración de red detallada no solo con los componentes de red que existen, sino también sus IP y los distintos protocolos que se ejecutan entre cada uno de los componentes de la instalación. Todos estos datos se podrían obtener mediante software de mercado denominado *Industrial Anomaly Detection*.
11	Uso compartido de la *WIFI* corporativa.	Segregación de la *WIFI* para usos corporativos, de producción y personales. Implementación de medidas de control de acceso a redes *WIFI*, etc.

ANEXO I – RESULTADOS DE LA CONSULTA

	ANÁLISIS DE RED	
	CARENCIA DE SEGURIDAD	**MEDIDAS COMPENSATORIAS**
1.	Detección de anomalías en el tráfico.	Es recomendable la inclusión, en segmentos críticos, de sistemas de análisis de comportamiento y detección de anomalías (*BAD*), tal como indica la NIST 1800-23. Estos sistemas son los responsables de, recibiendo una copia del tráfico de la red, realizar una "foto" del estado de la planta incluyendo, protocolos, *SSOO*, fabricantes, modelo Purdue, inventariado de activos, descubrimiento de vulnerabilidades. Además, una vez se pasa el equipamiento a modo operacional, genera alarmas en base a: desviaciones del tráfico, cambio de protocolo, cambio de instrucción, *upgrade* de *firmware* de un *PLC*, *downgrade* de *firmware*, descarga de configuración, carga de configuración, un nuevo activo se descubra en la red.
2.	Ausencia de análisis de vulnerabilidades.	Establecer un mayor control de configuraciones, conexiones y actualizaciones de *software*. Incluir planes de acción para remediación.
3.	Ausencia de sistemas de gestión de eventos.	Integración de *SIEM* para el control de eventos y *logs* de sistema de aquellos sistemas que lo permitan.
4.	Se desconocen las vulnerabilidades existentes.	Aplicación de diagnósticos de vulnerabilidades.
5.	Ausencia de métodos efectivos para prevenir fugas de información.	Uso de herramientas *DLP* en los sistemas *OT* relacionados para el servicio con sistemas *IT*. Control / restricción de la información en dispositivos portátiles. Uso de herramientas *IRM (Information Right Management)*. Eliminación segura de información en dispositivos obsoletos. Restricciones de acceso externo desde la red industrial (uso de internet, *e-mail*, etc.). Normativa de uso de los medios.

ANEXO I – RESULTADOS DE LA CONSULTA

6.	Detección y tratamiento de incidentes de ciberseguridad incompletos.	Establecer procesos para la monitorización de eventos y detección, notificación y respuesta ante incidentes de ciberseguridad (*SIEM*, *SOAR*, etc.).
7.	Ausencia de monitorización de red	Además de la identificación de activos no inventariados la monitorización de red nos permite detectar anomalías (*BAD*) a través del análisis de los protocolos industriales en uso. El uso de *IDS/IPS* y *DPI* se puede completar con la integración de *honeypots*, *deceptions hosts*, etc.
8.	No realización de escaneo automático de vulnerabilidades.	Control de configuración, segmentación con *DMZ*, Control de conectividad indirecta, llave en cabinas, sistema de control de acceso a instalación y sala, Monitorización de red y *SIEM*.
9.	Automatización en las respuestas. Hasta la fecha las respuestas se basan en procedimientos manuales sin aún confiar en los sistemas *ICT* para liderar nuevas acciones y respuestas contra fallos, incidentes o ataques.	Investigación en mecanismos de respuesta automática o semi-automática para proporcionar prevención.
10.	Modelo y Herramientas para la identificación de Elementos críticos en la Infraestructura, sensibles a efectos en cascada que provoquen disrupciones graves del funcionamiento o servicio esencial.	Basarse en el Comité de Gestión de Resiliencia y Gestión integral de Riesgos. Posibles categorías sensibles: 1. Centros de control *SCADA*, monitorización. 2. Infraestructura tecnológica *IT* y *OT*. 3. Personal esencial- comité crisis, seguridad, emergencias, *O&M*, Sistemas y ciber...- incluidas subcontratas. 4. Procesos críticos de la instalación (operación, sistemas safety, logística, etc.). 5. Sistemas de Seguridad *security*. 6. Equipamientos y maquinarias esenciales (estación energía/cuadros eléctricos, sist. agua y gases, etc.). 7. Infraestructuras físicas (edificios y entorno geofísico, red de comunicaciones: carretera, tren, etc., poblaciones próximas y entornos naturales). 8. Servicios externos y suministros básicos. 9. Otros ámbitos específicos del Sector.

ANEXO I – RESULTADOS DE LA CONSULTA

	PROTOCOLOS DE RED	
	CARENCIA DE SEGURIDAD	**MEDIDAS COMPENSATORIAS**
1	Protocolos industriales en las comunicaciones entre controladores lógicos y sistemas de supervisión sin capacidad de mecanismos de control y/o cifrado.	Aumentar las medidas de control físico y a nivel de las redes. Concienciar y formar a operadores, ingenieros, desarrolladores y personal de mantenimiento. Dispositivos adicionales que permitan establecer mecanismos de control y cifrado.
2	Protocolos de comunicaciones industriales inseguros.	La medida ideal, pero la más complicada y la que lleva un periodo de implantación mucho más largo es que los fabricantes de Sistemas Industriales incorporen en sus soluciones protocolos seguros que incluyan cifrado por ejemplo. Incluir cifradores *HW* en las comunicaciones punto a punto. Estos cifradores no deben introducir latencias significativas. Incluir medidas de control del comportamiento de tráfico, de forma que, aunque no sea capaz de bloquear, sí que permita alertar de una anomalía de comportamiento en el tráfico de red.
3	Ausencia de políticas de control y procedimientos específicos para redes *OT* establecidos.	Definición de un *framework* de control que permita realizar una gestión efectiva del entorno *OT*.
4	Ausencia de seguridad en los múltiples protocolos de comunicación empleados por los dispositivos *OT*.	Empleo de arquitecturas basadas en *OPC UA* para la homogenización de las comunicaciones y el establecimiento de medidas de seguridad dentro de los protocolos empleados. Asegurar que el tráfico de comunicación entre los dispositivos y sus controladores/ se ejecute en un canal cifrado/ o en un micro segmento de red protegido.

ANEXO I – RESULTADOS DE LA CONSULTA

5	Desconocimiento de los protocolos *OT* usados para su posible protección.	Debido a que los protocolos *OT* no van cifrados, es recomendable evitar problemas de "*man in the middle*". Para ello, habrá que implantar soluciones como: uso de *VPNs* para comunicaciones a través de redes públicas, emplear *hardware* específico de seguridad que proteja la red local, utilizar sistemas de cifrado en las comunicaciones, utilizar doble factor de autenticación, etc.
6	Falta de estandarización general de la integración de sistemas *IT/OT* de manera segura. Hay pocos estándares que se centran en la integración de *IT* en entornos de *OT*, como es el caso del *IEC* 62351 (para entornos de energía), e incluso, si todos las tecnologías integradas siguen estándares específicos.	Estandarización a nivel nacional como internacional de la integración de tecnologías *IT* en entornos complejos de *OT*.

ANEXO I – RESULTADOS DE LA CONSULTA

	CONFIGURACIÓN	
	CARENCIA DE SEGURIDAD	**MEDIDAS COMPENSATORIAS**
1	Carencia de productos *OT* certificados en entorno *IT*. Equipos no certificados a nivel de ciberseguridad en la instalación.	Definición de protocolos y normas de certificación / Certificación de dispositivos industriales. Utilización de equipos diseñados bajo la premisa de Ciberseguridad y con garantías de mantenimiento de la misma durante el ciclo de vida del producto y a ser posible certificados, aunque como todos sabemos lo que hay que certificar en último término es el 100% de la instalación.
2	Utilización de sistema operativo de propósito general.	Implantación de una política de parcheo de los sistemas operativos de propósito general. Instalación de sistemas de seguridad reactivos que permitan realizar técnicas de parcheo virtual.
3	Carencias en copias de seguridad y en su gestión. Política de gestión de dispositivos los cuales sean susceptibles de conectar a la red *OT*. Ausencia o incorrecta gestión de *backups* centralizados (resiliencia).	Desarrollo e implantación de medidas cubriendo aspectos como planificación, copias remotas y pruebas de recuperación. Desarrollar e implantar un proceso de copias de seguridad, externas en la medida de lo posible, que asegure la existencia de copias para configuración, para *logs* de actividad y para *logs* de administración. En caso de ciberataque y *ransomware*, poder restaurar los sistemas desde un punto centralizado y con garantías de versionado.

ANEXO I – RESULTADOS DE LA CONSULTA

4	Existencia de configuraciones por defecto (puertos, contraseñas, etc.). Equipos de red no configurados correctamente. Existencia de Puntos muy sensibles. Deficiencias de control del *software* en la consola de operación. Deficiencias de control de versiones de *SW* y configuración de la consola de operación.	Desarrollo e implantación de políticas/ procedimientos técnicos de configuración y despliegue de tecnologías basada en necesidades que sustituya las configuraciones por defecto. Modificación de estructura de red para evitar el uso de equipos *dual home*. Establecer guías de bastionado de los dispositivos de red. Revisiones periódicas de la configuración. Identificación de esos puntos y creación de *DMZs*. Desarrollar un procedimiento para vigilar y evitar la instalación de aplicaciones no autorizadas, en particular ofimáticas (*Office, Chat*, etc.). Aparte del control de copias de seguridad, establecer un entorno de pruebas y un mecanismo de autorización de puesta en producción con segregación de funciones.
5	Servicios innecesarios en dispositivos *OT*. Configuraciones por defecto de dispositivos *ICS*. Carencia de bastionado de los equipos (por ejemplo, deshabilitar *USB*).	Deshabilitar protocolos: *Snmp; Telnet; UPnP, RDP, FTP*, etc., así como las conexiones que no sean estrictamente necesarias para el funcionamiento del sistema. Bloqueo de puertos. Eliminar/bloquear/cambiar cuentas y contraseñas por defecto. Bloquear servicios/ puertos, *plugins*, etc., no usados o inseguros. Uso de herramientas de gestión de la configuración. Deshabilitar recursos/procesos que no se requieren y aplicar medidas de bastionado.
6	Ausencia de sistemas de *Blacklist* o *Whitelist*. Falta de protección en el *End-Point*.	Configuración de *Blacklists* o *Whitelists* para denegar o permitir la ejecución de ciertos comandos en los sistemas. *Whitelisting* unido a diversas tareas de bastionado de la instalación.
7	Ausencia de gestión de flujos de trabajo autoservicio.	Configurar y diseñar el sistema de flujos para el autoservicio en las diferentes aplicaciones.
8	Deficiencias de control de continuidad de la operación.	Establecer un sistema de evaluación de riesgos, similar a los *BIAs*, para localizar debilidades de continuidad, ante fallos imprevistos en equipos, configuración de consola y *SW*.

ANEXO I – RESULTADOS DE LA CONSULTA

9	La falsa automatización de los procesos. Gestión automatizada de activos *IT/OT* y siguiendo modelos dinámicos específicos de gestión de identidad.	Existen muchos procesos que erróneamente se consideran automatizados, pues requieren de una administración, un control y unas gestiones adecuadas. Los procedimientos asociados a los procesos automáticos críticos deben documentarse adecuadamente e identificarse los roles que los supervisan. Diseño e implementación de modelos de gestión de identidad y *tracking* de activos existentes o nuevos.
10	Falta de integración de la seguridad en todas las etapas del desarrollo e implantación de nuevos sistemas y en los cambios. Medidas de seguridad no integradas en Dispositivos *ICS*, especialmente en aquellos de gama baja.	Establecer requerimientos de seguridad para los nuevos *ICS*. Integrar estos requerimientos en las distintas fases del desarrollo e implantación, así como en los cambios. Establecer un proceso de gestión de cambios en los *ICS*. Realizar evaluaciones de seguridad de los nuevos sistemas antes de su adquisición e implantación en producción. Uso de los paradigmas de seguridad *'Security by Design*', '*Privacy By Design*' y '*Security By Default´*.
11	Mala gestión de la confianza y la integridad.	La confianza debe establecerse en el entorno de arranque (*secure bootstrapping*) para que se pueda verificar la integridad del dispositivo desde el principio. Firmar el código de forma criptográfica para asegurar que no ha sido manipulado posteriormente y supervisar la ejecución del mismo para asegurar que no se ha sobrescrito. Permitir que un sistema vuelva a un estado que se sabía que era seguro.
12	Utilización de equipos *IT* en la parte *OT*, los cuales no están diseñados para aguantar los ambientes industriales.	Sustituir estos por equipos con hardware adecuado o trasladar a espacios adecuados y seguros físicamente, para conseguir una disponibilidad de la instalación a ser posible 24/7 pudiendo garantizar en la medida de lo posible la continuidad del negocio.
13	Protección *HW/SW* y "desde" sus diseños, conocido como "*security by design*", y afecta a la gran mayoría de dispositivos *OT*, los cuales presentan altas restricciones computacionales para gestionar recursos criptográficos (ej. *RTUs/PLCs*). Esto se debe considerar durante el diseño de estos componentes.	Contemplar medidas de protección a nivel *HW* como *TPM (Trusted Platform Module)* y *TEE (Trusted Execution Environment)* para crear un entorno de confianza ("root of trust"), arranque seguro y protección integra de los sistemas operativos. Para ello, también es fundamental abordar las actuales restricciones *HW/SW* de la mayoría de los controladores.

ANEXO I – RESULTADOS DE LA CONSULTA

	ACTUALIZACIONES Y OBSOLESCENCIA	
	CARENCIA DE SEGURIDAD	**MEDIDAS COMPENSATORIAS**
1	Dispositivos *legacy* sin capacidad de manejar identificaciones y/o autorizaciones en controladores lógicos (*PLCs, RTUs, DCS*).	Aumentar las medidas de control físico y a nivel de las redes. Concienciar y formar a operadores, ingenieros, desarrolladores y personal de mantenimiento. Establecimiento de procedimientos de acceso y uso de dispositivos legacy con condiciones de uso seguro. Ubicación de dispositivos legacy en segmentos de red aislados. Dispositivos adicionales que permitan manejar identificaciones y/o autorizaciones.
2	*Software* o *firmware* sin actualizar	Como medida compensatoria, se propone la utilización de mecanismos de parcheo virtual a nivel de red (dado que es muy complejo el poder instalar agentes por parte de soporte del fabricante los activos industriales). Estos mecanismos protegen a nivel de red a los activos afectados por las distintas vulnerabilidades, haciendo imposible su explotación. Es recomendable que este mecanismo no solo incluya firmas propietarias *IT* sino también firmas de protección propias de los sistemas industriales y que puedan añadirse firmas en formatos conocidos como *SNORT* o *YARA*. Acordar con el proveedor una estrategia y cronograma de implantación de parches. Establecer un plan de mitigación para cubrir la ausencia de parches críticos Además es recomendable la creación de *test-bed* o sistemas de pre-producción sobre los que probar el impacto de las actualizaciones de los sistemas asociados a los procesos industriales. Estos *test-bed* pueden ser bien físicos o bien virtuales. Encapsulamiento de sistemas operativos obsoletos tales como *Windows XP* o *Windows 7* mediante la virtualización de estos sistemas operativos. Uso de criptografía en los dispositivos para validación de nuevas versiones de software a través de firma digital en los procesos de actualización y evitar la manipulación de código. Establecer un sistema centralizado de gestionado de parches (*WSUS*) en el caso de que exista.

ANEXO I – RESULTADOS DE LA CONSULTA

3	Falta de soporte para la instalación de *endpoints* de seguridad en los sistemas *HMI*	Se debe de instalar en los sistemas de propósito general *endpoints* certificados por el fabricante de sistemas industriales que protejan contra ataques avanzados. Estos sistemas serán capaces de bloquear no solo contra amenazas conocidas sino también contra *zero days* o amenazas desconocidas.
4	Existencia de conexiones *WIFI* con *hardware* obsoleto que no permite desplegar mecanismos de seguridad (cifrado/ autenticación, etc.).	Sustitución de puntos de acceso por dispositivos que permitan un mayor nivel de seguridad. Implantación de sistemas *RADIUS*/ filtrados *MAC*. Empleo/ en la medida de lo posible de conexión cableada.
5	Deficiencias en la actualización de antivirus.	Acordar con el proveedor una estrategia y cronograma de implantación de antivirus. Establecer un plan de mitigación para cubrir los retrasos en la actualización. Proteger la capa más externa de la red con elementos de vigilancia, f*irewalls, IDEs* y similares.

ANEXO I – RESULTADOS DE LA CONSULTA

	TRAZABILIDAD, MONITORIZACIÓN	
	CARENCIA DE SEGURIDAD	**MEDIDAS COMPENSATORIAS**
1	Ausencia de registros de actividad en controladores lógicos (*PLCs*, *RTUs*, *DCS*).	Incorporar sistemas de monitorización y registro de actividad en la red. Incorporar sistemas de monitorización y registro de actividad en los sistemas que sea posible. Concienciar y formar a operadores, ingenieros, desarrolladores y personal de mantenimiento.
2	No se dispone de control sobre *reporting*.	Integración de un sistema de *reporting* para todo tipo de métricas y volumetría.
3	No se dispone de un sistema de escaneado de sistemas.	Configuración en integración de escáneres periódicos para mantener actualizado la integración de cuentas sobre los sistemas.
4	Ausencia de registro en la gestión de cambios en los sistemas.	Establecimiento de repositorios de registro e histórico de cambios.
5	Ausencia de sistema de registros de seguridad (accesos, conexiones externas, etc.).	Implantación de medidas de detección y registro automático descentralizado de cambios de seguridad y gestión de los mismos.
6	Falta de visibilidad del tráfico de red *OT*.	Instalación de sondas. Control de puertos y servicios *TCP/IP* abiertos inseguros y/o innecesarios, como pueden ser los puertos 23, 21 o 80, así como el uso de puertos *UDP* para realizar transacciones de control críticas. Establecer políticas de seguridad rigurosas, y planes de mantenimiento y de seguimiento frecuentes.

ANEXO I – RESULTADOS DE LA CONSULTA

7	Control rutinario de los servicios web, los cuales se establecen para realizar tareas de seguimiento en remoto o para la gestión administrativa. Muchas aplicaciones web pueden presentar deficiencias de seguridad que pueden liderar a múltiples tipos de ataques en remoto.	Establecer políticas de seguridad para verificar el código *Web* aplicado, establecer planes de seguimiento y monitorización de las aplicaciones web, y endurecer el acceso a la planta de control desde localizaciones remotas (incluida desde la red corporativa). Considerar la implantación de *WAF* (*Web Application Firewall*)
8	Auditoría, *accountability* (rendición de cuentas) y trazabilidad de acciones, especialmente en aquellos escenarios *OT* en el que haya federación de entidades, como puede ser los *Smart Grids*.	Adaptación de las nuevas tecnologías de tipo *Distributed Ledger Technologies (DLT)*, las cuales ofrecen inmutabilidad de los datos, seguridad y procedencia.

ANEXO I – RESULTADOS DE LA CONSULTA

	USO DE DISPOSITIVOS MÓVILES	
	CARENCIA DE SEGURIDAD	**MEDIDAS COMPENSATORIAS**
1	Deficiencias de control de equipos portátiles	Política de gestión de los dispositivos que sean susceptibles de ser conectados a la red *OT*. Limitar la posibilidad de que equipos portátiles se conecten a las redes *OT*. Vigilar cada conexión cableada. Implantar una política para impedir el acceso simultáneo a la red cableada y a la red *WIFI*. Robustecer la red *WIFI* de invitados. Los dispositivos no siempre tienen un identificador único que facilite el seguimiento, la supervisión y la gestión de los activos. El personal encargado de supervisar los hosts en la red, no necesariamente considera los dispositivos *IoT* como un *host* más. Se deben tener sistemas de rastreo que incluyan todos los activos por muy sencillos que sean, como por ejemplo los termostatos.
2	Utilización de equipos *IoT* de bajas prestaciones y sin medidas de ciberseguridad apropiadas.	Utilizar cuando sea posible componentes *IoT* y diseñados teniendo en cuenta la ciberseguridad y durante todo el ciclo de vida del producto. En los casos donde no sea posible deberán extremarse las medias de detección y control en el entorno de adquisición y en las infraestructuras de comunicaciones y en los sistemas de información de análisis de los datos adquiridos.
3	Aplicar políticas de *BYOD* sin considerar medidas preventivas y políticas de seguridad. De hecho, existen riesgos de infecciones por *USB* y por el autorun.inf.	Definir políticas de seguridad específicas para *BYOD* y revisar el estado actual de los dispositivos, pasando regularmente herramientas *anti-malware* o antivirus (ej. al inicio de la jornada), e instalar mecanismos de detección de intrusiones (principalmente basados en anomalías). También, es fundamental abordar planes de concienciación y formación en este aspecto.

ANEXO I – RESULTADOS DE LA CONSULTA

	CONCIENCIACIÓN, PERSONAL, FORMACIÓN	
	CARENCIA DE SEGURIDAD	**MEDIDAS COMPENSATORIAS**
1	Falta de cultura de seguridad en el mundo *OT*.	Establecer políticas de empresa de formación y concienciación.
2	Formación específica para empleados y usuarios.	Impartición de cursos específicos y regulares con registro de asistencia a los empleados/operadores de las infraestructuras/sistemas.
3	Formación de los perfiles técnicos de operación *OT* en competencias *IT*.	Capacitación específica en las carencias identificadas.
4	Formación de los perfiles técnicos de operación *IT* en competencias *OT*.	Capacitación específica en las carencias identificadas.
5	No disponer de un responsable de ciberseguridad *OT* dedicado y personal formado para atender las necesidades del área.	Asignar dicha responsabilidad.
6	No realización de simulacros de intrusión avanzada (*Red Team*) combinando vectores físicos, digitales e ingeniería social.	Realización de un tests de intrusión periódicos y ejercicios de coordinación de respuesta en caso de crisis.
7	Inexperiencia en respuesta a incidentes de ciberseguridad.	Contar con un servicio bajo demanda de apoyo en respuesta a incidentes de ciberseguridad.

ANEXO I – RESULTADOS DE LA CONSULTA

	SEGURIDAD FÍSICA	
	CARENCIA DE SEGURIDAD	**MEDIDAS COMPENSATORIAS**
1	Insuficiente aislamiento de los sistemas de control.	Implantación de medidas de control, tanto físicas como lógicas para restringir los accesos (p.e. servidores "enjaulados").
2	Sistemas de control de acceso inseguros.	Asegurar que el cableado y acceso a equipos críticos se encuentra protegido y seguro. Establecer controles de acceso (acceso contraseña/ llaves/ o acceso biométrico) a los sistemas críticos. Registro de histórico de accesos físicos al centro de control de los sistemas (logs de acceso/ grabaciones de videovigilancia). Identificación visual de la restricción de acceso a áreas críticas.
3	Falta de control de la consola de administración.	Ubicar la consola de administración en la Sala de Control. Implantar un sistema de logs de tipo *SIEM*.
4	Deficiencias en el acceso físico a la red de operación.	Implantar una separación y distancia entre las redes de control y la red corporativa que dificulte la conexión errónea o maliciosa entre redes.
5	Deficiencias en el control del acceso físico a las instalaciones.	El acceso a los lugares en los que existan dispositivos activos (sala de control, sala de *PLCs*, actuadores y sensores, salas de comunicaciones, torres y *Shelters* de comunicaciones etc.) debe ser restringido y controlado adecuadamente.
6	Ausencia de medidas de seguridad en dispositivos especialmente sensibles.	Catalogación de dispositivos sensibles. Aislamiento, control de acceso, alarma en cabinas y posibles rondas en casos excepcionales.
7	Falta de control en sistemas *CCTV*	Revisión periódica de los sistemas *CCTV*. Establecer un procedimiento para la protección de datos.

ANEXO I – RESULTADOS DE LA CONSULTA

	GESTIÓN DE PROVEEDORES	
	CARENCIA DE SEGURIDAD	**MEDIDAS COMPENSATORIAS**
1	Proveedores únicos o monopolio.	Identificar a los proveedores únicos y exigirles medidas adicionales. Diversificar proveedores.
2	Productos sin medidas de seguridad de fábrica.	Políticas de comprobación e implantación de seguridad en productos adquiridos. Testeo de seguridad de los productos adquiridos. Establecer medidas de seguridad de red a nivel de detección y protección.
3	Falta de procedimiento en la contratación de productos y servicios con especial atención a la cadena de suministros.	Procedimientos contractuales sólidos y revisados periódicamente por el cliente.

ANEXO I – RESULTADOS DE LA CONSULTA

	ESTRATEGIAS	
	CARENCIA DE SEGURIDAD	**MEDIDAS COMPENSATORIAS**
1	Laboratorios *OT* donde testar la vulnerabilidad de los equipos *OT* en redes *IT*.	Diseño e implementación de laboratorios propios o de terceros.
2	Requerimientos de seguridad en la adquisición de dispositivos.	Establecimiento y aplicación de una *baseline* de requisitos de seguridad según estándares como *IEC-62443-33* que formen parte de los procesos de adquisición tecnológica.
3	No disponer de un plan de continuidad de negocio implementado.	Haber realizado el *BIA* y aplicado alguna medida de contingencia esencial.
4	Falta de revisiones regulares de hacking ético frecuentes de toda la infraestructura.	Realización de al menos un análisis anual de vulnerabilidades a las infraestructuras más críticas.
5	La gestión de crisis y su comunicación asociada.	La gestión de crisis es uno de los aspectos primordiales a la hora de abordar escenarios complejos relacionados con fallos de seguridad. Su plan de comunicación asociado es vital. Desarrollar un adecuado Plan de Crisis e integrarlo en toda la organización y todos los sistemas críticos es vital. A la hora de su desarrollo el Plan de comunicación y el árbol de toma de decisiones escrítico.
6	Análisis del Impacto de los Sistemas en el Negocio.	En multitud de ocasiones se realizan grandes inversiones en protección de la información y la salvaguarda de sus activos. Sin embargo estas inversiones no están soportadas por un análisis riguroso del impacto en el negocio. Sistemas que pueden ser considerados como no críticos a priori, después de un análisis pueden realmente causar un impacto a la organización muy importante. Es esencial realizar un análisis de impacto.
7	Documentación apropiada de sistemas y su configuración.	Los sistemas y su configuración asociada deben de documentarse adecuadamente. Las guías de protección aplicadas (*Security Guidelines*) y su cumplimiento deben ser apropiadamente descritas. Deben establecerse requisitos estrictos en esta materia, especialmente para los sistemas más críticos.

ANEXO I – RESULTADOS DE LA CONSULTA

8	Los datos no es el aspecto critico de los sistemas.	En muchos casos la seguridad de la información no está construida en base a la criticidad de los datos asociados a los sistemas. Se realizan muchas inversiones en seguridad, pero no siempre están focalizadas en la protección de los datos almacenados o en tránsito. Es primordial proteger ambas partes de los sistemas: los repositorios y las comunicaciones.
9	Ausencia Responsabilidades de Seguridad definidas o poco claras en el mundo *OT*.	Creación de roles y responsabilidades de seguridad específicos para *OT* (*OT Security Managers*), dependientes de un rol común integrador de la Seguridad *IT/OT* (*CSO, CISO*, etc.).
10	Ausencia de objetivos de seguridad establecidos.	Establecer los objetivos de mejora de la seguridad de forma periódica. Planificar y asignar recursos para la consecución de los objetivos marcados. Establecer indicadores de evolución de la consecución de dichos objetivos.
11	Ausencia de Normas de Seguridad internas o de conocimiento de las mismas por el personal.	Identificación de la normativa aplicable. Establecer un Marco Normativo Interno de seguridad integrando *IT* y *OT* (políticas, normas y procedimientos). Considerar el Marco general para *OT*, y el específico para cada sector (da lugar a varios módulos verticales y horizontales). Difusión del Marco Normativo al personal implicado.
12	Falta de una clasificación y criticidad de la información e *ICS* formal y las medidas a aplicar.	Establecer una norma y procedimientos para la clasificación y criticidad de la información e *ICS*.
13	Ausencia de Gestión del Riesgo	Realización de *AARR* periódicos (anuales) o cuando haya cambios relevantes. Establecimiento de criterios de aceptación del riesgo. Realización de Plan de Tratamiento del Riesgo (PTR) / Plan Director de Seguridad (PDS).

ANEXO I – RESULTADOS DE LA CONSULTA

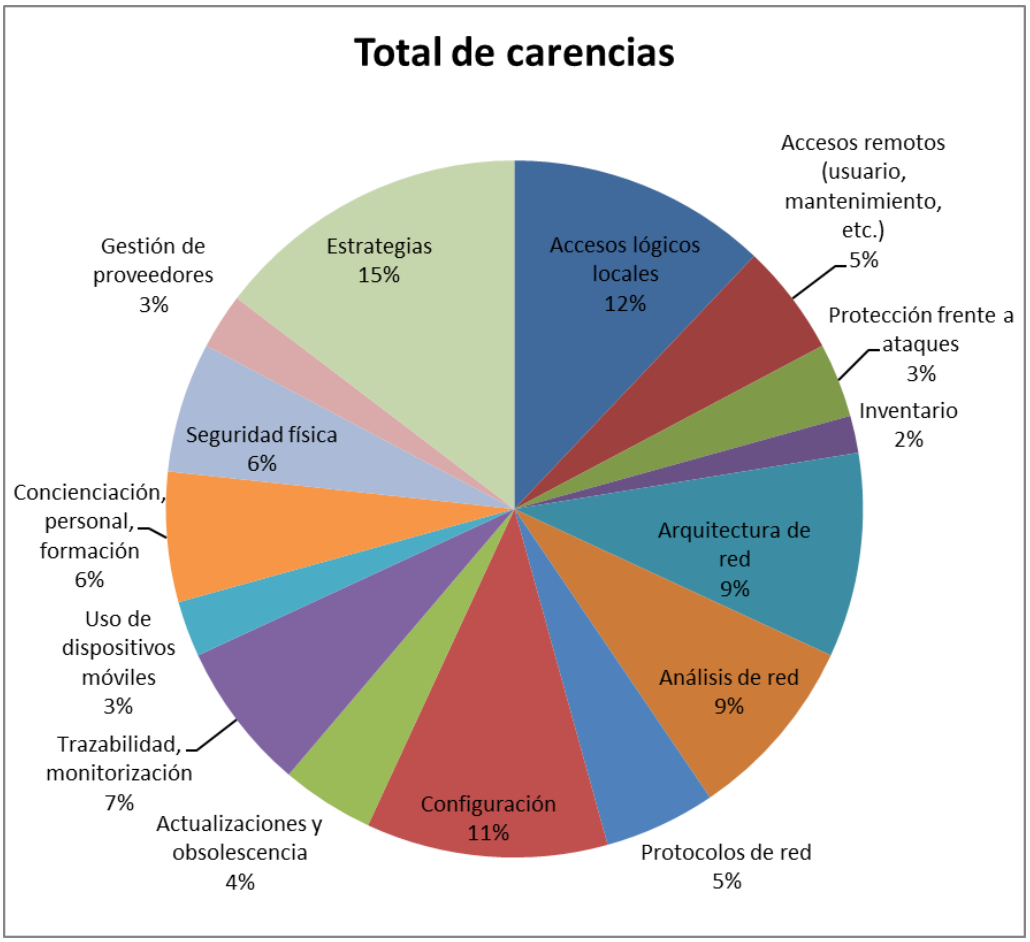
14	Falta de control de toda la cadena de suministro y complejidad de la misma.	Establecimiento de un proceso de Identificación, Evaluación y Gestión de proveedores. Identificación de interdependencias. Realización de *AARR* en la cadena de suministro. Sistema de Gestión de la cadena de suministro. Acuerdo con proveedores incluyendo seguridad (lógica, física y de las personas). Acuerdos de Nivel de Servicio (ANS). Establecer los requisitos de seguridad mínimos a cumplir por los proveedores.
15	Falta de conocimiento y control de Estado de la Seguridad y el Cumplimiento.	Establecimiento de un Marco de Controles. Proceso de Gestión del cumplimiento (implantación y revisión). Cuadro de Mando de Seguridad Integral. Establecer un plan de auditorías periódicas de Cumplimiento y Análisis de Vulnerabilidades y Planes para la corrección de las debilidades encontradas. Uso de herramientas de detección pasiva de vulnerabilidades. Establecer procesos de inteligencia de amenazas: detección de amenazas internas y externas. Uso de herramientas *GRC-IRM* para el Gobierno y Gestión de la Seguridad Integral.
16	Ausencia de Planes de Continuidad del Negocio formales.	Ausencia de Planes de Continuidad del Negocio formales. Realización de un análisis de impacto de negocio (*BIA)* para identificar los procesos críticos. Planes de Continuidad del Negocio. Planes de Gestión de Crisis. Normas y Procedimientos de Copias y recuperación de la información.
17	Falta de estudio de negocio en los sistemas y servicios relacionados con la Ciberseguridad.	Realizar auditoría para saber dónde estamos, dónde queremos llegar y un plan de cómo llegar al punto final, para poder hacer un presupuesto y poder discutirlo y aprobarlo con la dirección de la compañía.

ANEXO II – ESTADÍSTICAS

En forma de resumen, de las entidades consultadas se recabaron las siguientes carencias:

ÁMBITO	Nº CARENCIAS
Accesos lógicos locales	14
Accesos remotos (usuario, mantenimiento, etc.)	6
Protección frente a ataques	4
Inventario	2
Arquitectura de red	11
Análisis de red	10
Protocolos de red	6
Configuración	13
Actualizaciones y obsolescencia	5
Trazabilidad, monitorización	8
Uso de dispositivos móviles	3
Concienciación, personal, formación	7
Seguridad física	7
Gestión de proveedores	3

ANEXO II – ESTADÍSTICAS



ANEXO II – ESTADÍSTICAS

Número de entidades que han detectado carencias para cada ámbito:

	PARTICIPACIÓN POR ENTIDADES			
ÁMBITO	CONSULTORA	ASOCIACIÓN	UNIVERSIDAD	FABRICANTE
Accesos lógicos locales	2	2	0	3
Accesos remotos (usuario, mantenimiento, etc.)	1	0	0	4
Protección frente a ataques	0	1	1	3
Inventario	1	1	0	4
Arquitectura de red	2	2	1	5
Análisis de red	1	0	2	5
Protocolos de red	2	1	1	3
Configuración	2	2	1	4
Actualizaciones y obsolescencia	1	2	2	5
Trazabilidad, monitorización	1	2	1	2
Uso de dispositivos móviles	0	1	1	2
Concienciación, personal, formación	1	2	1	1
Seguridad física	2	1	0	2
Gestión de proveedores	2	1	0	5
Estrategias	1	1	1	5

ANEXO II – ESTADÍSTICAS

Representación en tanto por ciento de las entidades que han detectado carencias para cada ámbito, en relación con el número total de colaboradores de cada grupo:

	REPRESENTACIÓN POR ENTIDADES			
ÁMBITO	CONSULTORA	ASOCIACIÓN	UNIVERSIDAD	FABRICANTE
Accesos lógicos locales	100%	50%	0%	50%
Accesos remotos (usuario, mantenimiento, etc.)	50%	0%	0%	67%
Protección frente a ataques	0%	25%	50%	50%
Inventario	50%	25%	0%	67%
Arquitectura de red	100%	50%	50%	83%
Análisis de red	50%	0%	100%	83%
Protocolos de red	100%	25%	50%	50%
Configuración	100%	50%	50%	67%
Actualizaciones y obsolescencia	50%	50%	100%	83%
Trazabilidad, monitorización	50%	50%	50%	33%
Uso de dispositivos móviles	0%	25%	50%	33%
Concienciación, personal, formación	50%	50%	50%	17%
Seguridad física	100%	25%	0%	33%
Gestión de proveedores	100%	25%	0%	83%
Estrategias	50%	25%	50%	83%

ANEXO III – ADAPTACIÓN DE LAS AMENAZAS DEL CATÁLOGO MAGERIT A ENTORNOS OT

En base a la categorización realizada en el catálogo de amenazas MAGERIT – versión 3.0, existen cuatro tipologías de origen:

- Ataques intencionados.
- Desastres naturales.
- Errores y fallos no intencionados.
- De origen industrial.

Las amenazas identificadas a continuación se podrían duplicar, si fuera preciso, con el fin de establecer afectaciones diferentes en función del ámbito donde se puedan presentar dichas amenazas.

A.3	**Manipulación de los registros de actividad**	Los registros que en segundo plano crean las aplicaciones del ámbito *OT* no pueden garantizar su integridad por motivos técnicos u organizativos establecidos, impidiendo establecer imputabilidad.
A.4	**Manipulación de la configuración**	Prácticamente todos los activos dependen de su configuración y ésta de la diligencia del administrador: privilegios de acceso, flujos de actividades, registro de actividad, encaminamiento, etc.
A.5	**Suplantación de la identidad de usuario**	Cuando un atacante consigue hacerse pasar por un usuario autorizado, disfruta de los privilegios de este para sus fines propios. Es importante analizar el tipo de privilegios que implica la identidad suplantada y si la suplantación se ha producido en local o remoto.
A.6	**Abuso de privilegios de acceso**	Privilegio es una autorización especial otorgada a un usuario en particular para realizar operaciones de relevantes. El abuso de una cuenta privilegiada ocurre cuando se utilizan los privilegios asociados al usuario de forma inapropiada o fraudulenta, ya sea, con intencionalidad, de forma accidental o por ignorancia de los procedimientos.
A.7	**Uso no previsto**	Utilización de recursos del sistema para fines no previstos, típicamente de interés personal: juegos, consultas personales en internet, bases de datos personales, programas personales, almacenamiento de datos personales, etc.
A.8	**Difusión de *software* dañino**	Propagación intencionada de virus, *spyware*, gusanos, troyanos, ataques *DDOS* o *ramsomware* entre las principales categorías de *software* dañinos. Mención especial requiere el entorno Cloud mediante el cual un ataque puede afectar significativamente la actividad empresarial. Además del entorno *Cloud*, también habría que señalar aquellos ataques que proceden de la cadena de suministro.
A.9	**Re-Encaminamiento de mensajes**	Envío de información a un destino incorrecto a través de un sistema o una red, que llevan la información a dónde o por dónde no es debido. Puede tratarse de mensajes entre personas, entre procesos o entre unos y otros. Un atacante puede forzar un mensaje para circular a través de un nodo determinado de la red donde puede ser interceptado. Es particularmente destacable el caso de que el ataque de encaminamiento lleve a una entrega fraudulenta, acabando la información en manos de quien no debe.

ANEXO III – ADAPTACIÓN DE LAS AMENAZAS DEL CATÁLOGO MAGERIT A ENTORNOS OT

A.10	**Alteración de secuencia**	Alteración del orden de los mensajes transmitidos. Con ánimo de que el nuevo orden altere el significado del conjunto de mensajes, perjudicando a la integridad de los datos afectados o a las actuaciones realizadas.
A.11	**Acceso no autorizado**	El atacante consigue acceder a los recursos del sistema sin tener autorización para ello, típicamente aprovechando un fallo del proceso de autorización o del sistema de control de acceso.
A.12	**Análisis de tráfico**	El atacante sin necesidad de entrar a analizar el contenido de las comunicaciones es capaz de extraer conclusiones a partir del origen, destino, metadatos, volumen y frecuencia de los intercambios.
A.13	**Repudio**	Negación a posteriori de actuaciones o compromisos adquiridos en el pasado. Repudio de origen: Negación de ser el remitente u origen de un mensaje o comunicación. Repudio de recepción: Negación de haber recibido un mensaje o comunicación. Repudio de entrega: Negación de haber recibido un mensaje para su entrega a otro.
A.14	**Interceptación de información (escucha)**	El atacante llega a tener acceso pasivo a información que no le corresponde, sin que la información en sí misma se vea alterada.
A.15	**Modificación de la información**	Alteración intencional de la información, con ánimo de obtener beneficio o causar un perjuicio.
A.18	**Destrucción de información**	Eliminación intencional de información, con ánimo de obtener un beneficio o causar un perjuicio. Señalar la creciente migración de la información a entornos *cloud* con lo que ello significa respecto a los soportes clásicos.
A.19	**Divulgación de información**	Revelación de información relevante de forma deliberada.
A.22	**Manipulación de programas**	Alteración intencionada del funcionamiento de programas y *firmware*, persiguiendo un beneficio indirecto cuando se utilice.
A.23	**Manipulación de equipos**	Alteración intencionada del funcionamiento de los equipos, persiguiendo un beneficio indirecto cuando cuando se utilice.
A.24	**Denegación de servicio**	La carencia de recursos suficientes provoca la caída del sistema cuando la carga de trabajo es desmesurada.
A.25	**Robo**	La sustracción de equipamiento provoca directamente la carencia de un medio para prestar los servicios, indisponibilidad. El robo puede afectar a todo tipo de equipamiento, siendo el robo de equipos y el robo de soportes de información los más habituales.
A.26	**Ataque destructivo**	Sabotaje, vandalismo, terrorismo, acción militar, etc.
A.27	**Ocupación enemiga**	Cuando los locales han sido invadidos y se carece de control sobre los propios medios de trabajo.

ANEXO III – ADAPTACIÓN DE LAS AMENAZAS DEL CATÁLOGO MAGERIT A ENTORNOS OT

A.28	**Indisponibilidad de personal**	Ausencia deliberada del puesto de trabajo: Huelgas, absentismo laboral, bajas no justificadas, bloqueo de los accesos, etc.
A.29	**Extorsión**	Presión que, mediante amenazas, se ejerce sobre alguien para obligarle a obrar en determinado sentido.
A.30	**Ingeniería social**	Recopilación de información personal, sin el uso de la tecnología.
A.31	**Indisponibilidad de proveedores**	Ausencia deliberada de un proveedor: Huelgas, absentismo laboral, bajas no justificadas, bloqueo de los accesos, etc. Esta tipología de ataque afecta directamente a la cadena de suministro.
A.32	**Indisponibilidad de edificios / Instalaciones (A)**	Indisponibilidad de edificios / Instalaciones por ataques intencionados de origen interno o externos

DESASTRES NATURALES		
N.1	Todo aquel fenómeno natural peligroso para el sistema.	Existe una gran variedad dentro de las posibles categorías, tales como atmosférico, hidrológico, sísmico, volcánico o incendios. Algunos ejemplos concretos serían huracanes, tormentas, sequía, erosión, inundaciones, tsunamis, fallas, flujos de lava, hundimientos o incendios, frio o calor extremos, etc.

ANEXO III – ADAPTACIÓN DE LAS AMENAZAS DEL CATÁLOGO MAGERIT A ENTORNOS OT

ERRORES Y FALLOS NO INTENCIONADOS		
E.1	**Errores de los usuarios**	Equivocaciones de las personas cuando usan los servicios o los sistemas.
E.2	**Errores del administrador**	Equivocaciones de las personas con responsabilidades de instalación y operación.
E.3	**Errores en la monitorización**	• equipos no monitorizados • equipos no autorizados • medidas no monitorizadas • entradas / salidas no monitorizadas (de pdi) • *input data, output data, intermediate data*
E.4	**Errores en la configuración**	• servicios autorizados • flujos autorizados (*routing*) • protocolos autorizados • [formatos de] datos autorizados • cuentas de usuario no autorizadas (por defecto, personal ausente,…) • arquitectura del sistema (zonas y conducciones) • certificados (validación de firmas) • bastionado (fortificación) configuración [de seguridad]
E.7	**Deficiencias en la organización**	Cuando no está claro quién tiene que hacer exactamente qué y cuándo, incluyendo tomar medidas sobre los activos o informar a la jerarquía de gestión. Acciones descoordinadas, errores por omisión, etc.
E.8	**Difusión de *software* dañino**	Propagación inocente de virus, *spyware*, gusanos, troyanos, ataques *DDOS* o *ramsomware* entre las principales categorías de *software* dañinos. Mención especial requiere el entorno *Cloud* mediante el cual un error puede afectar significativamente la actividad empresarial. Además del entorno *Cloud*, también habría que señalar aquellos errores que proceden de la cadena de suministro.
E.9	**Errores de re-encaminamiento**	Envío de información a través de un sistema o una red usando, accidentalmente, una ruta incorrecta que lleve la información a dónde o por dónde no es debido; puede tratarse de mensajes entre personas, entre procesos o entre unos y otros. Es particularmente destacable el caso de que el error de encaminamiento suponga un error de entrega, acabando información en manos de quien no se espera.
E.10	**Errores de secuencia**	Alteración accidental del orden los mensajes transmitidos.

ANEXO III – ADAPTACIÓN DE LAS AMENAZAS DEL CATÁLOGO MAGERIT A ENTORNOS OT

E.15	**Alteración de la información**	Alteración accidental de la información. Esta amenaza sólo se identifica sobre datos en general, pues cuando la información está en algún soporte informático.
E.18	**Destrucción de información**	Pérdida accidental de la información. Esta amenaza sólo se identifica sobre datos en general, pues cuando la información está en algún soporte informático, hay amenazas específicas. Señalar la creciente migración de la información a entornos *cloud* con lo que ello significa respecto a los soportes clásicos.
E.19	**Divulgación de información**	Revelación por indiscreción. Incontinencia verbal, medios electrónicos, soporte papel, etc. La información llega accidentalmente a personas que no deberían tener conocimiento de ella. Señalara la creciente migración de la información a entornos *cloud* con lo que ello significa respecto a los soportes clásicos.
E.20	**Vulnerabilidades de los programas**	Defectos en el código que dan pie a una operación defectuosa sin intención por parte del usuario, pero con consecuencias sobre la integridad de los datos o la capacidad misma de operar.
E.21	**Errores de mantenimiento / actualización de programas**	Defectos en los procedimientos o controles de actualización de los equipos que permiten que sigan utilizándose programas con defectos conocidos y reparados por el fabricante.
E.22	**Errores de mantenimiento / actualización de equipos**	Defectos en los procedimientos o controles de actualización de los equipos que permiten que sigan utilizándose más allá del tiempo nominal de uso
E.24	**Caída del Sistema por agotamiento de recursos**	La carencia de recursos suficientes provoca la caída del sistema cuando la carga de trabajo es desmesurada.
E.25	**Pérdida de equipos**	La pérdida de equipos provoca directamente la carencia de un medio para prestar los servicios, es decir una indisponibilidad. Se puede perder todo tipo de equipamiento, siendo la pérdida de equipos y soportes de información los más habituales. En el caso de equipos que hospedan datos, además se puede sufrir una fuga de información.
E.28	**Indisponibilidad de personal (pandemia y otros)**	Ausencia accidental del puesto de trabajo: pandemia Sars Covid19, alteraciones del orden público, guerra bacteriológica, fuga de gas, accidente, etc.
E.29	**Indisponibilidad Edificios/Instalaciones [E]**	Indisponibilidad de edificios o instalaciones por errores y fallos no autorizados. Puede separarse por edificios o instalaciones clave.

ANEXO III – ADAPTACIÓN DE LAS AMENAZAS DEL CATÁLOGO MAGERIT A ENTORNOS OT

ORIGEN INDUSTRIAL		
I.1	**Fuego**	Incendios: Posibilidad de que el fuego acabe con recursos de los sistemas industriales. Se puede separar esta amenaza por edificios o instalaciones clave.
I.2	**Daños por agua**	Escapes, fugas, inundaciones: posibilidad de que el agua acabe con recursos de los recursos de los sistemas industriales.
I.3	**Contaminación mecánica**	Vibraciones, polvo, suciedad, etc.
I.4	**Contaminación electromagnética**	Interferencias de radio, campos magnéticos, luz ultravioleta, etc.
I.5	**Avería de origen físico o lógico**	Fallos en los equipos y/o fallos en los programas. Puede ser debida a un defecto de origen o sobrevenida durante el funcionamiento de los sistemas industriales. En sistemas de propósito específico, a veces es difícil si el origen del fallo es físico o lógico; pero para las consecuencias que se derivan, esta distinción no suele ser relevante.
I.6	**Corte del suministro eléctrico**	Cese de la alimentación de potencia.
I.7	**Condiciones inadecuadas de temperatura y/o humedad**	Deficiencias en la aclimatación de los locales, excediendo los márgenes de trabajo de los equipos: excesivo calor, excesivo frio, exceso de humedad.
I.8	**Fallo de servicios de comunicaciones**	Cese de la capacidad de transmitir datos de un sitio a otro. Típicamente se debe a la destrucción física de los medios de transporte, detención o simple incapacidad para atender al tráfico presente.
I.9	**Interrupción de otros servicios o suministros esenciales**	Otros servicios o recursos de los que depende la operación de los equipos, por ejemplo, papel para las impresoras, tóner, refrigerante, …
I.10	**Degradación de los soportes de almacenamiento de la información**	Como consecuencia del paso del tiempo o condiciones físicas como temperatura, humedad, presión, etc. Señalar la creciente migración de la información a entornos *cloud* con lo que ello significa respecto a los soportes clásicos.
I.11	**Emanaciones electromagnéticas**	Hecho de poner vía radio datos internos a disposición de terceros. Es una amenaza donde el emisor es víctima pasiva del ataque. Prácticamente todos los dispositivos electrónicos emiten radiaciones al exterior que pudieran ser interceptadas por otros equipos (receptores de radio) derivándose una fuga de información.
I.12	**Indisponibilidad de edificios / Instalaciones (I)**	Indisponibilidad de edificios o instalaciones por accidentes de origen industrial.

ANEXO IV - GLOSARIO DE TÉRMINOS

ACL:	*Access Control List*
ANS:	Acuerdo de Nivel de Servicio
BAD:	*Behavioral analytics and anomaly detection*
BIA:	*Business Impact Analysis*
BYOD:	*Bring Your Own Device*
CISO:	*Chief Information Security Officer*
CSIRT:	*Computer Security Incident Response Team*
CSO:	*Chief Security Officer*
DCS:	*Distributed Control System*
DDOS:	*Distributed Denial of Service*
DLP:	*Data Loss Prevention*
DLT:	*Distributed Ledger Technologies*
DMZ:	*Demilitarized Zone*
DOS:	*Denial of Service*
EDR:	*Endpoint Detection and Response*
ENS:	Esquema Nacional de Seguridad
ERP:	*Enterprise Resource Planning*
FW:	*Firewall*
GDPR:	Reglamento General de Protección de Datos (2016/679)
GRC:	Gobernabilidad, Riesgo y Cumplimiento
HMI:	*Human-Machine Interface*
HW:	Hardware
I+D:	Investigación + Desarrollo
IA:	Inteligencia Artificial
ICS:	*Industrial Control Systems*
IDS:	*Intrusion Detection System*
IEC:	*International Electrotechnical Commission*

ANEXO IV - GLOSARIO DE TÉRMINOS

IoT:	*Internet Of Things*
IP:	*Internet Protocol*
IPS:	*Intrusion Prevention System*
IRM:	*Information Rights Management*
ISA:	*International Society of Automation*
ISO:	*International Organization for Standardization*
IT:	*Information Technology*
LAN:	*Local Area Network*
MES:	*Manufacturing Execution System*
NAC:	*Network Access Control*
NGFW:	*Next-Generation Firewall*
NIS:	*Network and Information Systems*
NIST:	*National Institute of Standards and Technology*
O&M:	*Operation and Maintenance*
OPC UA:	*Open Protocol Communication Unified Architecture*
Orden PCI:	Orden Presidencia Relaciones con las Cortes e Igualdad
OSE:	Operador de Servicio Esencial
OT:	*Operation Technology*
PbD:	*Privacy by Design*
PDS:	Plan Director de Seguridad
PERA:	*Purdue Enterprise Reference Architecture*
PIC:	Protección de Infraestructuras Críticas
PLC:	*Programmable Logic Controller*
PTR:	Plan de Tratamiento del Riesgo
RBAC:	*Role Based Access Control*
RD:	Real Decreto
RTU:	*Remote Terminal Unit*

ANEXO IV - GLOSARIO DE TÉRMINOS

SCADA:	*Supervisor Control and Data Acquisition*
SCI:	Sistema de Control Industrial
SIEM:	*Security Information and Event Management*
SO:	Sistema Operativo
SOAR:	*Security Orchestration, Automation and Response*
SW:	Software
TCP/IP:	*Transmission Control Protocol/Internet Protocol*
TEE:	*Trusted Execution Environment*
TIC:	Las Tecnologías de la Información y las Comunicaciones
TPM:	*Trusted Platform Module*
UE:	Unión Europea
UPnP:	*Universal Plug and Play*
USB:	*Universal Serial Bus*
VHF:	*Very High Frequency*
VLAN:	*Virtual Local Area Network*
VPN:	*Virtual Private Network*
WIFI:	*Wireless Fidelity*
WSUS:	*Windows Server Update Services*

GUÍA SOBRE CONTROLES DE SEGURIDAD EN SISTEMAS OT

isms forum INTERNATIONAL INFORMATION SECURITY COMMUNITY

OCC OFICINA DE COORDINACIÓN DE CIBERSEGURIDAD

GOBIERNO DE ESPAÑA MINISTERIO DEL INTERIOR