UNIVERSIDAD INTERNACIONAL DE LA RIOJA

Universidad Internacional de La Rioja
Máster universitario en Seguridad Informática

NUTRIA: "Una metodología de Ciberseguridad para Pymes en entornos industriales"

Trabajo Fin de Máster

Presentado por: Palafox Pascual, Lorena

Director: Acebrón Antón, José Jesús

Ciudad: Madrid
Fecha: 25 de Julio de 2019

Resumen

Los procesos industriales son operados y supervisados gracias a los **Sistemas de Control Industrial**, dichos sistemas se encuentran expuestos a amenazas que antes no eran contempladas, debido a sus características intrínsecas de dichos sistemas y la nueva era de la Industria 4.0, donde la **interconexión** de los sistemas de control a las redes corporativas forma parte del nuevo entorno industrial.

De este modo, son expuestos nuevos riesgos y vulnerabilidades del sector industrial, que en muchas ocasiones no son analizados, contemplando que las compañías, no cuentan con medidas de ciberseguridad apropiadas, por lo que podrían acarrear serias consecuencias en caso de incidente, en relación a los procesos y finanzas de la empresa, así como daños en el entorno y en el personal de la planta.

Por tanto, la existencia de una metodología para la implementación de controles de ciberseguridad en el entorno industrial, centrado en la Pequeña y Mediana Empresa, que contemple las premisas anteriormente nombradas, resulta de gran utilidad a las compañías de forma que puede servir de guía de **protección** de sus sistemas de operación e información, en todo el ciclo de vida.

Abstract

The industrial processes are operated and supervised thanks to the **Industrial Control Systems,** these systems are exposed to threats that were not previously contemplated, due to their intrinsic characteristics of said systems and the new era of Industry 4.0, where the **interconnection** from control systems to corporate networks is part of the new industrial environment.

In this way, new risks and vulnerabilities of the industrial sector are exposed, which in many cases are not analyzed, considering that the companies do not have appropriate cybersecurity measures, so that they could have serious consequences in case of incident, in relation to the processes and finances of the company, as well as damages in the environment and in the staff of the plant.

Therefore, the existence of a methodology for the implementation of security controls in the industrial environment, centered on the Small and Medium Company, which contemplates the previously mentioned premises, is very useful to companies in a way that can serve as a guide for **protection** of their operation and information systems, throughout the life cycle.

Índice

Índice de tablas

Índice de figuras

1. Introducción

1.1 Justificación

1.1.1 La evolución de la industria y las nuevas técnicas de ataque.

Las técnicas de los atacantes han ido evolucionando con una velocidad mayor que las metodologías de defensa. El Estudio de Referencia de las Capacidades de Seguridad de Cisco 2018 (CISCO, 2018) define la importancia de tener en cuenta la explotación de las debilidades en los dispositivos IoT que permiten obtener acceso a los sistemas de control industrial. De este modo, en la actualidad pocas compañías ven las botnets de la IoT como una amenaza, aunque deberían.

De este modo, los sistemas de control industrial (ICS) son el epicentro de todos aquellos sistemas concernientes a los procesos de fabricación. Los ICS son conectados a diferentes sistemas electrónicos que forman parte del proceso de control, por lo que se implementa una red de dispositivos conectados con alto riesgo de vulnerabilidad, debido a las características de dichos sistemas.

La pequeña y mediana empresa, también denominada PYME, es un objetivo creciente de ciberdelencuencia, teniendo en cuenta la dificultad para proteger los sistemas y datos sensibles y confidenciales es mayor que en empresas más grandes debido a su falta de recursos.

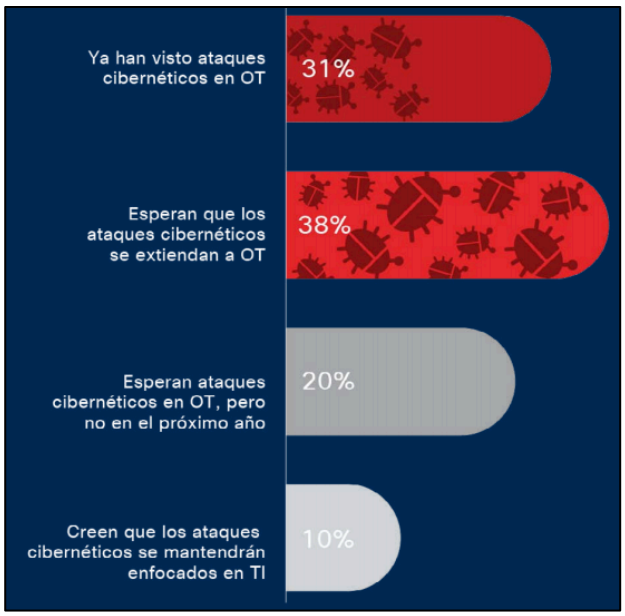

Figura 1.Porcentaje de ataques cibernéticos en la infraestructura de TO. Fuente: *(CISCO, 2018)*

1.1.2 Un nuevo tipo de riesgo: el ciberriesgo.

En relación a la realidad actual de la ciberseguridad en el entorno industrial, se ha de contemplar que la industria cuenta con sectores de muy diferente índole, lo que ocasiona diferencias sustanciales en relación a la definición de ciberseguridad industrial.

Este ámbito abarca desde la distribución de energía, denominada como infraestructura crítica, que ofrece servicios esenciales para el funcionamiento de otras industrias, por lo que su protección se encuentra dentro del marco normativo de la Ley de Protección de Infraestructuras Críticas (PIC, 2011), el principal objetivo de protección se centra en los operadores de dichas infraestructuras, para que proporcionen un apropiado nivel de protección ante amenazas físicas como lógicas mediante tecnologías de cibersguridad TI e industrial.

Por otro lado, el sector de máquina herramienta o automoción, centra su objetivo de protección en un contexto diferente, en el cual la prevención, monitorización y mejora de la resiliencia de los sistemas es la principal funcionalidad a proteger.

De este modo, concretar que la industria actualmente encuentra vulnerabilidades principalmente en dos tipos de amenazas. En primer lugar, el robo o destrucción de información para fines comerciales y/o administrativos, este tipo de amenaza se encuentra relativamente comprendida en las compañías, por lo que existen soluciones avanzadas de protección como antivirus o por medio de herramientas para la prevención de intrusiones.

Por otro lado, el segundo tipo de amenazas centra su punto de ataque en las tecnologías operacionales TO, en relación con los sistemas de control y producción, que cuenta hasta el momento con menor numero de soluciones integrales de ciberseguridad, contando con que gran parte de los sistemas industriales fueron desarrollados hace mas de una década, por lo que se trata de una tecnología obsoleta desde el punto de vista TI, en gran parte de los sistemas del sector industrial.

De este modo, la ciberseguridad en entornos industriales cobra una gran relevancia teniendo en cuenta que, las compañías tienen como objetivo de negocio la optimización de los productos y servicios que ofrecen. Así, la optimización de los servicios se encuentra ligada al cumplimiento de normativa, regulación y estándares relacionadas con la gestión de riesgo.

El cambio hacia la interconexión entre servicios de tecnologías TI, con servicios o/y operaciones de las tecnologías TO, ha crecido a un nivel más elevado que el conocimiento del sector industrial en relación a técnicas, metodologías y/o procedimientos de operación seguros. De este modo, las compañías del sector industrial deben contemplar que la conexión de sus equipos al mundo virtual conlleva un tipo de riesgo diferente a los considerados hasta el momento: el ciberrriesgo. (Ayerbe, 2019).

1.1.3 La relevancia de replantear los parámetros de ciberseguridad.

Las pérdidas que podrían ocasionarse tras un ataque pueden producir un gran daño económico a la empresa, así como daños a la imagen de la compañía, el riesgo financiero comienza a relacionarse con el riesgo cibernético o ciberriesgo. Por tanto, evitar o minimizar los posibles ataques cuenta con un gran valor, teniendo en cuenta su implicación directa en la gestión de la continuidad de servicio para las compañías, la continuidad de negocio e incluso en la supervivencia de la empresa en el sector.

Así, contemplando los diferentes vectores de ataque con los que cuentan las compañías por el momento, cabe mencionar la necesidad de generar una cultura de ciberseguridad, muchos de los ataques sufridos en los sistemas de las compañías, surgen mediante la obtención de información por medio de los usuarios y/o operadores del sistema por medio de técnicas de ingeniería social para obtener unos resultados mas eficientes y con el menor riesgo posible.

Por tanto, contemplando el elevado aumento de demanda de "fabricas inteligentes", el sector industria encuentra una carencia en el mercado laboral de personal con conocimientos de ciberseguridad. Según el resumen ejecutivo de Mcafee (McAfee, 2016):

> *"La escasez mundial de talento cualificado en ciberseguridad agrava la tarea ya difícil de proteger contra el volumen creciente de amenazas avanzadas y sofisticadas. El CSIS (del inglés, Center for Strategic and International Studies, Centro de estudios estratégicos e internacionales) ha realizado un estudio para cuantificar la escasez de profesionales especializados en ciberseguridad en ocho países (Alemania, Australia, Estados Unidos, Francia, Israel, Japón, México y Reino Unido). Se ha encuestado a los responsables de la toma de decisiones (TI), tanto del sector público como del sector privado, en relación a cuatro áreas clave del desarrollo de la plantilla en el ámbito de la ciberseguridad: gasto en seguridad, programas de formación, estrategias del empleador y políticas públicas. El estudio ofrece información de gran utilidad que puede ayudar a las empresas y a los organismos públicos a desarrollar un equipo de trabajo especializado en*

> *ciberseguridad más sólido y sostenible, y que disponga de las competencias necesarias. También incluye varias recomendaciones concretas sobre cómo solucionar el déficit actual de talento en el campo de la ciberseguridad y cómo mejorar la ciberseguridad en su conjunto."*

En consecuencia, se ve la necesidad de profesionales que dominen las técnicas de protección frente ataques y amenazas, así como metodologías y/o estándares para la implementación de técnicas seguras de protección para las empresas.

Según el informe especial de Ciberseguridad de CISCO (CISCO, 2018), la mayoría de la pequeña y mediana empresa reconoce que está generando un entrono de proveedores y productos con mayor complejidad, por lo que le resulta difícil o muy complejo, coordinar las alertas de ciberseguridad producidas en las diversas soluciones que tienen implementadas:

Figura 2. Porcentajes de alertas de seguridad sin investigar o solucionar en PYMES. Fuente: *(CISCO, 2018)*.

Por tanto, es recomendable para el mercado de la pequeña y mediana empresa, con finalidad de implementar mejoras en relación a la ciberseguridad, reconocer el cambio que la Industria 4.0 está generando, teniendo en cuenta que realizar un cambio gradual, es mejor que no realizar ningún cambio.

De este modo, no se contempla la existencia de una solución única y completamente eficaz para combatir los desafíos de ciberseguridad, debido a la complejidad y dinamismo del entorno industrial. La respuesta se centra en la estrategia a implementar, en relación a las tecnologías de ciberseguridad que deben ir evolucionando en la compañía constantemente, a través de impartición de conocimiento y metodologías de implementación segura en función de las necesidades de la empresa.

1.2 Planteamiento del trabajo

La principal arma contra la ciber-delincuencia es la anticipación, mediante la concienciación a la plantilla de la compañía de la importancia de la seguridad en operación, resulta un concepto clave tanto para trabajadores como propietarios ofreciendo así una visión de la realidad a la que se enfrentan para evitar diferentes ataques.

Por otro lado, en relación a la pequeña y mediana empresa, debido al tipo de jerarquización de este tipo de organizaciones, se otorga un elevado número de accesos a la plantilla de la compañía a gran parte de la información y/o sistemas de la compañía, por lo que son más vulnerables.

Así, mediante la elaboración de una metodología de seguridad, consistente en la identificación de los activos más importantes de la compañía, en función de los sistemas a proteger y las características intrínsecas de los mismos, se pretende identificar qué se debe proteger y cuales son los riesgos de no hacerlo.

De este modo, mediante la implementación de medidas proactivas, basadas en la evaluación e identificación de los riesgos particulares de cada compañía, la presente metodología aporta una herramienta para implantar controles de seguridad específicos en función de la necesidad de la empresa, basados en los estándares y normativa vigente actual en relación a la ciberseguridad en entornos industriales.

Por tanto, con la existencia de una metodología de ciberseguridad industrial para PYMES, en castellano, puede resultar de gran utilidad para las compañías del sector, teniendo en cuenta que dicha metodología pueda servir como sistema de protección de sus sistemas de control industrial, todo ello en base a los estándares, guías existentes e iniciativas en desarrollo para la protección de los sistemas de control industrial así como de la seguridad de las Tecnologías de la Información.

1.3 Estructura de la memoria

El trabajo se estructura en los siguientes capítulos:

- **Introducción:** Se expone el panorama relacionado con la ciberseguridad industrial y las PYMES y su problemática.
- **Estado del Arte:** Recoge los conceptos relacionados con las Tecnologías de la Información (TI), así como de las Tecnologías de la Operación (TO), contemplando los ataques sufridos por TO. Además de la situación de la Pequeña y Mediana empresa del sector industrial.
- **Desarrollo específico de la contribución:** Este documento es el resultado de la metodología, consistiendo en un marco integral de gestión, dividido a su vez en 6 partes:
    - Preparación: estado actual, sensibilización y formación.
    - Identificación y análisis de entorno.
    - Defensa y detección.
    - Respuesta.
    - Recuperación.
    - Evaluación continua.
    - Anexo I: Cuestionario de Ciberseguridad Industrial.
- **Conclusiones:** Verificaciones efectuadas y conclusiones extraídas en todo el proceso de elaboración del Trabajo Fin de Master, teniendo en cuenta ideas de trabajo futuro.
- **Términos y acrónimos:** Cuenta con las definiciones de los términos y acrónimos utilizados en el trabajo.
- **Bibliografía / Referencias.**

2. Contexto y estado del arte

2.1 ¿Qué es la Industria 4.0?

La innovadora organización de la metodología de producción, debida a la alta conectividad de los componentes y procesos del nuevo ámbito industrial, hace referencia al término Industria 4.0. Así es como ha sido creada la nueva revolución industrial, acuñada como Cuarta Revolución Industrial. El Centro de Investigación Alemán en Inteligencia Artificial, DFKI en 2011 aporta la siguiente ilustración en la cual se contempla la evolución de la industria desde finales del siglo XVIII hasta la actualidad:

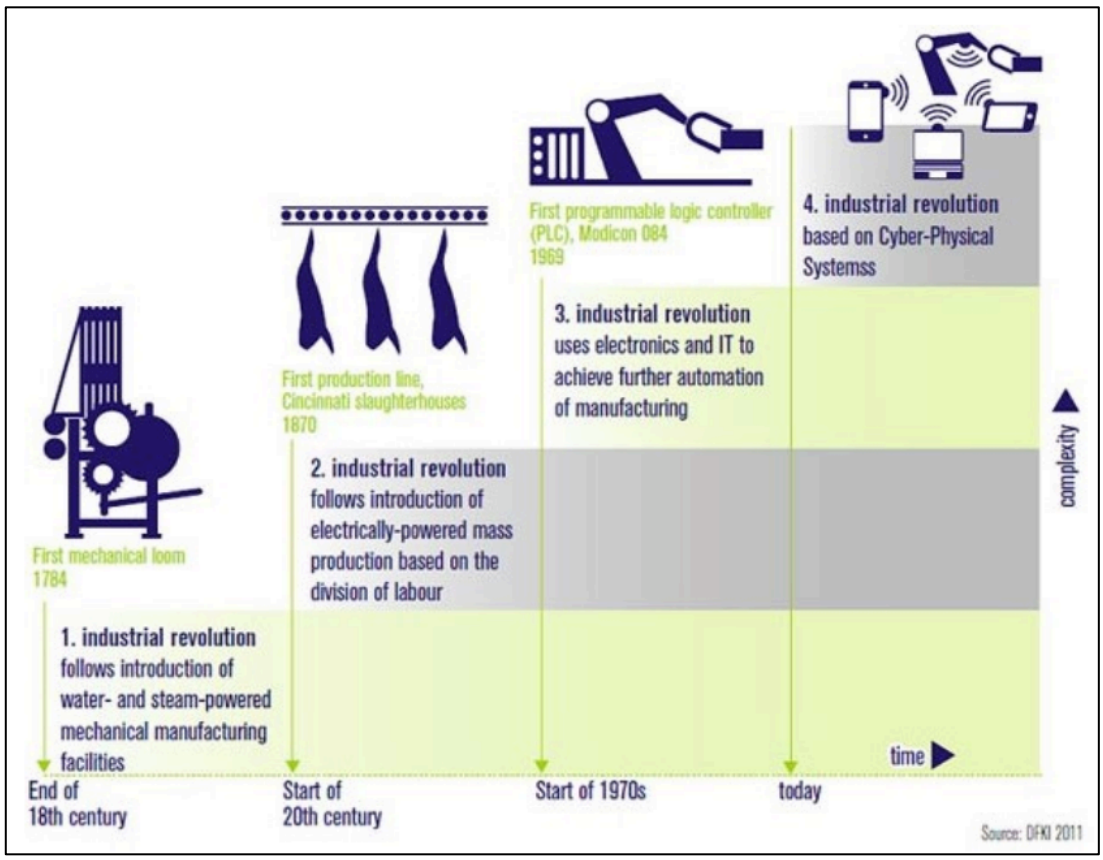

Figura 3. La cuarta revolución industrial, Fuente: *(INCIBE, 2015)*.

Las tecnologías de la operación y su interacción con las tecnologías de la información, comienzan a fusionarse, generando una vinculación entre el mundo virtual y el mundo real, dando paso a los CPS o Cyber-Physical Systems, (Jay Lee, 2015) definidos como aquellos sistemas capaces de administrar sistemas interconectados entre los diferentes activos de la compañía y las funcionalidades de computación, lo que permite una optimización de la disponibilidad en relación a dispositivos como sensores de adquisición de datos.

Tecnologías como Big Data ayudan a que los CPSs desarrollen capacidades de gestión mediante el aprovechamiento de la interconectividad de las máquinas, para alcanzar el objetivo de la Industria 4.0, la implementación de máquinas inteligentes, resilientes y con capacidad autónoma de adaptación a las diferentes circunstancias de producción.

Jay Lee, Behrad Bagher en su artículo (Jay Lee, 2015), define una estructura de CPS, establecida en cinco niveles diferentes, en los cuales se puede comprobar el cambio sufrido en la industria y por consiguiente las nuevas metodologías que han de ser llevadas a cabo por las industrias que cuenten con este tipo de sistemas.

De este modo, un CPS consta principalmente de dos componentes funcionales: la conectividad que garantiza la adquisición de datos relativos al mundo físico en tiempo real y la gestión y análisis de datos mediante la implementación de técnicas relacionadas con las tecnologías de la información.

La **arquitectura 5C** es detallada en la siguiente figura:

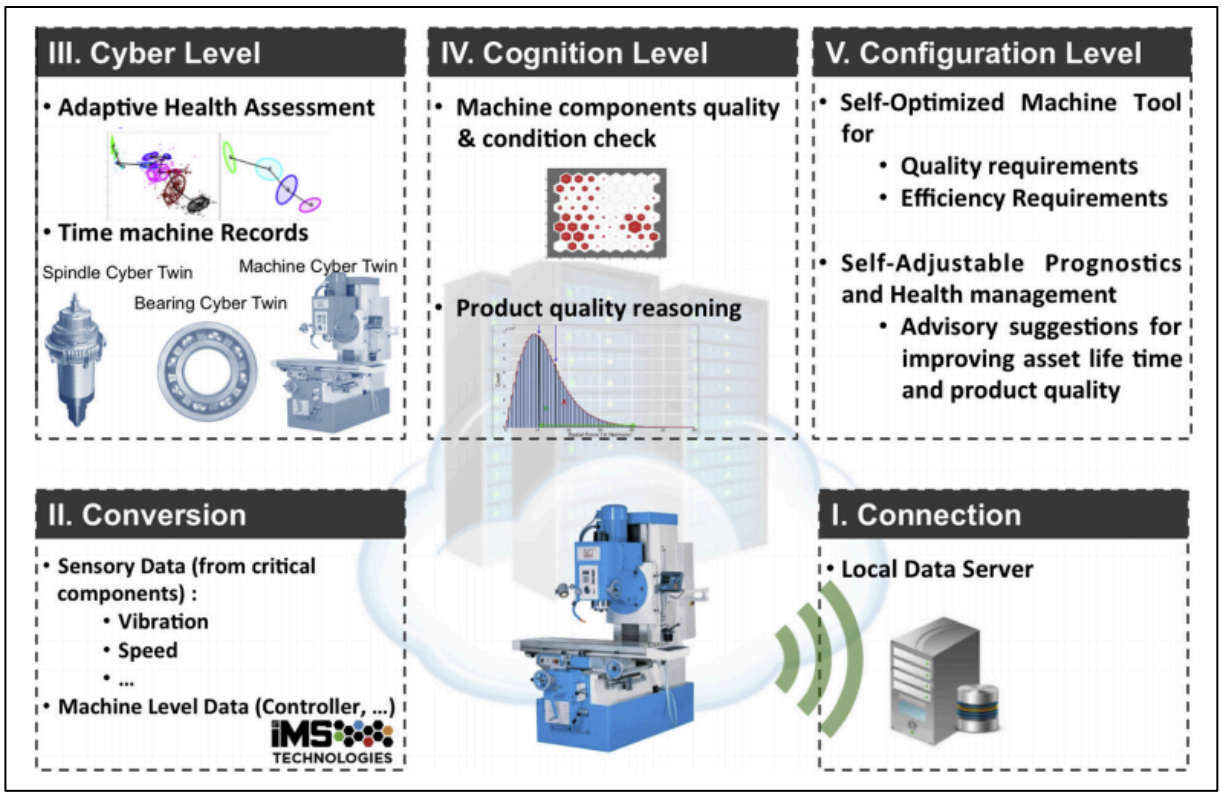

Figura 4. Flujo de datos e información en una fábrica con arquitectura 5C CPS. Fuente: *(Jay Lee, 2015)*

De este modo, dicha arquitectura define 5 niveles (Jay Lee, 2015) diferentes:

- **Nivel de Conexión:** Este nivel trata de la adquisición de datos precisos y fiables de las máquinas y sus componentes, los datos pueden ser medidos por medio de sensores, sistemas de control o herramientas empresariales como ERP, MES, SCM y CMM. En este nivel se debe tener en cuenta que son gestionados diferentes tipos de datos por lo que la transferencia de datos al servidor central debe realizarse bajo un método seguro y libre de fisuras.

- **Nivel de Conversión entre datos e información:** Dicha conversión hace referencia a la información significativa que debe ser deducida de los datos, mediante algoritmos específicamente creados para el pronostico de valores que permiten estimar la vida útil de diferentes funcionalidades.

- **Nivel cibernético:** Actúa como plataforma central de información de la arquitectura 5C, la información es dirigida hasta este nivel desde todas las máquinas conectadas para formar la red de máquinas, proveyendo una mejora en la visión sobre el estado de las máquinas individuales además de capacidad de auto-comparación.

- **Nivel de Conocimiento:** La implementación de un CPS en este nivel genera un conocimiento profundo del sistema monitorizado. Por medio de usuarios expertos, con conocimientos adquiridos se aporta apoyo para la toma de decisiones, mediante la información comparativa y de los estados de las máquinas, se toman las decisiones sobre las prioridades para la optimización de los procesos.

- **Nivel de Configuración:** En este nivel, a través de la información recibida los equipos actúan como sistemas de control resilientes para aplicar acciones correctivas a los incidentes encontrados, así como decisiones preventivas.

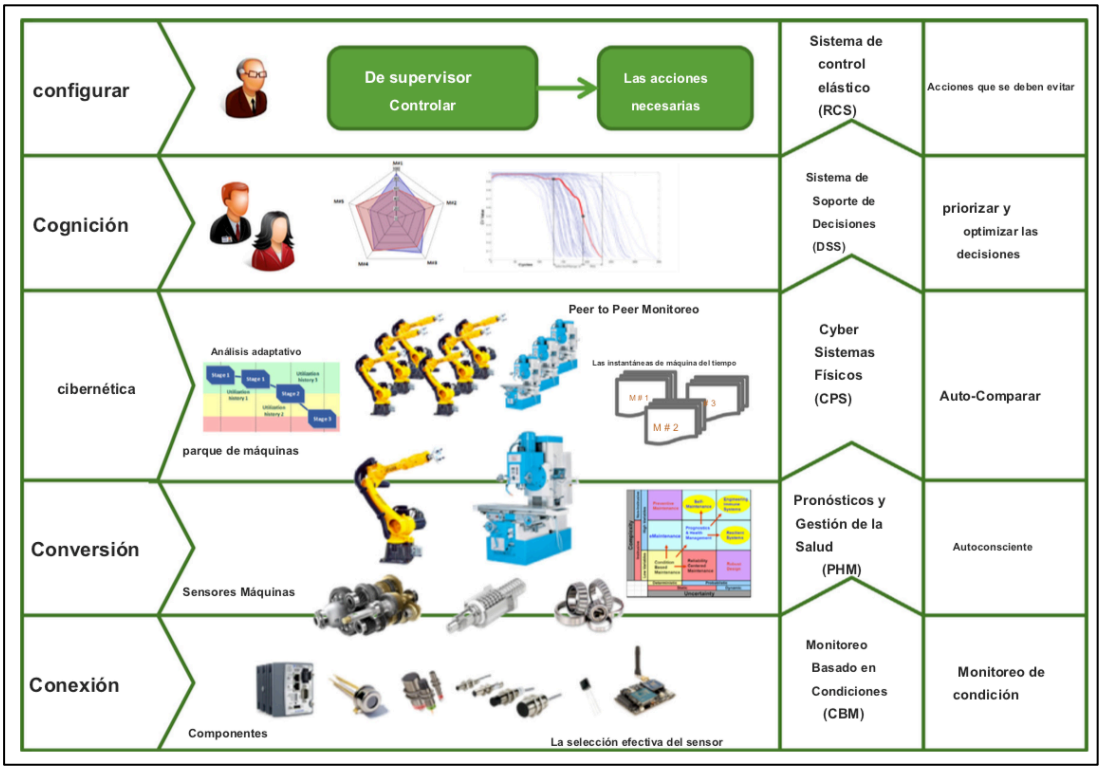

Figura 5. Técnicas asociadas a cada nivel de la arquitectura 5C, Fuente: *(Jay Lee, 2015)*.

La digitalización de los procesos productivos o la denominada Industria 4.0, implica un **cambio cultural** que contempla una elevada transformación dentro de las compañías del sector. De este modo, en entorno industrial debe adaptarse a una profunda **transformación estructural** en diferentes niveles empresariales, teniendo en cuenta la interconexión con nuevos entornos y plataformas conectadas.

Según datos del **Centro de Ciberseguridad Industrial (CCI)**, España es el quinto país de mundo con más equipos que controlan procesos e instalaciones industriales por medio de conexión a Internet, publicado en el artículo de Diego Caldentey para la revista UNIRrevista de la Universidad Internacional de La Rioja, (Caldentey, 2019). Así, con la llegada de las fábricas inteligentes, las compañías del ámbito industrial contemplan nuevas amenazas, que hasta el momento no suponían un problema debido a la inexistencia de interconexión entre los mundos TI y TO.

Uno de los principales desafíos que encuentra la industria, es la **falta de personal especializado**, que tenga conocimientos sobres las técnicas de protección frente a ataques en las diferentes redes, software, sistemas operativos y bases de datos de las compañías del sector industrial.

De este modo, es necesario crear una restructuración en los parámetros de ciberseguridad mediante la incorporación de la seguridad informática en los procesos tecnológicos de

producción, así como en los llamados CPS o Cyber-Physical Systems, (Marcelo Guato Burgos, 2019).

Por otro lado, se ha de tener en cuenta la protección de **la confidencialidad** de la información, cualidad que, según la estructuración de las empresas relacionadas con el ámbito industrial, anterior a la llamada Cuarta Revolución Industrial, carecía de interés, teniendo en cuenta las características de producción con redes aisladas de las redes de gestión empresarial, que hasta el momento habían sido utilizadas.

De este modo, la ciberseguridad aplicada en la Industria 4.0 debe proteger la integridad de las comunicaciones y la adquisición de datos, en las diferentes etapas de los procesos de producción, asegurando los datos confidenciales relacionados a dichos procesos productivos.

La protección de **la propiedad intelectual** de la nueva industria inteligente, basa su idea en la prevención de diferentes ataques, tanto externos, como internos a través de medidas de protección desde diferentes niveles, tanto a nivel de gestión de la planta como a nivel de campo, implementando diferentes sistemas para control de acceso y control de la información que es compartida entre los diferentes niveles jerárquicos a nivel empresarial.

Nuevas funcionalidades embebidas son llevadas a cabo, esta nueva metodología de operación permite la incorporación de nuevas medidas para capacitar a los dispositivos de una interactuación a nivel de proceso sin riesgos, lo que permite asegurar la accesibilidad e integridad mediante diferentes métodos de autenticación y cifrado.

La nueva tendencia tecnológica se caracteriza por ofrecer las siguientes **ventajas**, según (MAPFRE, 2019):

- Capacidad de adaptación a la demanda en tiempo real. De esta manera, se evita el excedente de stock.
- Transformación de los entornos de trabajo y las fábricas en general, la finalidad es optimizar la productividad.
- Servicio al cliente más cercano y profesional, mediante nuevos servicios conectados.
- Análisis de la información obtenida, datos relevantes sobre usuarios, que permite mejorar la calidad en la fabricación de productos, con una mayor adaptación a los gustos y preferencias de los clientes finales.
- Auge de la inteligencia artificial, extrapolada a cualquier maquinaria industrial.

De este modo, se observa los beneficios que porta la industria a cualquier sector, también existen nuevos riegos con los que anteriormente no se contaba, teniendo en cuenta que en la industria conectada, prácticamente cualquier proceso de producción está informatizado, por lo que, aumenta la exposición al malware. Por esta razón, cobra un valor importante tomar medidas para combatir el cibercrimen, y así, salvaguardar los datos sensibles de la compañía.

Por tanto, teniendo en cuenta los diversos cambios que introduce la Industria 4.0 a nivel de gestión, tanto como de proceso, es necesario el establecimiento de protocolos de seguridad, para llevar a cabo esta tarea el primer paso trata de realizar una evaluación del estado actual de la compañía a evaluar. De este modo, es posible realizar un análisis de los posibles riesgos y amenazas a la que esta sujeta actualmente, así como diferentes vulnerabilidades conforme a la normativa vigente.

2.2 ¿Por qué es necesaria la ciberseguridad en la Industria 4.0?

Así, la nueva industria aporta una serie de ventajas hacia la producción como la posibilidad de evitar el excedente de stock gracias a la adaptación a la demanda que genera el mercado en tiempo real.

La profunda transformación de los entornos de producción, no solo optimiza los procesos, también establece una atención al cliente de una manera más cercana y profesional, gracias al análisis de la información, lo que permite la adquisición de una elevada cantidad de datos relevantes sobre los usuarios y por consiguiente una optimización en a la fabricación de los productos con una adaptación a las características que busca el usuario final.

De este modo, contemplando los beneficios con los que cuenta la industria conectada, también cuenta con riesgos relacionados con la seguridad de sus activos. Así, la informatización de los procesos conlleva una exposición inevitable a ataques informáticos en forma de malware.

Independientemente del tamaño de la empresa, dicha exposición conlleva un peligro en la viabilidad de la compañía. Así, es necesario salvaguardar la información relevante y/o confidencial mediante medidas de seguridad cuyo objetivo principal ha de centrarse en combatir el cibercrimen, (MAPFRE, 2019). La carencia de información y conocimiento con la que cuentan las empresas, desafortunadamente hace que las medidas implementadas sean insuficientes, incluso inexistente. Por lo que se contempla la necesidad de potenciar la ciberseguridad en entornos TO, a través de diferentes metodologías o practicas a seguir.

Así, se deben contemplar metodologías para la gestión de la ciberseguridad en sistemas de control industrial, contemplando los riesgos asociados a la materialización de ciberamenzas

con elevado impacto en los sistemas, obligando al desarrollo de metodologías o estándares particularizados como herramienta para la gestión eficiente, continua y alineada con las necesidades de las compañías, así como de los proveedores de servicios relacionados. La disponibilidad, integridad y confidencialidad deben ser salvaguardadas.

El Centro de Ciberseguridad Industrial, propone el siguiente diagrama de capas para determinar las relaciones existentes entre los componentes de alcance y los elementos auxiliares de los sistemas a proteger, (CCI, 2014):

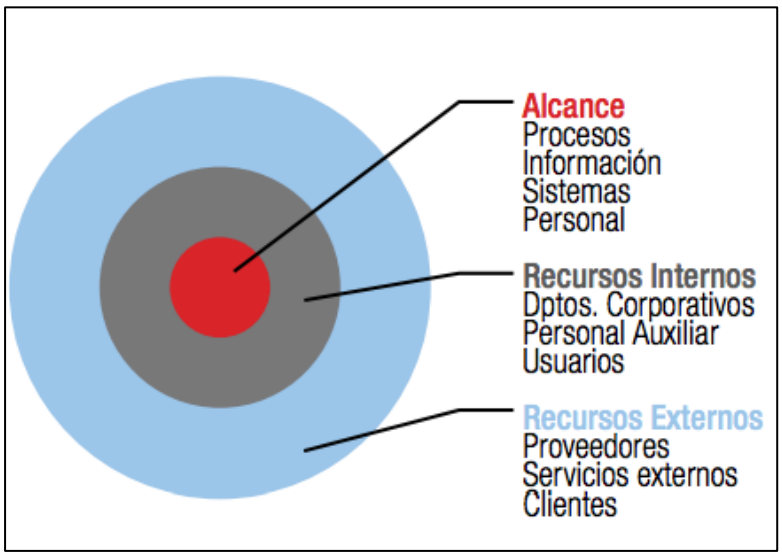

Figura 6. Ejemplo de diagrama de capas para protección de sistemas industriales. Fuente: *(CCI, 2014)*.

De entre las mejoras, que están incorporando los fabricantes industriales en relación a la normativa de obligado cumplimiento o recomendaciones de buenas prácticas en el ámbito de la ciberseguridad industrial, INCIBE en su publicación (INCIBE, 2018):

- **Comunicaciones**: Uso de certificados para cifrar las comunicaciones entre cliente y servidor. Soporte para las versiones seguras de protocolos industriales y otros, que son utilizados por los dispositivos, como DNP3 secure, WirelessHART, Zigbee, OPC UA, SNMP v3, etc.

- **Sistema Operativo**: Uso de guías de bastionado para realizar configuraciones seguras en los servicios y procesos que se ejecutan dentro del sistema. Parametrización de sistemas operativos a medida para evitar la ejecución de servicios o procesos innecesarios que aumenten la superficie de exposición del dispositivo. Uso de listas blancas de procesos para evitar la ejecución de posibles archivos maliciosos o la creación de subprocesos de procesos no controlados de forma correcta.

- **Hardware:** Soporte para almacenamiento externo (tarjetas SD), donde se almacena información del dispositivo, con un tipo especial de formato que sólo se puede leer desde el dispositivo o desde un software específico proporcionado por el fabricante. Incorporación de mecanismos para evitar la manipulación de los dispositivos. En este caso, algunos fabricantes han optado por mecanismos conocidos como antitampering, para evitar aperturas y que un atacante pueda llegar a hacer modificaciones en placas, o la resina epoxy para evitar lecturas directas de señales en los pines de un chip.

- **Aplicaciones:** Desarrollo de aplicaciones utilizando guías de buenas prácticas para evitar ataques y errores básicos, como desbordamientos de búfer, inyecciones de diferentes tipos, etc Incorporación de un sistema de gestión de roles (RBAC) que permita tener un control de los permisos que posea cada usuario dependiendo del rol asignado dentro de la aplicación. Creación de un registro de actividad de seguridad (log) para tener unas trazas a analizar en el caso de sufrir ataques o detectar comportamientos anómalos por parte del dispositivo afectado.

2.3 Diferencias entre Sistemas TI y sistemas TO

INCIBE en su publicación (INCIBE, 2015), realiza una comparativa entre el mundo de las Tecnologías de la información contra las Tecnologías de la Operación. De este modo, se presenta un estudio a cerca de los nexos de unión entre ambas así como las características intrínsecas de cada una.

La independencia entre el ámbito TI (Tecnologías de la Información) y TO (Tecnologías de la Operación) quedaban claramente diferenciadas en base a la tecnología que utilizaban, por un lado el sector TI se trata de un entorno de oficina, en el cual se contempla un número elevado de activos a proteger, teniendo en cuenta la confidencialidad, característica primordial a proteger en este ámbito.

Sin embargo, la tecnología predominante en el mundo TO trataba únicamente de dispositivos relacionados con el entorno industrial, sensores, controladores, actuadores, incluso registradores que en ningún momento obtenían acceso a las redes de gestión de la compañía.

La llamada “Cuarta Revolución Industrial” o “Industria 4.0”, cambia por completo las diferencias que anteriormente se observaban entre los mundos TI y TO, con la introducción

de las tecnologías digitales en las fábricas, es decir, la transformación digital aplicada a la producción industrial.

De este modo, con el nuevo punto de vista introducido por el concepto de la digitalización de los procesos, gran parte de las compañías "puramente industriales" buscan resistir el cambio producido por la introducción de sistemas de información en el ámbito industrial.

Las compañías independientemente del nivel de producción con el que cuenten, que no quieran participar en el cambio de gestión a nivel de procesos, a futuro, cuentan con la posibilidad de encontrarse con situaciones incomodas y con dificultad de resolución, teniendo en cuenta que el concepto que introduce la "Industria 4.0" es de una fuente de alta competitividad, reduciendo el coste de mano de obra, mejorando la producción adaptándose al elevado nivel de demanda que acarrea el consumidor actual, mejorar la relación con el cliente aportando nuevos servicios para la optimización de la compañía. Además de sacar partido a la información con la que cuenta para realizar análisis y explotación de la misma.

En este contexto, la convergencia entre estos dos mundos que interconectan diferentes entornos de producción plantea nuevos retos relacionados con la ciberseguridad en la "Industria 4.0". Así, sistemas que tradicionalmente no contaban con la problemática de vulnerabilidades de los sistemas de la información, comienzan a ver comprometida la seguridad de sus activos. Además de la situación de un entorno con cada vez mas amenazas de distinta naturaleza.

De este modo, se observa que el diseño llevado a cabo por diferentes compañías del ámbito industrial no estaba realizado para contar con redes de información e interconexión con redes externas a través de internet o diferentes dispositivos inalámbricos. Además, el control remoto por parte de los suministradores, la obsolescencia de sistemas operativos crea un escenario de crecientes amenazas de ciberseguridad en el entorno industrial, cobrando mayor envergadura en las infraestructuras críticas.

Por consecuencia, toda aquella compañía que quiera formar parte de la "Cuarta Revolución Industrial" debe implementar un sistema o metodología de transformación de su modelo de negocio mediante la resolución de las vulnerabilidades del ámbito TO y por tanto, iniciar un proceso de fusión con el ámbito TI corporativo, contemplando la necesidad de establecer protección mediante políticas de ciberseguridad guiadas en la misma línea que el plan de inversión y acción de las compañías del sector.

Así, cobra una gran importancia para el mundo TO considerar como la convergencia entre ambos mundos genera una nueva posición en la cual, un ataque puede generar grandes pérdidas económicas, de salud y productividad.

Según, Marcos Fernández Martín, Director en Altran Business Consulting, en su artículo (Martín, 2016), la experiencia ganada a lo largo de años de gestión TI, puede ser aplicada a los sistemas de soporte de operaciones, si bien existen ligeras diferencias

	IT	OT
Entorno	▪ Mutifuncional, condiciones favorables. ▪ Se prima la rapidez y se puede permitir el reinicio. Recambios entre 2 y 5 años	▪ Limitación de funciones, condiciones desfavorables. ▪ Se prima la fiabilidad, integridad y cero paradas. Recambios entre 10 y 20 años
Compatibilidad	▪ Selección de equipos por funcionalidad. Rápida adaptabilidad	▪ Dependencia de terceros. Acondicionamiento en el proceso con pruebas de estrés e imprevistos
Seguridad	▪ Concepto maduro, tanto para acceso físico como electrónico	▪ Aplicabilidad de conocimientos de IT en un entorno distinto. Vulnerabilidades
Homogeneización	▪ Funcionalidades claras y concretas. Equipamiento homogéneo	▪ Variabilidad de entornos y elementos. Distinción de equipamiento de múltiples marcas y funciones
Comunicaciones	▪ Tecnología IP, protocolos de acceso, gestión estándar de puertos	▪ Protocolos de procesos, variabilidad de tipología de tecnologías (serie, IP, buses de control, etc.)

Figura 7. Diferencias tecnológicas entre TI y TO, Fuente: (Martín, 2016).

2.4 Ciberserguridad industrial en la Pequeña y Mediana empresa (PYME)

El sector industrial está sufriendo una transformación de entorno, los procesos de fabricación incorporan cada vez más elementos tecnológicos versátiles, esta transformación reflejada en avances tecnológicos, ha de ir acompañada de una optimización de las medidas de seguridad para evitar accidentes.

Partiendo de esta premisa, surge una pregunta, ¿Cómo puede la Pequeña y Mediana Empresa hacer frente a los nuevos incidentes de seguridad que surgen en el entorno de interconexión entre la Tecnología de la Información y la Tecnología de Operación?

Cada vez cobra una mayor normalidad que los operarios interactúen con máquinas a través de HMI (Human Machine Interface), pantallas táctiles o visualización de procesos por medio de dispositivos conectados a internet con acceso a la red exterior. La trasformación digital forma parte de las pymes industriales del mismo modo que ha afectado a aquellas que no se encuentran dentro del ámbito de industria.

Aspectos como la atención a cliente, reclutamiento de personal, innovación tecnológica son claves para el establecimiento de avances tecnológicos en las empresas. De este modo, cobra una mayor importancia como la trasformación digital afecta a las actividades propias del

sector industrial como son el proceso de diseño, fabricación y logística, es decir, fases del ciclo de vida de producto desde que se fabrica hasta que se transporta.

Así, las pymes encuentran por un lado nuevas oportunidades de negocio, teniendo en cuenta la optimización de la producción que se obtiene de la implementación de nuevos avances tecnológicos a la vez que muchos y nuevos retos a los que hacer frente. Por un lado, el sector industrial tiene que adaptar su metodología de trabajo a procesos, productos y modelos de negocio, todo ello acompañado del establecimiento de la máxima prioridad para la ciberseguridad, contemplando que los ataques a sistemas industriales pueden ocasionar daños de carácter financiero, produciendo perdidas en las finanzas, afectar a la innovación, reducir la producción, incluso ocasionar víctimas.

La pequeña y mediana empresa, las compañías del sector que cuentan con años de experiencia en la producción comienza a entrar en la industria conectada, muchas de ellas considerando que no corren riesgos debido a su tamaño. La carencia de un interés especial en invertir económicamente en aspectos relacionados con la ciberseguridad de este tipo de compañía, hace necesaria una concienciación y formación de seguridad, más extensa, ya que datos de CISCO establecen que el 53% (CISCO, 2018) de los ataques en 2017, fueron realizados a PYMES, teniendo en cuenta que tienen puntos de acceso penetrables fácilmente en comparación a las grandes empresas, que ya cuentan con medidas de ciberseguridad establecidas.

2.4.1 ¿Por qué es importante la ciberseguridad en las PYMES?

La situación financiera en la que pueden encontrase las PYMES, en contraposición con la gran empresa, difiere en números, siendo la PYME aquella que obtiene unos beneficios menores en comparación. Por tanto, sufrir un ataque que ocasione pérdidas muy elevadas o la producción durante un periodo largo, podría suponer la no recuperación de dicha compañía, podría ocasionar el cierre por no poder volver a la situación de normalidad en la que se encontraban antes de sufrir un ataque.

Debido a estas circunstancias, que la PYME obtenga características resilientes ,en relación a la ciberseguridad, controles y medidas para que en caso de ataque en los sistemas, tenga la capacidad para volver al estado de estabilidad inicial, da un elevado aporte de valor a la empresa, además de seguridad en el uso de las nuevas tecnologías, por lo que podrá optimizar el rendimiento de la producción con una protección mas elevada de sus activos.

La híper-conectividad introducida en los procesos, gracias a la Industria 4.0, representa una oportunidad para la pyme industrial, sin embargo, dicha oportunidad debe ir sincronizada con controles de ciberseguridad, para garantizar la continuidad de negocio.

La pequeña y mediana empresa sufre incidentes de seguridad cibernética, la principal problemática de dichos incidentes, es el coste de los mismos y por consecuencia, para las empresas de menor tamaño, acarrea un problema mayor, debido a su nivel económico.

Los ciber-delincuentes aprovechan una gran variedad de ataques cibernéticos sofisticados, que cuentan con una alta velocidad y potencial capaz de paralizar a la pequeña y mediana empresa. Para abordar de un modo efectivo las necesidades de los clientes, los socios de las compañías deben comprender cuales son las modernas amenazas que aplican en la actualidad a sus activos.

De este modo, se identifican diferentes amenazas centradas en el ámbito de la pequeña y mediana empresa para que sean conocidos los riesgos a los que están expuestos:

- **Crecimiento continuo en el desarrollo de amenazas:** En la actualidad los ciberdelincuentes continúan enfocándose en métodos de ataques efectivos, asequibles y escalables mediante la implementación de variantes de malware demostrando la experimentación continua y la expansión del conocimiento que van adquiriendo.

- **La nueva amenaza IoT y móvil:** Conforme crece la transformación digital gran cantidad de dispositivos móviles, IoT y BYOD son introducidos en las infraestructuras de red. Del mismo modo que permiten a las PYMES satisfacer la demanda de sus clientes, a menos de estar bien protegidos, abren una cantidad de vectores de amenaza a los ciberdelincuentes. Además, otros dispositivos como cámaras, impresoras, enrutadores que son utilizados como redes de bots permiten expandirse rápidamente a través de las redes.

Los desafíos de ciberseguridad que encuentran las PYMES van cambiando a medida que los ciberdelincuentes modelan sus capacidades de ataque, observando a la pequeña y mediana empresa como un objetivo fácil, asequible teniendo en cuenta la oposición que este tipo de empresa encuentra a invertir en seguridad. De este modo, los directivos de las compañías deben entender, los desafíos con los que deben lidiar si son partidarios del crecimiento hacia la transformación digital.

La brecha de habilidades de seguridad cibernética es una realidad actualmente, la escasez de conocimiento afecta a compañías de todos los tamaños, especialmente a las PYMEs que usualmente carecen de recursos para la implementación de un control de seguridad en equipos y redes que disponen.

Muchas PYMEs confían en soluciones de productos legados o soluciones puntuales para controlar la amenaza, sin contemplar la realización de un análisis exhaustivo el entorno en el que se encuentran. Además, otro de los inconvenientes encontrados por la pequeña y mediana empresa, se trata de la falta de tiempo que tienen debido a su volumen de producción, por lo que no se llega a establecer una metodología de seguridad sólida de redes aisladas, dando facilidades a los delincuentes para evitar los controles básicos implementados y, por consiguiente, el acceso a su red.

La creencia sobre que el riesgo de ataque es proporcional al tamaño de la empresa, pone en peligro a las PYMEs, dado que la inversión en formación adecuada para la lucha contra las amenazas cibernéticas es menor. Sin embargo, según el informe de investigación de violación de datos de Verizon, 2018 (Verizon, 2018), determina que el 58 por ciento de las víctimas de ataque de malware, son clasificadas como PYMEs. De este modo, se contemplan muchos ataques relacionados con errores humanos como phishing u otras técnicas de ingeniería social.

2.5 Amenazas en la Tecnología de la Operación, TO

Tras el estudio de la problemática de la ciberseguridad en las PYMES industriales, son mostrados algunos ejemplos de ataques a las Tecnologías de la Operación que han tenido lugar a lo largo de la historia:

2.5.1 Stuxnet

En Junio de 2010, es descubierto en la central nuclear de Natanz, Irán el primer gusano capaz de espiar y reprogramar sistemas industriales. La firma de seguridad cibernética Symantec explica en su dossier (Symantec Security Response, 2011). la probabilidad de que la entrada en el sistema, fuera realizada por medio de una memoria USB infectada.

De este modo, únicamente, mediante la inserción física de la memoria en un ordenador conectado a la red, el gusano se propago a través del sistema informático y así, una vez que se hallaba dentro de la red, su misión era encontrar el software encargado del control de las centrifugadoras.

La misión principal de dichas centrifugadoras, constaba en la separación de componentes para la obtención final de uranio 235 o uranio enriquecido, sustancia fundamental para la generación de energía nuclear. Así, Stuxnet consiguió implementar una reprogramación de las centrifugadoras, tomando el gobierno de las máquinas.

El gusano, centró su estrategia en dos vectores diferentes de ataque, por un lado, elevó la velocidad de las centrifugadoras en intervalos de tiempo, e incrementando el periodo en el cual la velocidad aumenta, es decir, una primera fase aumentó la velocidad durante 15 minutos antes de volver a la velocidad de operación normal, pasado un mes disminuyó la velocidad durante 50 minutos, esta técnica fue utilizada durante meses.

Finalmente, las velocidades elevadas produjeron con el paso del tiempo un nivel de tensión en las centrifugadoras que las llevó a la desintegración, cerca de un 20 % de las máquinas fueron siniestradas durante el ataque del gusano Stuxnet.

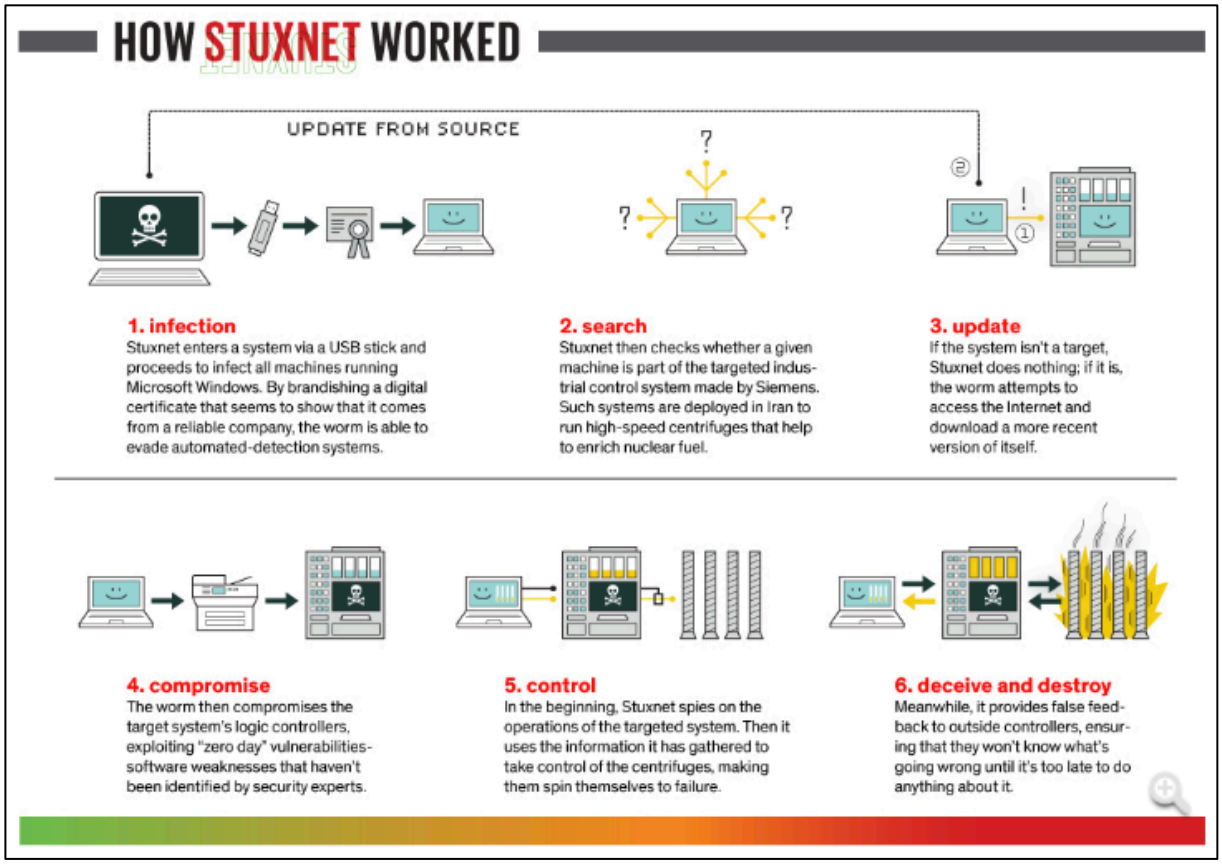

Figura 8. Cómo funciona el gusano STUXNET. Fuente: *(Kushner, 2013)*

2.5.2 Havex

Este malware trata de un troyano de acceso remoto, su descubrimiento en 2013 vislumbro que formaba parte de una estrategia de espionaje hacia los sistemas de control industrial (ICS).

El Instituto SANS en su artículo sobre el impacto del malware de Dragonfly en sistemas de control industrial (Nelson, 2016), data el comienzo de este troyano en 2010, quedando implementado en el sistema, por medio de tres fases diferenciadas.

En primer lugar, los atacantes realizaron una concienzuda estrategia de phising, mediante la cual se obtuvo información sobre los objetivos a atacar.

Por otro lado, otro de los vectores de ataque a la hora de obtener información fue llevado a cabo por medio del ataque "watering hole attack", cuya metodología de trabajo se centra en campañas de ataques dirigidos a webs de confianza, que son visitadas por empleados de la compañía, una vez el usuario se encuentra dentro de la página infectada, estos son re direccionados a servidores en los que se encontraba el software infectado por el troyano Havex.

Así, una vez Havex se encontraba dentro del sistema, por medio de los trabajadores de la compañía, éste aprovechando el estándar Open Platform Communications (OPC), encargado de gestionar la comunicación en el control y supervisión de procesos industriales, que permite interactuar y compartir datos mediante una interfaz común, utilizó DCOM, Modelo de Objetos de Componentes Distribuidos para establecer la conexión con los servidores OPC que se encontraban dentro de las redes ICS y así, obtener información relacionada con el nombre del servidor, ID, estado de los procesos que estaban siendo ejecutados y diversa información de los dispositivos de control SCADA o ICS que se encontraban en la red.

De este modo, en este caso, el troyano Havex no buscaba destruir el sistema como Stuxnet sino un hurto de información, con la principal misión del espionaje, dado que obtener la información sobre el funcionamiento de este tipo de dispositivos, ayuda al diseño y desarrollo de novedosos ataques contra entornos industriales específicos.

2.5.3 Black Energy

INCIBE en su publicación (INCIBE, 2016) describe las consecuencias de BlackEnergy, definido como crimeware, es decir, un software diseñado para la realización de delitos financieros en entornos de línea.

Este troyano ha comprometido la seguridad de distribuidoras eléctricas ucranianas, hasta los sistemas informáticos del aeropuerto de Kiev, con misión principal de implantar el caos el sistema aéreo, cadenas de televisión y medios de comunicación. BlackEnergy cuenta con una evolución desde su primera aparición en 2007 hasta convertirse en una amenaza Persistente Avanzada (APT Advanced Persistent Threat).

Así, la misión principal de BlackEnergy, trata de realizar ataques DoS, espionaje y destrucción de información mediante, la técnica de phising, incluyendo documentos Excel cuyas macros, están infectadas para acceder al objetivo de ataque, tras realizar la descarga de dicho documento, aparece un cuadro de diálogo mediante el cual se sugiere activar las macros para observar el contenido. Una vez abierto, es activado la infección ocasionada por el malware BlackEnergy.

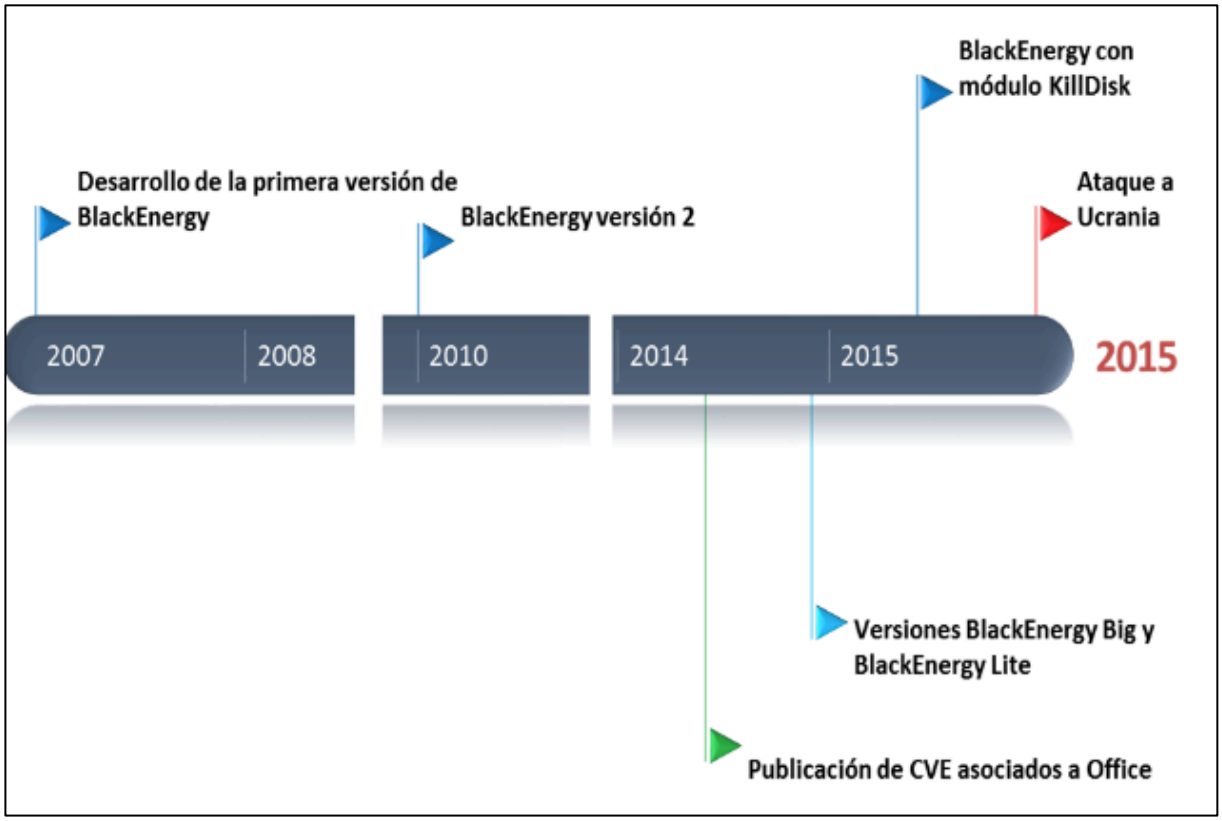

Figura 9. Evolución de BlackEnergy. Fuente: *(INCIBE, 2016)*.

2.5.4 PLC Blaster

El articulo (Ralf Spenneberg, 2016) realizado por investigadores de seguridad de Black Hat, Estados Unidos de América, definen el gusano PLC Blaster como un malware centrado en buscar debilidades de los sistemas de control industrial, de manera que, se propaga de forma autónoma por los PLC que se encuentran en la red a la que ha accedido.

El diseño principal fue implementado para los dispositivos PLC SIMATIC S7-1200 de Siemens, aunque hay que tener en cuenta que este tipo de gusano es un peligro potencial para cualquier red industrial teniendo en cuenta que se trata de un tipo de nueva amenaza con la que tradicionalmente las compañías de control industrial no contaban, contemplando el aislamiento con el que contaban hacia el exterior de la red.

De este modo, un ataque realizado mediante este tipo de malware es capaz de administrar la información a la que tiene acceso y ser la puerta de entrada para diferentes ataques, permitiendo el acceso remoto los PLC conectados a la red pública, manipulación de los componentes que dependen de las órdenes recibidas a través de la consola de administración.

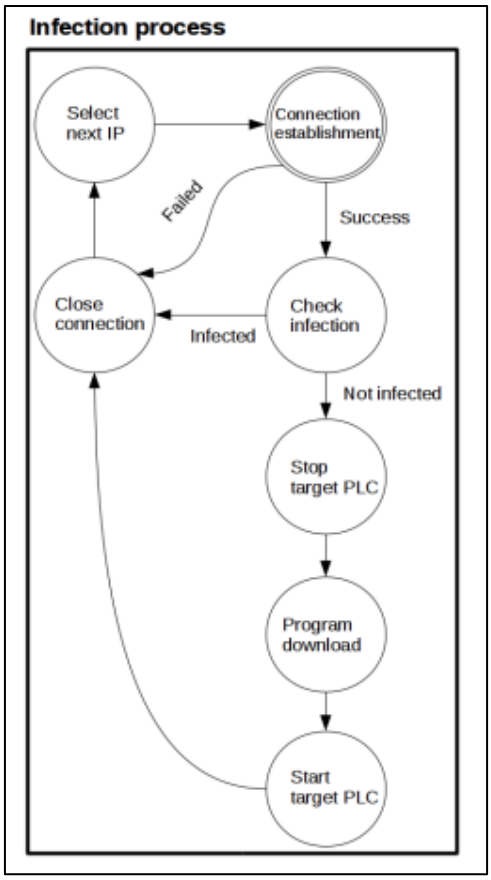

Figura 10. Secuencia de ejecución del gusano. Fuente: *(Ralf Spenneberg, 2016)*.

Maik Bruggemann, desarrollador de software e ingeniero de seguridad en OpenSource Security cita en el artículo (Ralf Spenneberg, 2016) la importancia de tener en cuenta, que no se trata de problemas específicos de la compañía Siemens, sino que actualmente el control industrial debe contemplar posibles ataques de este tipo:

> *"Estos no son problemas específicos de Siemens. Todas estas empresas de control industrial han estado haciendo las cosas de la misma manera durante los últimos 30 años. Necesitan desarrollar nuevas actitudes hacia la seguridad para hacer que los dispositivos sean seguros ",* (Ralf Spenneberg, 2016).

2.5.5 Tritón

Tritón, se trata de un malware de código malicioso, capaz de desactivar los sistemas de seguridad diseñados para prevenir accidentes industriales catastróficos. Fue descubierto en una planta petroquímica en Arabia Saudita en 2017, su método de operación se basa en obtener el control de los sistemas instrumentados de seguridad de planta, es decir, controlar los sistemas que se encuentran en la última línea de defensa contra desastres que amenazan a la vida humana dentro de las industrias.

Los sistemas instrumentados de seguridad, son activados en caso de detección de condiciones peligrosas, su misión trata de devolver los procesos que están siendo ejecutados a niveles seguros o desactivar dichos procesos activando elementos como válvulas de cierre o mecanismos de liberación de presión.

Tritón consiguió tomar el control de estos sistemas instrumentados de seguridad de forma remota, las consecuencias podrían haber sido catastróficas teniendo en cuenta que, mediante la intrusión en el sistema, cabía la posibilidad de llevar a cabo la des-habilitación o manipulación del software para ocasionar el mal funcionamiento de equipos. Afortunadamente, el código malicioso que los atacantes habían implementado contenía un error, por lo que dejaron pistas sobre su identidad y se pudo reconocer a los atacantes.

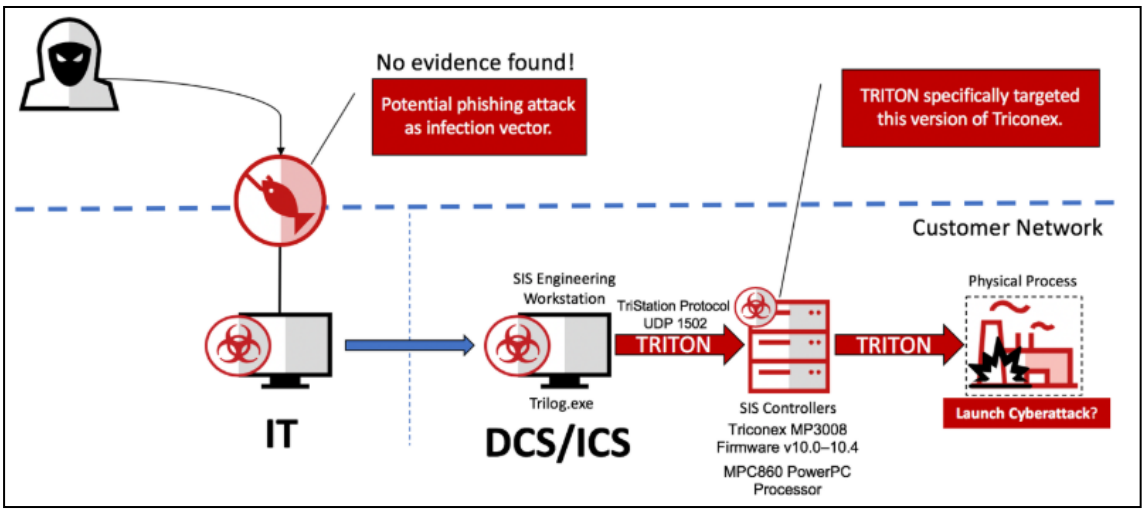

Figura 11. Funcionamiento de Tritón. Fuente: *(Roccia, 2018)*.

2.6 Iniciativas de protección de sistemas de control industrial, TO.

A continuación, son definidas algunas de las iniciativas de protección de sistemas industrial a nivel internacional y nacional:

2.6.1 ENISA – Protecting Industrial Control Systems

La Agencia Europea de Ciberseguridad ENISA (ENISA, 2019), cuenta con 15 años de experiencia contribuyendo a la ayuda en implementación de políticas de seguridad, desde su fundación en 2004.

El organismo trabaja en colaboración con los estados miembros de la Unión Europea y el sector privado para brindar asesoramiento y soluciones, así como mejora de las capacidades de las empresas involucradas. De entre el soporte que brinda se incluyen entre otras funcionalidades:

- Ejercicios paneuropeos de ciberseguridad.
- Desarrollo y evaluación de las Estrategias Nacionales de Ciberseguridad.
- Cooperación y desarrollo de capacidades de CSIRT.
- Estudios sobre IoT e infraestructuras inteligentes, en relación a la protección de datos, metodologías para mejorar la privacidad e identificación de amenazas cibernéticas.
- Apoyo al desarrollo e implementación de la directiva NIS (Europea, 2013), así como ayuda al establecimiento de políticas de divulgación de vulnerabilidades de forma voluntaria.

Desde 2019, a raíz de la entrada en vigor de la Ley de Ciberseguridad (Reglamento 2019/881), ENISA tiene la tarea de realizar los esquemas de certificación de ciberseguridad europeos, como base para la certificación de productos, procesos y servicios.

ENISA publicó en 2011, unas recomendaciones para la protección de los sistemas de control industrial para los estados miembros de la Unión Europea (ENISA, 2011), dichas recomendaciones son las siguientes:

- **Recomendación 1**: Implementación de estrategias de seguridad ICS pan-europeas y nacionales.
- **Recomendación 2**: Generación de guías de buenas prácticas para seguridad ICS.

- **Recomendación 3**: Plantillas de seguridad ICS.

- **Recomendación 4**: Concienciación y la formación

- **Recomendación 5**: Creación de un banco de pruebas común, o alternativamente, un marco de certificación de seguridad ICS.

- **Recomendación 6**: Capacidad de respuesta de emergencia nacionales sobre ICS-informática.

- **Recomendación 7**: Investigación en seguridad ICS haciendo uso de los programas de investigación existentes.

2.6.2 ISA/IEC- 62443

A comienzos del siglo XXI, da comienzo el desarrollo de las normas ISA99 como un aporte de conocimiento para la seguridad en los sistemas de control industrial, implementando nuevos documentos para ayudar al incremento de la protección de los sistemas industriales frente ataques informáticos.

De este modo, fueron establecidos diferentes grupos de trabajo encargados de diferentes partes de un conjunto de normas de seguridad industrial. Así, de entre los aspectos con mayor relevancia de estas publicaciones, el establecimiento de zonas y conductos , cuenta con elevada importancia desde la perspectiva de la seguridad, teniendo ene cuenta que la agrupación de activos y la comunicación mediante caminos conocidos facilita la protección de los sistemas de control e información.

En el año 2010, la numeración de la ISA 99 para a denominarse ANSI/ISA-62443 con motivo de la alineación de los documentos con la nomenclatura de la IEC, generando otros 4 documentos, un informe técnico a 8 documentos y 5 informes técnicos.

De este modo, la norma IEC 62443 se compone de los siguientes documentos (INCIBE, 2015):

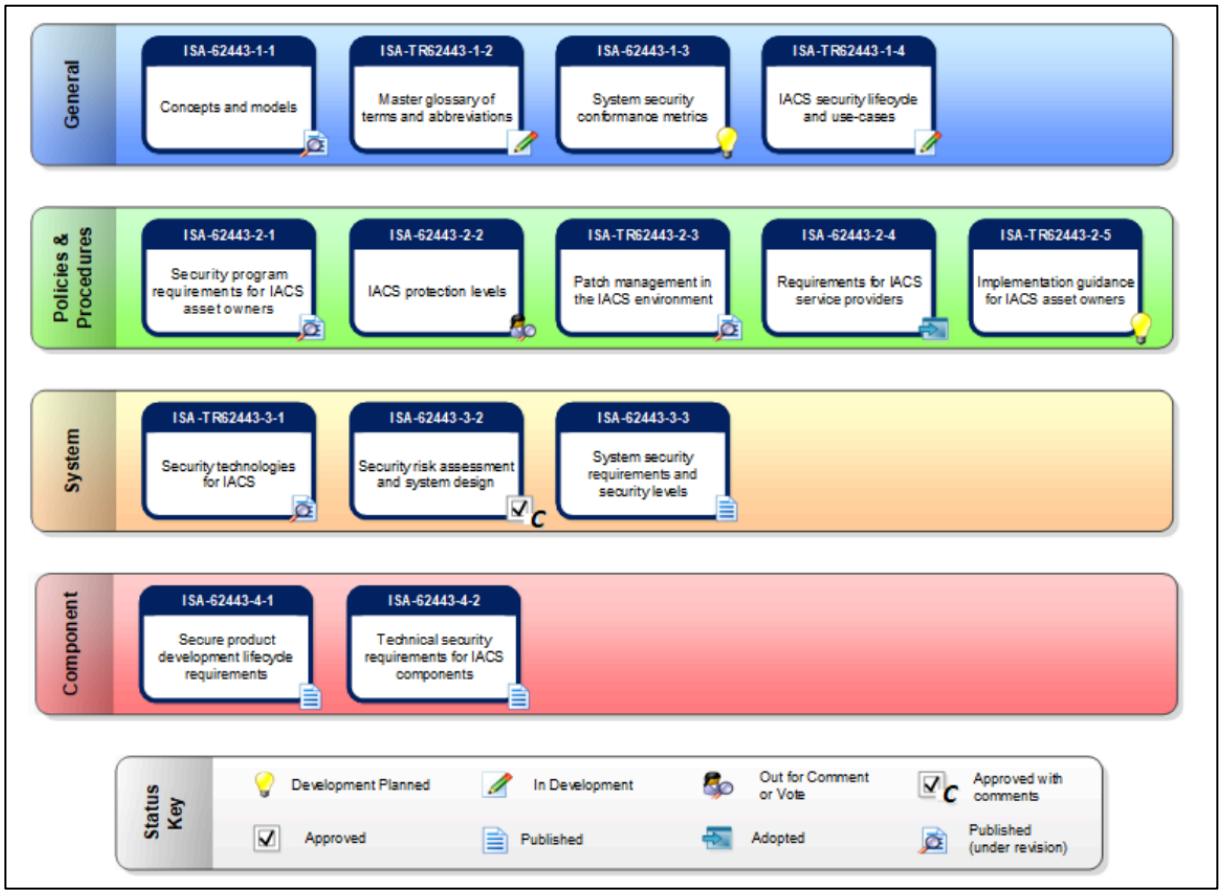

Figura 12. Norma IEC 62443. Fuente: *(ISA, 2019)*

- **IEC 62443-1-1 "Models and Concepts":** Se corresponde con el primero publicado dentro de la ISA99, aunque se ha revisado para que quede alineado con el resto de documentos que forman ahora la serie IEC 62443.
- **IEC TR 62443-1-2 "Master Glossary of Terms and Abbreviations":** Recoge el glosario de términos y las abreviaturas usadas en la serie.
- **IEC 62443-1-3 "System Security Compliance Metrics":** Define las métricas de cumplimiento para la seguridad en los sistemas de control y automatización industrial.
- **IEC TR 62443-1-4 "Security Life Cycle and Use Cases":** Se centra en el ciclo de vida y en dar ejemplos de uso para aplicaciones típicas dentro de los sistemas de control.
- **IEC 62443-2-1 "Requirements for an IACS Security Management System":** Recoge la información ya publicada por la ISA99 en el segundo documento (ANSI/ISA 99.02.01-2009).

- **IEC TR62443-2-2 "Operating a Control Systems Security Program":** Aborda la operación eficiente de un programa de ciberseguridad en sistemas de control industrial.
- **IEC TR 62443-2-3 "Patch Management in the IACS Environment":** Guía práctica para llevar a cabo un programa de gestión de actualizaciones, desde el punto de vista tanto del propietario como del proveedor de soluciones.
- **IEC 62443-2-4 "Certification of IACS supplier security policies and practices":** Se centra en la certificación de proveedores de productos de seguridad para los sistemas de control y automatización industrial.
- **IEC TR62443-3-1 "Security Technologies for IACS":** Es una actualización del publicado dentro de la ISA 99 "ANSI/ISA-TR99.01.02-2007" y ofrece una descripción de tecnologías existentes para la protección de redes y sistemas industriales, exponiendo sus ventajas y limitaciones.
- **IEC 62443-3-2 "Security Risk Assessment and System Design":** Describe los conceptos de security zone y conduit introducidos en la ISA99. Además, indica cómo se debe llevar a cabo la segmentación siguiendo estos principios. Únicamente plantea una segmentación teórica, la segmentación real se trata en el documento IEC 62443-4-2.
- **IEC 62443-3-3 "System Security Requirements and Security Levels":** Describe los requisitos técnicos del sistema para definir el nivel de seguridad del activo analizado.
- **IEC 62443-4-1 "Product Development Requirements":** Define el proceso de desarrollo que tienen que llevar a cabo los nuevos dispositivos que se creen para los sistemas de control, aunque también puede ser aplicado a los dispositivos ya existentes.
- **IEC 62443-4-2 "Technical Security Requirements for IACS Components":** Esta parte de la serie IEC 62443 agrupa los requisitos técnicos para mejorar la seguridad de los componentes, de forma individual, dentro de la red industrial. También se aborda la segmentación de la red para restringir los flujos de datos dentro de la red y entre redes.

2.6.3 NIST SP800-82

El Instituto Nacional de Estándares y Tecnología, NIST por sus siglas en inglés National Institute of Standars and Technology, trata de una agencia de Administración de Tecnologías del Departamento de Comercio de los Estados Unidos.

El principal objetivo de este instituto, se centra en promover la innovación y la competencia en la industria mediante avances legislativos, tecnológicos y metrológicos que optimicen la estabilidad económica y ciclo de vida de las compañías del sector industrial.

De este modo, de entre sus diversas publicaciones se encuentra el documento *SP800-82 Guide to Industrial Control Systems (ICS) Security - Supervisory Control and Data Acquisition (SCADA) systems, Distributed Control Systems (DCS), and other control system configurations such as Programmable Logic Controllers (PLC)* (NIST, 2015), dicho documento trata de una guía de establecimiento de sistemas ICS seguros, mediante la estrategia de defensa en profundidad por medio del establecimiento de controles de seguridad apropiados.

Así, la guía SP800-82, trata de los siguientes asuntos en materia de ciberseguridad industrial:

- **Sección 3**: Diferencias entre sistemas TO y TI, amenazas, vulnerabilidades e incidencias.

- **Sección 4**: Desarrollo y puesta en marcha de un programa de seguridad de TO para mitigar el riesgo de las vulnerabilidades identificadas en la Sección 3.

- **Sección 5**: Recomendaciones para la implementación de la seguridad en arquitecturas de red típicamente encontradas en ICS, así como segregación de redes.

- **Sección 6**: Controles identificados y orientación inicial sobre la aplicación de dichos controles de seguridad TO.

2.6.4 Centro de Ciberseguridad Industrial

Junio de 2013, comienza la iniciativa española con motivo de impulsar y mejora la ciberseguridad industrial en España y Latinoamérica, con el Centro de Ciberseguridad Industrial (CCI, 2019).

De este modo, el centro desarrolla actividades relacionadas con el análisis, estudios, guías e información relacionada con las diferentes prácticas, tecnologías y operaciones dentro el ámbito de la ciberseguridad industrial.

Así, se trata del primer centro que nace desde la industria, sin ser subvencionado y sin ánimo de lucro, centrados en impulsar la ciberseguridad industrial como *"el conjunto de prácticas, procesos, tecnologías, diseñadas para gestionar el riesgo del ciberespacio derivado del uso, procesamiento, almacenamiento y transmisión de información utilizada en las*

organizaciones e infraestructuras industriales, utilizando las perspectivas de personas, procesos y tecnologías" (CCI, 2019).

De este modo, los objetivos principales del Centro de Ciberseguridad Industrial (CCI, 2019) son los siguientes:

- **Aglutinar a los principales actores y expertos** implicados en la Ciberseguridad Industrial con objeto de que colaboren, intercambien experiencias y conozcan los últimos avances y desarrollos en esta materia.

- **Proporcionar un Ciber-Estado de Situación**, prestando especial atención a la evolución de las ciberamenazas y las nuevas formas de ataque.

- **Establecer canales de interlocución con autoridades y reguladores**, para facilitar la comunicación entre los diferentes actores involucrados en la Ciberseguridad Industrial (administración, organizaciones industriales e infraestructuras críticas, ingenierías e integradores, fabricantes, consultoras, asociaciones, organismos de estandarización y buenas prácticas y los ciudadanos).

- **Mejorar la concienciación de todos los actores mencionados mediante cursos, eventos, seminarios, publicaciones y la presencia en los medios de comunicación.**

- **Cualificar a profesionales en Ciberseguridad Industrial** con el fin de facilitar a las empresas su contratación

- **Fomentar la dinamización y difusión del mercado español** de la Ciberseguridad Industrial

2.7 Iniciativas de protección de la información, TI.

Tras la definición de las iniciativas de protección de los sistemas industriales, se define el principal estándar de para la seguridad TI, contemplando la interconexión existente con el área TO.

El conjunto de estándares y guías de seguridad ISO/IEC 27000, cuenta con las mejores prácticas para el ámbito de los Sistemas de Información, en relación al desarrollo, implementación y mantenimiento de los Sistemas de Gestión de la Seguridad de la Información. Se trata de una norma con capacidad de certificación para las compañías que cumplan los controles establecidos en la serie de estándares.

De este modo, la serie cuenta, entre otros con los siguientes documentos:

- ISO/IEC 27000. Vocabulario y términos relacionados con el SGSI.
- ISO/IEC 27001. Norma que contiene los requisitos de implantación de un SGSI, certificable.
- ISO/IEC 27002. Código de buenas prácticas en forma de controles para la gestión de la SI.
- ISO/IEC 27007. Guía de auditoría de un SGSI.
- ISO/IEC 27799:2008. Guía de implementación de ISO 27002 en la industria de la salud.
- ISO/IEC 27035:2011. Gestión de incidentes de seguridad.

De este modo, haciendo un mayor hincapié en la norma ISO 27001, se trata de una norma internacional que describe como realizar la gestión de la seguridad de la información en una compañía. Así, puede ser implementada en cualquier tipo de organización, privada o publica, pequeña o grande.

El objetivo de la norma es la protección de la confidencialidad, integridad y disponibilidad dentro de las compañías, mediante la investigación de los potenciales problemas, que pueden afectar a la información ,por medio de la evaluación de riesgos inicial, para posteriormente, introducir controles para la mitigación o tratamiento de los problemas que pueden llegar a producirse.

3. Objetivos concretos y metodología de trabajo

3.1 Objetivo general

El objetivo general del presente trabajo queda centrado en el desarrollo de una metodología, cuyo enfoque práctico trate de manera integral la implementación de un sistema de gestión de ciberseguridad industrial. De modo, que aporte cobertura a las compañías involucradas en el sector, obteniendo una metodología mediante la cual, sean capaces de proteger sus activos, por medio de la implantación de controles y recomendaciones, basadas en la actual legislación, y buenas practicas del sector industrial.

Así, mediante la realización de dicho estudio se pretende ofrecer una ayuda a las compañías del sector industrial, generando un documento en castellano, que sintetice la actual información referente a la protección de los sistemas de control industrial e implemente nuevas buenas prácticas a seguir conforme a lo establecido en la actual normativa vigente.

Por otro lado, con la presente metodología se pretende formar parte de la creación de una cultura de ciberseguridad en los entornos industriales, enfocado en la pequeña y mediana empresa, de forma que, el personal implicado en el diseño, desarrollo, implantación, adquisición y operación, cuenten con el conocimiento necesario, para actuar en caso de incidente.

A través del presente estudio, se propone como determinar el riesgo para así, medir y analizar cuales son los eventos que podrían afectar a los sistemas que se desean proteger. Además, de ayudar a la identificación de las posibles vulnerabilidades y amenazas, para determinar cuales son los puntos débiles de los sistemas a proteger, y cómo podría afectar al funcionamiento de los procesos de negocio.

Se ofrece una diferenciación entre las características que componen los sistemas de información corporativa, contra los entornos industrializados, contemplando diferencias entre los protocolos de comunicación, tolerancia a retardos, frecuencia de actualización y parcheo, integridad de los mensajes, sistemas operativos entre otras funcionalidades.

Así, la presente metodología pretende impulsar y contribuir a la mejora de la Ciberseguridad en el entorno industrial, mediante el análisis de diferentes buenas prácticas, estándares y guías, implementando una metodología para ayudar a la gestión del riesgo relacionado con la ciberseguridad industrial, contemplando el procesamiento, transmisión de datos y almacenamientos que son utilizados en las compañías del entorno industrial.

3.2 Objetivos específicos

De este modo, los objetivos específicos de la metodología son los siguientes:

- Explorar la problemática actual de los sistemas de control industrial, en relación a la protección de sus activos, amenazas y vulnerabilidades, así como el estado actual internacional de las indicativas de protección de sistemas de control industrial.

- Desarrollar guías en castellano, teniendo en cuenta que la mayoría de la documentación a consultar se encuentra en inglés, por lo que servirá de ayuda al sector nacional, para llevar a cabo un sistema de protección de sus activos.

- Establecer una metodología que abarque el ciclo de vida completo de los sistemas de control, teniendo en cuenta que la mayor premisa a proteger en este ámbito, se trata de la disponibilidad, por lo que un ciclo de vida seguro es de vital importancia.

- Sintetizar un enfoque hacia procesos, teniendo en cuenta, los diferentes elementos que participan en la actividad del sistema de gestión de ciberseguridad industrial y el encadenamiento de procesos.

- Establecer unas directrices para la implementación de técnicas de ciberseguridad industrial para la Pequeña y Mediana Empresa, con misión de evitar pérdidas económicas incalculables, así como pérdida de reputación y por tanto, confianza de los clientes en caso de incidente.

- Sintetizar el concepto de aplicación dentro de una organización industrial, mediante la diferenciación entre la ciberseguridad de la red corporativa (red TI) y la ciberseguridad de la red de operación (red TO).

- Analizar las prioridades de las empresas para definir a que riesgos se enfrentan, cuales son los factores internos y externos que impactan en los sistemas a proteger, así como la estrategia y/o medidas a implementar.

3.3 Metodología del trabajo

Para alcanzar los objetivos anteriormente nombrados, el presente trabajo queda fundamentado en cuatro fases diferenciadas:

- **Investigación:** En esta etapa se procede a la recopilación de información relacionada con los sistemas de control industrial, estándares, guías y buenas prácticas de ciberseguridad en entornos industriales.

  Por otro lado, es analizado el contexto actual, en relación a las amenazas y vulnerabilidades de este tipo de sistema, extrayendo el conocimiento sobre la información relevante para la elaboración de la memoria.

- **Adaptación de la información recopilada:** Una vez se ha seleccionado la información para la elaboración de la metodología, se procede a la traducción, modificación de redacción, anexión de contenido de otros artículos y/o documentación concerniente al trabajo para la alineación de la información existente.

- **Identificación de necesidades:** En esta etapa se lleva a cabo el reconocimiento de los aspectos mejorables o sin definir por las fuentes consultadas en el estado del arte actual, en relación a la aplicación de medidas de ciberseguridad industrial en la pequeña y mediana empresa.

- **Propuesta de metodología como nueva solución:** En la última etapa, se propone una metodología de trabajo basada en estándares, normas y buenas practicas, tratando de actualizar las medidas existentes al contexto de las PYMES, inter-conexionando controles y técnicas existentes, para tratar de mejorar o contemplar las carencias encontradas.

El proceso completo de realización de la presente metodología está basado en la documentación publicada en relación al ámbito del trabajo, por medio de diferentes medios y formatos, además del conocimiento de expertos en la materia, mediante la presentación de la metodología para la obtención de sugerencias, cambios y consejos en la realización del trabajo.

4. Desarrollo específico de la contribución

4.1 Identificación del problema a tratar

- Operación de las empresas (pequeña y mediana empresa) con cada vez mayor dependencia de los sistemas y equipos que son vulnerables a incidentes de seguridad.

- Impacto en el negocio de un incidente.

- Capacidad de respuesta ante un incidente o ataque contra la ciberseguridad de la empresa.

- Identificación de las características de la empresa en función de las dos grandes categorías relacionadas con sistemas y equipos: Tecnología de la Información (IT) y Tecnología de Operación (OT).

- Evaluación de riesgos en función de las amenazas y vulnerabilidades con las que cuenta la compañía, así como las acciones correctivas o mitigadoras para una futura incidencia de ciberseguridad.

- Consecuencias de un incidente en función de la compañía.

- Evaluación del diseño, defensa en profundidad.

4.2 Descripción de la metodología

NUTRIA, trata de una nueva metodología de ciberseguridad para PYMES en entornos industriales, contemplando como la transformación digital afecta a la protección de sus activos, así como a la disponibilidad de operación. De este modo, los avances tecnológicos dentro del entrono industrial suponen elevados retos, así como nuevas oportunidades.

Con la presente metodología, se pretende establecer un modelo para la adaptación de los procesos, productos y modelos de negocio con los que cuentan las compañías dedicadas al sector industria mediante un nuevo modelo industrial de ciberseguridad.

De este modo, además de implementar un nuevo modelo de protección para la pequeña y mediana empresa, se pretende garantizar la continuidad de negocio, teniendo en cuenta que con la adopción de nuevas técnicas las empresas industriales son expuestas a nuevos riesgos, por lo que la hiperconectividad debe estar sincronizada con la adopción o mejora de planes o

metodologías de ciberseguridad que incorporen las nuevas tecnologías que son adaptadas a las compañías.

Así, NUTRIA se encuentra inspirada en el marco de ciberseguridad de NIST (NIST, 2018), es decir, en el conjunto de actividades para obtener resultados específicos de seguridad mediante ejemplos para orientar la obtención del éxito en la implementación. Así, el marco de ciberseguridad NIST define cinco funciones de seguridad para la obtención de una cultura de ciberseguridad capaz de abordar el riesgo dinámico de seguridad, las cinco funciones son las siguientes:

- **Identificar:** Desarrollar una comprensión organizacional para administrar el riesgo de seguridad cibernética para sistemas, personas, activos, datos y capacidades.
- **Proteger:** Desarrollar e implementar medidas de seguridad adecuadas para garantizar la entrega de servicios críticos.
- **Detectar:** Desarrollar e implementar actividades apropiadas para identificar la ocurrencia de un evento de seguridad cibernética
- **Responder:** Desarrollar e implementar actividades apropiadas para tomar medidas con respecto a un incidente detectado de seguridad cibernética.
- **Recuperar:** Desarrollar e implementar actividades apropiadas para mantener los planes de resiliencia y restablecer cualquier capacidad o servicio que se haya visto afectado debido a un incidente de seguridad cibernética.

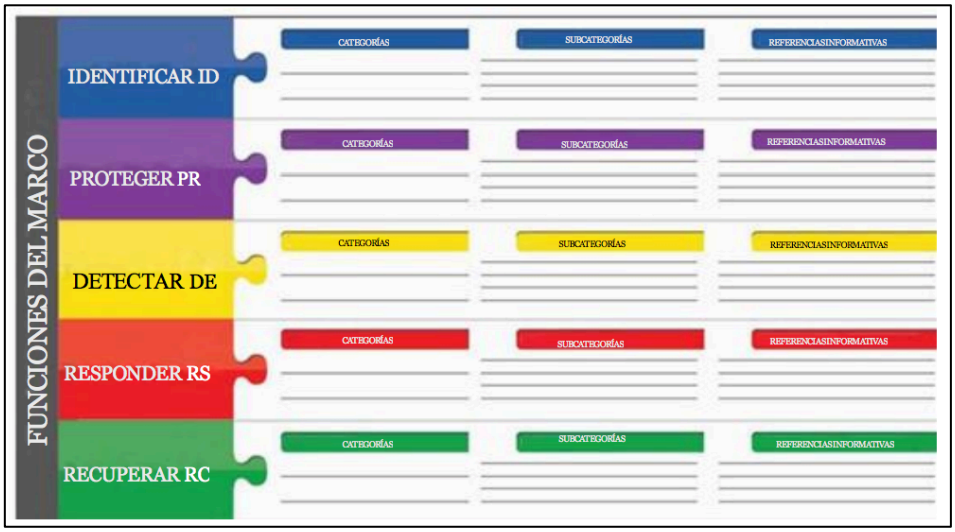

Figura 13. Funciones del marco de cibersguridad NIST, Fuente: *(NIST, 2018)*.

De este modo, la metodología NUTRIA se inspira en el marco de ciberseguridad NIST, aportando una adaptación de las fases a la pequeña y mediana industria, teniendo en cuenta

que el marco de ciberseguridad NIST centra su implementación en las infraestructuras críticas.

El origen de las fases de NUTRIA, ha sido establecido en función de las características de las compañías del sector, mediante la alineación de estándares, buenas prácticas y normas bajo un escenario de implementación particular, la pequeña y mediana empresa.

La metodología cuenta con seis fases diferenciadas:

- Fase I: Preparación
- Fase II: Identificación y análisis
- Fase III: Defensa y detección
- Fase IV: Respuesta
- Fase V: Recuperación
- Fase VI: Evaluación continua

De este modo, se puede observar que la metodología NUTRIA cuenta con una fase más de las que propone el marco de ciberseguridad NIST. La división es debida a la diferenciación, entre una primera fase de toma de contacto con la situación actual de la compañía, tarea desarrollada en la **Fase I: Preparación**, y el análisis e identificación del problema a tratar en base a la información obtenida anteriormente, dicha tarea es llevada a cabo en la **Fase II: Identificación y análisis.**

Por otro lado, la **Fase III: Defensa y detección**, centra su ámbito de aplicación en protección de la gestión de la ciberseguridad industrial. La **Fase IV: Respuesta**, teniendo en cuenta la importancia de la vuelta a operación de cualquier empresa del sector, está centrada en los procesos de obtención de copias de seguridad en los sistemas.

La resiliencia es el factor mas importante en la implementación de la **Fase V: Recuperación** para finalmente cerrar el circulo de la metodología con la **Fase VI: Mejora continua**, para cerciorarse que los controles implementados, se encuentran actualizados, revisados e implementados apropiadamente periódicamente.

A continuación, se muestran las fases de la metodología NUTRIA o Nueva Industria:

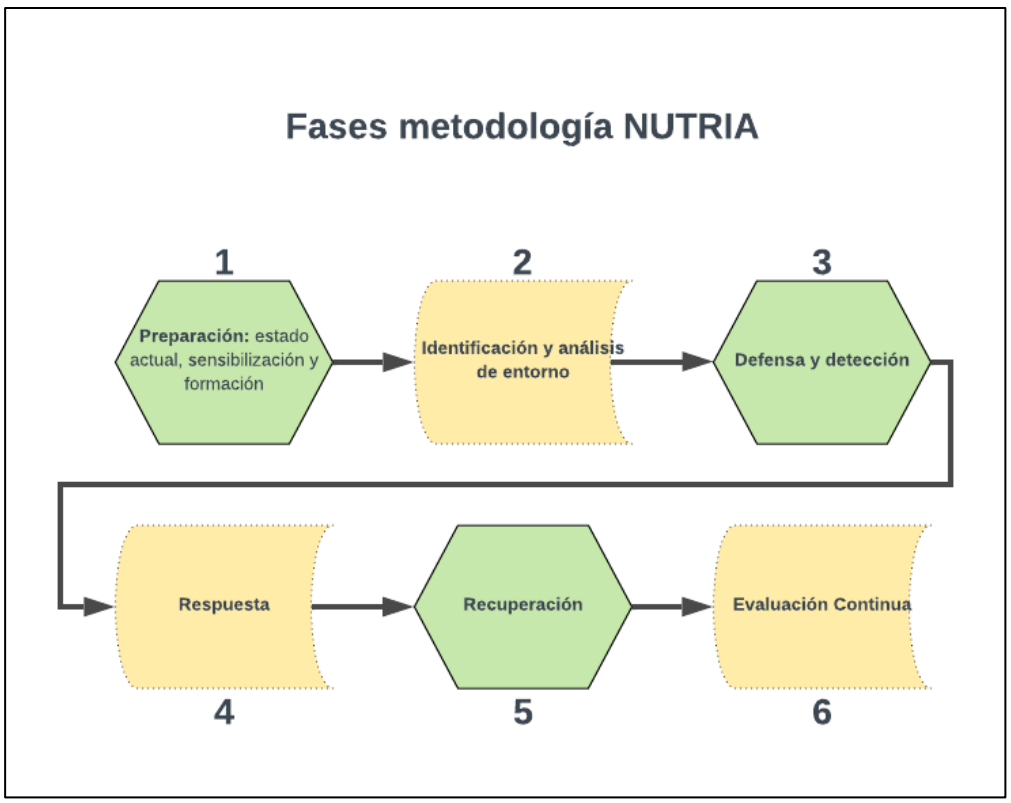

Figura 14. Fases de la metodología NUTRIA. Fuente: elaboración propia.

4.2.1 FASE I: PREPARACIÓN: ESTADO ACTUAL, SENSIBILIZACIÓN Y FORMACIÓN

La realización de un estudio previo, tiene como objetivo principal obtener conocimiento en relación al entorno industrial, a nivel de proceso de producción, así como los diferentes emplazamientos involucrados en el entorno industrial bajo estudio.

De este modo, durante esta fase es solicitada información relacionada con la protección de la seguridad de las instalaciones, así como de las comunicaciones que son llevadas a cabo, obteniendo la siguiente información de la compañía:

- Esquemas de red.
- Inventario de los diferentes sistemas involucrados, tanto TI como TO.
- Planes de direccionamiento en la interconexión de redes.
- Políticas y procedimientos: contratación, formación continua, auditoria interna, reevaluación y revisión de las políticas.

- Información, esquemas, planos de la instalación.
- Comunicación y distribución con terceras partes.
- Histórico de seguridad de la compañía.
- Procedimientos de actuación en caso de incidentes.

Con el aporte de información anteriormente citado, da comienzo la obtención de conocimiento del estado del entorno y su seguridad. De este modo, se procede a realizar la visita física a las instalaciones con objetivo de realizar el diagnostico real en que se encuentra la compañía, mediante la recopilación de información, por medio de entrevistas con el personal implicado en la producción desde el responsable de planta, ingenieros y responsable de mantenimiento que estén relacionados con las operaciones de planta.

De este modo, se obtiene la idea principal del estado actual de redes, sistemas e instalaciones de las que dispone la planta como punto de partida del análisis e implementación de la ciberseguridad para el desarrollo de la metodología.

4.2.1.1 Identificación de funciones y responsabilidades

La identificación de las funciones y responsabilidades de los empleados involucrados en el proceso de operación y/o gestión, relacionado con la ciberseguridad de planta, cumple un papel de gran importancia, teniendo en cuenta que roles específicos han de llevar a cabo diferentes tareas relacionadas con la protección de la compañía, en diferentes niveles.

En función del tamaño de la compañía, los roles establecidos varían según el volumen de empleados. A continuación, se definen los diferentes roles que pueden establecerse como responsables de la seguridad de la planta.

- **Dirección:** Participación en la implementación del sistema de seguridad para entornos industriales, responsable de que todos los empleados de la compañía conozcan y apliquen las políticas de seguridad definidas.

- **Empleados:** La responsabilidad del trabajador recae en el debido cumplimiento de las políticas establecidas y/o procedimientos de seguridad implementados en la compañía.

- **Proveedores y/o contratistas:** Toda aquella compañía externa con acceso a los activos a proteger la de la empresa, están obligados al cumplimiento de la normativa vigente en referencia a políticas y controles de seguridad.

- **Administradores de los sistemas (TI/TO):** Los administradores o encargados de procesos en función del ámbito TI/TO en el que estén involucrados, se trata de un rol esencial para la protección de los activos de la compañía. La participación activa en la gestión y mantenimiento de los sistemas les hace responsables del cumplimiento de las políticas definidas.

  Así, los administradores deben supervisar que se cumplan todas las políticas, estándares, normas y/o procedimientos definidos por la dirección de la empresa que son de obligada aplicación, bajo su responsabilidad, junto el departamento de formación o el rol definido para llevar a cabo dicha actividad

- **Departamento de formación:** El personal perteneciente a este departamento, debe realizar junto con dirección, un plan de formación para los empleados, contemplando las necesidades de cada uno de ellos en función del cargo desempeñado. La formación debe servir como canal de conocimiento entre la empresa y el trabajador, permitiendo divulgar metodologías de protección y defensa en el ámbito de la seguridad.

Una vez sea establecido el sistema de gestión de seguridad en entornos industriales, cabe la posibilidad de un incremento de roles, o que las responsabilidades de los roles definidos se incrementen y/o varíen, en función de la estrategia a seguir.

Así, para la presente metodología es definido un nuevo rol, el **Encargado de Zona y/o Conducto**. En los pasos siguientes de la metodología (Fase 3), se llevará a cabo la segregación de zonas en función de los activos a proteger y la comunicación de dichas zonas por medio de conductos seguros.

Tras el establecimiento de la metodología, en función de las zonas con las que cuenten, es necesario establecer el rol de encargado de zona, es decir, aquella persona cuya tarea trata de la supervisión del cumplimiento de controles y políticas establecidas por zona y la comunicación por medio de los conductos que forman parte de la zona.

4.2.1.2 Estudio de la formación y sensibilización con la ciberseguridad

La formación y concienciación en relación a la seguridad, se trata de un factor clave en la implementación de controles y metodologías de gestión de las partes que integran tanto las Tecnologías de la Operación como las de la Información. De este modo, personas y organizaciones deben conocer los objetivos y responsabilidades que conllevan las actividades realizadas en la planta.

Para obtener una protección de los sistemas y de la información de las compañías, es necesario invertir tiempo y esfuerzo en la concienciación y formación de los empleados, teniendo en cuenta, que se trata del eslabón más débil en la cadena de seguridad. Las políticas y procedimientos implementados, sin una adecuada implicación del personal hacen que las medidas tomadas sean ineficaces.

De este modo, se propone la implementación de acciones formativas, para cubrir las necesidades de conocimiento de los trabajadores y así, obtener un valor seguro en seguridad para la empresa.

- **Identificación de necesidades**

  Una vez ha sido realizada la evaluación de la seguridad de la compañía, es implementado un informe de Identificación de Necesidades, conforme a los resultados obtenidos, mediante entrevistas a personal, así como de las observaciones de campo realizadas y documentadas.

  Con una periodicidad anual desde la primera realización del informe, son definidas las necesidades de formación, en base a las auditorias realizadas, no conformidades encontradas en el plan de seguridad de la empresa, así como la aportación que desde la dirección, se desee llevar a cabo.

- **Plan interno de formación**

  Con la identificación de las necesidades de formación definidas, se procede a realizar el plan interno de formación en seguridad, en base a las necesidades de la empresa la formación puede ser de carácter interno o externo.

  Los cursos destinados al personal de la compañía, deberán de estar definidos conforme a las necesidades de formación de cada rol involucrado, teniendo en cuenta

su participación en el proceso de producción y su involucración en la seguridad de los sistemas a proteger.

La situación geografía y disponibilidad horaria de los trabajadores son funcionalidades imprescindibles a la hora de establecer el plan interno de formación, contemplando la necesidad de que todos los trabajadores estén en conocimiento de la metodología de trabajo en un entorno seguro, procedimientos y acciones a realizar según las labores que sean desarrolladas en planta.

- **Ejercicios prácticos y teóricos para los trabajadores**

  El departamento de formación o la persona asignada para desarrollar dicha tarea, debe implementar acciones formativas mediante la realización de una evaluación posterior a los trabajadores, que asegure que, el personal de la compañía ha alcanzado el conocimiento para la realización de sus tareas en un entorno seguro.

- **Registro de evaluación**

  La evaluación del personal puede ser realizada a través de exámenes, cuestionarios, cursos, talleres o cualquier metodología que certifique el alcance del conocimiento esperado por parte de los trabajadores.

  La evaluación de la eficacia y eficiencia de la formación realizada es indispensable, al finalizar cualquier acción formativa los trabajadores de la compañía ofrecerán una evaluación sobre la formación recibida para el departamento de formación o persona designada a la realización de esta tarea.

La formación y sensibilización busca como meta el enfoque global de la compañía hacía la implementación de sistemas resilientes, es decir, sistemas capaces de volver al funcionamiento normal o volver a un estado anterior de estabilidad capaz de vencer los problemas surgidos, la capacitación y conocimiento del personal es una herramienta imprescindible para el establecimiento de un modelo de operación seguro en la planta.
(IEC, 2013)

4.2.2 FASE II: IDENTIFICACIÓN Y ANÁLISIS DEL ENTORNO

4.2.2.1 SuC "System under Consideration"

Siguiendo la recomendación del estándar 62443 (IEC, 2013), se propone comenzar el análisis mediante la clara identificación del SuC o "Sistema bajo Consideración", siendo este la infraestructura completa bajo análisis.

De este modo, en función del tipo de compañía y de los activos a proteger, este sistema quedará definido, como punto de partida para la implementación de la metodología, pudiendo incluir las redes de control, supervisión en red, infraestructura de comunicaciones y seguridad. Se tiene en cuenta que cada compañía cuenta con diferentes sistemas industriales, que cuentan con una mayor o menor complejidad, por lo que se ha de estudiar el nivel de seguridad a aplicar a todos sus componentes para finalmente establecer, dentro del SuC definido los conceptos de Zona y Conductos identificados para el "Sistema bajo Consideración".

La identificación del sistema bajo consideración o SuC es la primera actividad a implementar para la realización de un análisis de riesgos apropiado dentro del ámbito industrial (TO). La finalidad de esta actividad pretende alcanzar el conocimiento relativo al diseño del sistema, la configuración e instalación establecida de los activos, las modificaciones de diseño que han sido efectuadas desde su puesta en marcha, así como los procesos de operación y mantenimiento que son llevados a cabo en la compañía.

4.2.2.2 Análisis de la documentación existente

Para obtener un primer borrador del estado de la compañía, es necesario llevar a cabo una evaluación de la documentación disponible y suministrada para realizar un análisis centrado en los cambios que han sido implementados en los sistemas, así como las diferentes conexiones no documentadas o que difieran del estado físico-real que se encuentra implementado.

Como consecuencia del primer análisis documental llevado a cabo, los datos obtenidos son registrados para la implementación de un adecuando tratamiento al finalizar el análisis realizado.

En esta fase de evaluación, otro de los objetivos fundamentales es realizar la determinación de las necesidades, en materia de ciberseguridad, con las que debe contar la compañía en relación a procesos de negocio, tanto a nivel de proceso como financiero, teniendo en cuenta que dichos procesos se retroalimentan el uno del otro.

La evaluación no queda centrada únicamente en los procesos de operación o financieros, se contempla que, en el ámbito industrial, el factor medioambiental, así como todas aquellas actividades relacionadas con la salud cobran una gran importancia. De este modo, la evaluación documental recae sobre cualquier actividad y/o elemento que tenga alguna conexión con el apropiado funcionamiento de los diferentes procesos de negocio en la compañía.

4.2.2.3 Inventario de activos TI y TO.

El establecimiento de un inventario es una de las tareas de mayor importancia, teniendo en cuenta la importancia de localizar los activos principales a proteger y el ámbito de conversión TI-TO en el que se encuentra. La valoración de cuando un elemento es considerado activo, varía en función de las compañías y de la magnitud de la misma.

Una vez han sido definidos los activos TI y TO, se deben diferenciar dichos activos entre activos lógicos y físicos, así como la interconexión entre ellos. La sección **2.4 Comparing ICS and IR Systems Security** de la publicación (NIST, 2015) realiza una comparación entre los sistemas, teniendo en cuenta las diferentes características que difieren entre los sistemas tradicionales TI contra los sistemas TO, contemplando riesgos significantes relacionados con la salud, la seguridad de las vidas humanas, los riesgos medioambientales, problemas financieros, así como las pérdidas de producción y su impacto negativo a nivel económico.

La siguiente tabla ofrece la comparativa entre las diferencias de los sistemas relacionados con las Tecnologías de la Información y las Tecnologías de Operación, en relación a las diferencias operativas y de riesgo entre los sistemas TI y los sistemas TO.

De este modo, en base a la siguiente información ofrecida, se pretende establecer un mayor nivel de sofisticación en la aplicación de los controles y estrategias operativas, contemplando las características que constituyen cada una de las tecnologías según su ámbito de aplicación tomando como base la tabla a continuación expuesta

Tabla 1. Referencia a tabla 2.1 Summary of IT System and ICS Differences. Fuente: *(NIST, 2015)*

CATEGORIA	TI	TO
Requerimientos de Operación	No es en tiempo real.	Tiempo real.
	Respuesta consistente.	La respuesta es crítica en el tiempo.
	Exigencia de alto rendimiento.	El rendimiento modesto es aceptable.
	Alto retardo y jitter pueden ser aceptables.	Alto retardo y / o jitter no es aceptable.
	Interacción de emergencia menos crítica.	Respuesta a la emergencia humana es crítica.
	Control de acceso restringido puede ser implementado en el grado necesario para la seguridad.	El acceso a ICS debe ser estrictamente controlado pero no debe obstaculizar o interferir con interacción hombre-máquina.
Disponibilidad		
	Respuestas como reiniciar son aceptables.	Las respuestas como reiniciar pueden no ser aceptables, debido a la disponibilidad del proceso.
	Las deficiencias de disponibilidad a menudo pueden ser toleradas, dependiendo de la requerimientos operacionales.	Los requisitos de disponibilidad pueden requerir sistemas redundantes.
		Las interrupciones deben ser planificadas y programadas días / semanas de antelación.
		La alta disponibilidad requiere pruebas exhaustivas previas al despliegue.
Requerimientos de Administración de Riesgo		
	La confidencialidad e integridad de los datos es principal.	La seguridad humana es primordial, seguida de la protección del proceso.

	Tolerancia a fallos es menos importante.	La tolerancia a fallos es esencial, incluso momentánea.
	Tiempo de inactividad momentáneo no es un riesgo importante	El tiempo de inactividad puede no ser aceptable
	El mayor impacto del riesgo es el retraso del negocio.	Los principales impactos de riesgo son: el incumplimiento normativo, los impactos ambientales, la pérdida de vida humana, equipamiento o producción.
Operación del Sistema		
	Los sistemas están diseñados para ser utilizados con sistemas operativos.	Operación diferenciada y posiblemente propietaria.
	Las actualizaciones son sencillas con herramientas de despliegue automatizadas.	Sistemas, a menudo sin capacidades de seguridad.
		Los cambios de software deben hacerse cuidadosamente, por lo general por los proveedores de software, debido a la algoritmos de control especializados y tal vez hardware modificado y software involucrado.
Recurso	Los sistemas se especifican con suficiente recursos para apoyar la adición de aplicaciones de terceros, como soluciones de seguridad.	
Restricciones		Los sistemas están diseñados para soportar el proceso industrial previsto y puede no tener memoria suficiente y recursos informáticos para apoyar la adición de capacidades de seguridad.
Comunicaciones	Protocolos de comunicaciones estándar.	Muchos protocolos de comunicación propietarios y estándares.

	Principalmente redes cableadas con funcionalidades inalámbricas.	Varios tipos de medios de comunicación incluyendo cable dedicado e inalámbrico (radio y satélite)
	Prácticas típicas de redes de TI.	Las redes son complejas y en ocasiones requieren experiencia de los ingenieros de control.
Cambio administración		
	Los cambios de software se aplican de manera oportuna.	Los cambios de software deben ser probados a fondo y desplegados de forma incremental, a lo largo de un sistema para garantizar que la integridad del sistema de control.
	Moda ante la buena seguridad.	Desconexiones de sistemas ICS deben ser planificados y programados con días / semanas de antelación. Además, pueden usar sistemas operativos que ya no son compatibles
	Política y procedimientos. Los procedimientos son automatizados.	
Soporte	Estilos de soporte diversificados.	El servicio de asistencia suele ser a través de un único proveedor.
Vida Útil	Vida útil del orden de 3 a 5 años.	Vida útil del orden de 10 a 15 años
Ubicación Componentes	Los componentes son generalmente locales y fáciles de acceso.	Los componentes pueden ser aislados, remotos, y requieren un esfuerzo físico extenso para su acceso y manejo.

De este modo, tras la caracterización de los activos, se procede a seguir la metodología definida en el estándar ISA99/IEC62443, la cual establece diferentes niveles jerárquicos diferenciando entre la planificación y logística de negocio, operaciones de control y fabricación, así como el control discreto y continuo. La presente metodología basa su estudio en el establecimiento de niveles jerárquicos como se muestra a continuación:

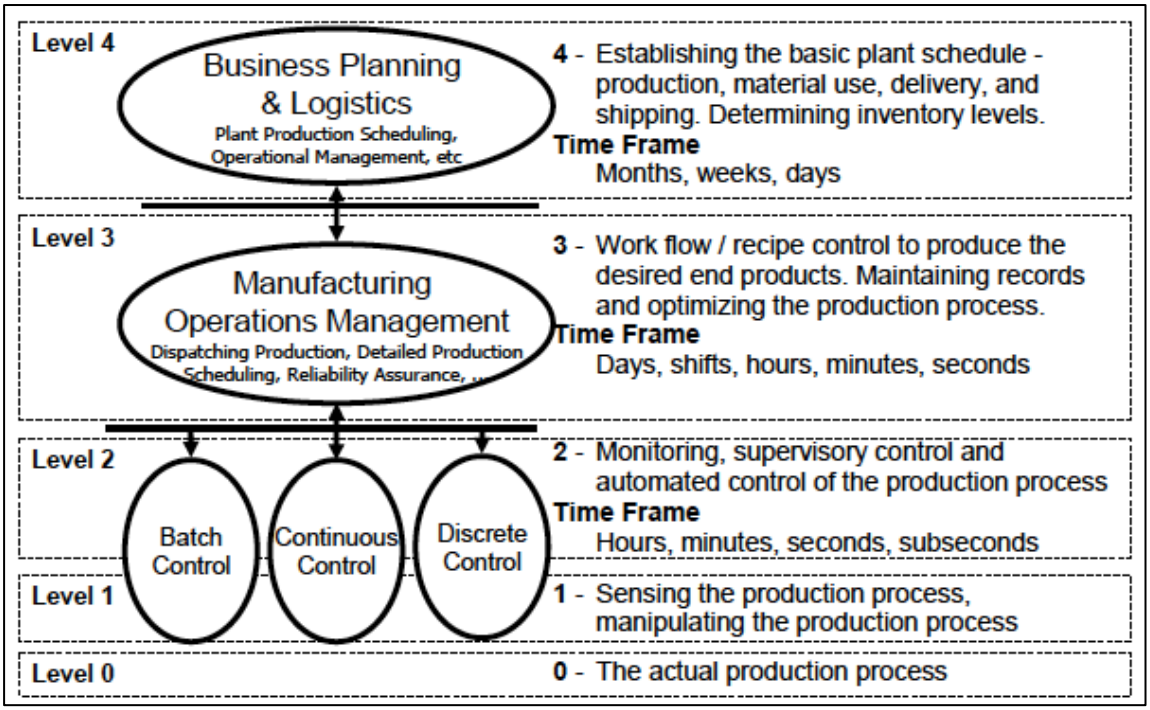

***Figura* 15.** Establecimiento de niveles jerárquicos. Fuente: *(IEC, 2010)*.

Cada uno de los diferentes niveles definidos por el estándar, cuenta con las siguientes características para el establecimiento de los activos de la planta:

- **Nivel 0:** El proceso de producción a nivel físico, este nivel centra su objetivo en obtener el conocimiento de sensores y actuadores situados en el proceso físico, así como los diferentes dispositivos que hacen posible la realización del proceso.

- **Nivel 1:** La obtención de datos sobre el proceso físico llevado a cabo y las actividades que se realizan para la operación con dicho proceso. En este nivel se encuentran ubicados los Sistemas de Control Distribuido (DCS), Controladores Lógicos Programables (PLC), es decir, todo equipamiento conectado a los sensores y actuadores del proceso físico.

- **Nivel 2:** La monitorización y los controles implementados para los procesos físicos forman parte de este nivel, contemplando funcionalidades como las interfaces

hombre-máquina, gestión de las alertas desde operación, registro de los datos de los procesos realizados y supervisión de los procesos.

- **Nivel 3:** La gestión de los flujos de trabajo para la producción en relación a los aspectos relacionados con el mantenimiento y obtención de la información de los procesos, turnos de trabajo de los empleados, costes y organización de la producción de planta, este nivel queda centrado en los objetivos nombrados anteriormente.

- **Nivel 4:** Las operaciones relacionadas con el negocio, gestión de inventario, así como el stock de los materiales necesarios para la producción. Además, en este último nivel del proceso industrial, las actividades relacionadas con la planificación de la planta, mantenimiento preventivo o planificación de la capacidad de generación de la misma, son objetivos bajo estudio según el estándar (IEC, 2010).

Por tanto, para establecer una correcta caracterización de los activos a proteger, es esencial determinar la misión, objetivos y valores de cada uno de ellos, contemplando en primer lugar cual es el sistema bajo consideración. De este modo, se permite asegurar la consistencia y alineamiento entre los productos y servicios de la compañía, los procesos clave a proteger, los sistemas de control involucrados en los procesos clave identificados, así como los proveedores que se encuentran involucrados en cada uno de los procesos a evaluar.

4.2.2.4 Análisis de la seguridad física

Dentro del mundo de las Tecnologías de la Operación, se aprecia una relación íntima entre la seguridad física y la seguridad de la información o cibernética, la evaluación documental de las diferentes políticas y/o buenas prácticas implementadas en la compañía, no aporta la suficiente información sobre el entorno, por lo que se ha de establecer una visualización o auditoria del contexto físico en el que se encuentran cada uno de los activos definidos bajo el sistema bajo consideración (SuC).

La información referente a dichos activos ha de estar definida en la documentación aportada conforme a la implementación física con la que cuentan en realidad, datos relativos a las distancias entre activos, metodología llevada a cabo para la instalación, así como el mantenimiento tanto correctivo como preventivo han de contar con una trazabilidad definida formalmente mediante la cual es posible obtener información de cada uno de los activos a evaluar.

Los procesos que interactúan dentro del sistema bajo consideración han de ser registrados físicamente, todos los registros con los que cuenta la compañía a nivel de proceso son información que ante futuros inconvenientes o amenazas ayudan a alcanzar una solución en el menor tiempo posible, teniendo en cuenta que la rapidez en la resolución de incidencias es el mayor escudo en la lucha contra los ciberataques.

4.2.2.5 Análisis del tráfico entre activos y sus interconexiones

El esquema de red industrial es un aspecto clave a estudiar dado que condiciona como es implementada la ciberseguridad en la planta, por lo que es esencial realizar el estudio de los posibles conductos existentes entre la red corporativa con las redes de control y proceso, así como los diferentes servicios disponibles en la red y los protocolos que son llevados a cabo.

La identificación de los protocolos industriales presentes en la compañía para la evaluación del tráfico es una tarea importante a realizar, se ha de analizar los dispositivos que se comunican entre sí, de tal modo que se recopile la información concerniente a la comunicación de los dispositivos en relación al acceso y caudal de comunicaciones que implementan en función de la metodología de operación de la planta.

La recopilación de toda esta información debe de obtener trazabilidad con la información documental relacionada con las políticas de seguridad, procedimientos para el control de cambios, así como los controles de acceso.

Además, en relación a la capa de red implementada en la compañía se ha de evaluar cómo esta implementada la protección del perímetro, segmentación de redes, la instalación existente de cortafuegos, detectores de intrusiones y proxies. Así como la instalación de antivirus en consolas y ordenadores de planta que cuentan con comunicación entre los activos definidos anteriormente.

Por tanto, una vez han sido localizados los activos y procesos dentro del sistema bajo consideración para la compañía, es determinante analizar el tráfico de red para identificar las diferentes comunicaciones existentes dentro del entorno de la empresa, funcionalidades relativas a la separación y segmentación de red, limitaciones de accesos o realización de actividades involucradas en la operación de la instalación.

Las necesidades a analizar para posteriormente optimizar si no cumple los requisitos o mejorar en caso de tener un buen sistema implementado, recaen en documentar las

diferentes comunicaciones con independencia del segmento y desplegar elementos relacionados con la seguridad perimetral para asegurar la separación y segmentación de las redes TI y TO bajo evaluación en la compañía.

4.2.2.6 Análisis de Vulnerabilidades, identificación de técnicas conocidas.

La identificación de las posibles vulnerabilidades mediante diferentes metodologías y/o fuentes de información del sistema bajo consideración van implementándose conforme se obtiene mayor información del entorno bajo análisis. De este modo, se ha de contemplar que las vulnerabilidades de los sistemas de control no son encontradas únicamente en la parte relacionada con las Tecnologías de la Información, también son encontradas en los sistemas de control a través de la información que con los años se ha ido aportando sobre el diseño de los mismos, su implementación y como es realizada su operación.

Así, teniendo en cuenta la posibilidad de que en la compañía existan activos a proteger con una antigüedad elevada, es posible que hayan sido víctimas en diferentes empresas de vulnerabilidades específicas de estos sistemas, que no han sido solventadas.

4.2.2.7 Análisis de Amenazas en los Sistemas Industriales

La imagen que una empresa proyecta al mercado cuenta con un vínculo estrecho con la importancia de asegurar sus sistemas de control. De este modo, el malware, así como ataques de denegación de servicio comienzan a ser más comunes en las compañías lo que puede llegar a ocasionar impactos en diversas áreas (INCIBE, 2015):

- **Seguridad Física:** Se hace referencia a la consecuencia directa de obtener fallos en los sistemas de control de la planta pudiendo ser extremadamente críticos teniendo en cuenta la posibilidad de ocasionar pérdidas de vidas o lesiones en personas, así como fuga de información o daño medioambiental.

- **Economía de la empresa:** Tras un impacto negativo en la compañía, debido a intrusiones o perdida de la disponibilidad, las pérdidas económicas influyen en el correcto funcionamiento de la empresa, bien por la necesidad de recambio de dispositivos dañados o por una parada en el proceso de producción y/o distribución de servicios.

- **Imagen social:** Un impacto negativo en la compañía debido a un ataque, pérdida de información o bien perdida de la disponibilidad de los equipos que forman parte de la cadena de producción, ocasiona una pérdida de confianza por parte de los clientes de la compañía, así como daño en su imagen y por consiguiente pérdidas económicas.

De este modo, según define INCIBE en su artículo (INCIBE, 2015) entre las incidencias habituales que pueden encontrarse en los sistemas de control, cabe nombrar las siguientes, las cuales forman parte de la presente metodología como objeto de análisis:

- **Interrupción de las operaciones** por retrasos o bloqueos del flujo de información a través de las redes corporativas o de control, denegando los servicios activos en las redes de control o causando cuellos de botella a la hora de transferir información.
- **Cambios no autorizados** realizados en instrucciones de programas en PLCs, RTUs, DCS o controladores SCADA, cambios en los parámetros de las alarmas, problemas con comandos no autorizados en equipos de control que lleguen a dañar el propio equipo, paradas prematuras de procesos o incluso deshabilitar el equipo de control.
- **Envío de información falsa** a los operadores encargados de controlar el sistema, ya sea para disimular cambios no autorizados o para iniciar acciones inapropiadas.
- **Modificación de software o configuración del sistema** produciendo resultados impredecibles.
- **Introducción en el sistema de software malicioso** (por ejemplo, virus, gusanos, troyanos).
- **Modificación de instrucciones** para la creación de un producto con el fin de provocar daños personales o a equipos pertenecientes a la organización.

Así, se ha de tener en cuenta que las amenazas siempre han estado presente en los sistemas de control industrial, la inclusión de la tecnología en el ámbito TO, hace que la explotación de dichas amenazas sea más fácil, por lo que cobra una mayor importancia realizar un análisis exhaustivo de la compañía y sus riesgos.

4.2.2.8 Evaluación de riesgos

La evaluación de riesgos trata sobre el análisis sobre todo aquello que potencialmente puede ser un peligro en una situación particular en condiciones específicas con configuraciones propias del sistema bajo análisis.

Para descubrir dichos fallos en la seguridad o vulnerabilidades en los sistemas, es evaluada la posibilidad de que algo falle y el impacto que genera en la compañía.

Según Pascal Ackerman, en su publicación (Ackerman, 2017), ofrece una definición completa sobre los tipos de riesgos que pueden encontrarse en la realización del análisis de riesgos:

> *"El riesgo es la probabilidad de que una fuente de amenaza cause un evento de amenaza, mediante un vector de amenaza, debido a una vulnerabilidad potencial en un objetivo, y cuál será la consecuencia y el impacto resultante"*

- Fuente de amenaza, es quien inicia la explotación en el sistema, también llamado agente malicioso.

- Evento de amenaza, es el acto de explotación de la vulnerabilidad o ataque en el sistema bajo consideración o SuC.

- Vector de ataque, es el camino de ataque o el método de transporte llevado a cabo para la explotación, pudiendo ser mediante infección de dispositivos externos o phising, mediante correo electrónico para enviar componentes maliciosos.

- Probabilidad, es la oportunidad de encontrar una vulnerabilidad que pueda llegar a ser un evento de amenaza.

- El objetivo, es el sistema bajo consideración SuC.

- La consecuencia es el resultado directo de un evento de amenaza exitoso, como la pérdida de un servicio o instalación de programas maliciosos en la red.

- El impacto es el resultado de las operaciones, la imagen de la compañía o el bienestar económico.

Por tanto, la evaluación de riesgos gira en torno a cuáles son las principales vulnerabilidades del SuC, cuales son las oportunidades de explotación de las mismas, así como las consecuencias que dichas vulnerabilidades pueden ocasionar en la compañía.

El resultado del análisis de riesgos es una puntuación para la vulnerabilidad encontrada, dicha puntuación considera todos los factores que determinan el riesgo mediante la aplicación de la siguiente ecuación:

$$Riesgo = \frac{severidad + (criticidad * 2) + (probabilidad * 2) + (impacto * 2)}{4}$$

Cada uno de los factores de la ecuación anterior quedan definidos con la siguiente puntuación:

- **Severidad:** Se trata de la puntuación dada que oscila entre 0 y 10, dada a la vulnerabilidad en función de la base de datos de vulnerabilidades públicas mediante la aplicación de un algoritmo como el Common Vulnerability Scoring System (CVSS), que proporciona un marco de referencia para el cálculo de las características e impacto de las vulnerabilidades TI.

- **Criticidad:** Se trata de una puntuación entre 1 y 5 que refleja la importancia del Suc en conjunto con todos los procesos que abarca.

- **Probabilidad:** Se trata de un número entre 1 y 5 que refleja la oportunidad de que la vulnerabilidad pueda ser explotada con éxito. La calidad de una evaluación de riesgo queda basada en gran medida en la puntuación de la probabilidad teniendo en cuenta la información que aporta a cerca de la posibilidad de explotación de vulnerabilidades descubiertas, así como de producirse un evento de amenaza.

- **Impacto:** Se trata de una puntuación de entre 1 y 5 que refleja el impacto financiero en la compañía, el daño asociado a la imagen corporativa, el impacto potencial en el entorno, así como los riesgos asociados a los empleados y la seguridad de la salud en caso de comprometer o fallar dicho sistema. Por tanto, el impacto calcula el coste total de compromiso que genera una puntuación procesable correlacionando con los sistemas dentro del proceso.

El presupuesto para la protección de los activos TI y TO son limitados en las compañías, por lo que los esfuerzos en la mitigación de los riesgos estimados deben concentrarse en las áreas que son capaces de mitigar el mayor riesgo en función del esfuerzo y la inversión a realizar.
Por tanto, para llevar a cabo una correcta evaluación de riesgos se deben llevar a cabo diferentes actividades durante el análisis:

- **Identificación de los activos y caracterización del sistema:** En este primer paso se trata de definir los activos que forman parte del "Sistema bajo Consideración" y evaluar la criticidad del valor de los activos para obtener la puntuación del factor "impacto" mediante una lista de objetivos potenciales.

- **Identificación de vulnerabilidades y Threat Modeling:** En este paso del análisis de riesgos son descubiertas las vulnerabilidades potenciales dentro de los activos definidos y su asociación con la puntuación CVSS para el cálculo de la severidad. Por medio del Threat Modeling, definido por SANS Institute (SANS INSTITUTE, 2019) como el proceso de identificación de amenazas potenciales desde diversas perspectivas, incluyendo los puntos de vista del atacante, riesgo y software y cuyo propósito es proporcionar controles de seguridad con un análisis sistemático de los probables vectores de ataque para el estudio de los activos atacados por el atacante y por tanto la identificación del perfil del atacante.

  Algunos de los métodos de modelado de sistemas ICS más conocidos son:

  - Perdue Enterprise Reference Arquitecture Model (PERA), (Williams).
  - Smart Grid Architecture Model (SGAM), (Mathias Uslar 1, 2019)
  - RAMI 4.0 Model, (Bill Lydon, 2019).

  Mediante la realización de esta actividad, también se obtiene la evaluación de la probabilidad de impacto de las vulnerabilidades en el sistema.

  Los resultados obtenidos ofrecen un listado de escenarios de riesgo potencial cuya información es relevante para el "Sistema bajo Consideración".

- **Cálculo del riesgo y mitigación:** Por medio de este cálculo se obtiene el impacto total de un evento de amenaza en cada vulnerabilidad encontrada dentro de los activos del "Sistema bajo Consideración", la combinación de la información analizada hasta el momento ofrece la puntuación del riesgo. Los resultados obtenidos en este punto serán la puntuación de riesgo procesable por vulnerabilidad encontrada y una ayuda para la estrategia de mitigación.

4.2.3 FASE III: DEFENSA Y DETECCIÓN

La protección en relación a la gestión de la ciberseguridad industrial queda definida en la presente metodología como el pilar principal que una compañía debe llevar a cabo de modo continuo.

La implementación de metodologías de protección implica tomar acciones en diferentes ámbitos de la empresa, contemplando los activos a proteger definidos anteriormente y su implicación con las tecnologías IT-OT.

El CCI en su serie de cuadernillos CCI. Número uno define el establecimiento de zonas y conductos según el estándar ISA99/IEC6443 (IEC, 2013). De este modo, una vez ha quedado analizado el entorno que vamos a proteger dentro de la compañía, se procede a establecer el nivel de seguridad en función de los componentes del sistema, es decir, a proteger los activos que forman parte del sistema bajo consideración, en función de sus características TI-OT.

Así, entran en juego los conceptos de Zonas y Conductos como las divisiones e interconexiones que van a ser establecidas dentro de la compañía para asegurar una segregación de redes y una división de los activos según el ámbito aplicable a cada uno de ellos.

Una **Zona** queda definida como un conjunto de activos, bien sean físicos, aplicaciones o relativos a la información de la compañía que cuentan con las mismas características relacionadas con la seguridad.

Un **Conducto**, trata de una zona con características particulares cuya misión principal es establecer la comunicación entre diferentes zonas bajo unos requisitos de seguridad apropiados.

De este modo, en primer lugar, se procede al establecimiento de las zonas que aplican dentro del SuC definido anteriormente. Así, cada una de las zonas definidas en función del volumen de la empresa deben contar con las siguientes características:

- **Agrupación de los activos de características comunes:** En función de la definición de activo ofrecida en el inventario, son agrupados aquellos que cuentan con características comunes en el proceso industrial, es decir, PLCs, RTUs, estaciones de ingeniería, dispositivos de comunicación, etc.

- **Sub-zonas:** La división de zonas en sub-zonas depende de el volumen de la empresa, y del nivel de seguridad que se desea establecer en función del SuC y del volumen de activos que éste abarca, pudiendo aplicar el establecimiento de sub-zonas dentro de una zona común o no aplicar contemplando que la zona abarca con todos los requerimientos de seguridad que se desean implementar.

- **Herencia:** Existe la posibilidad que, al realizar la disgregación de las zonas de protección que algunos activos compartan características con diferentes zonas, es decir, debido a sus cualidades forman parte de dos zonas diferentes. En tal caso, dichos activos deben cumplir con los requerimientos implementados en la zona principal de la que parten.

- **Características de la zona:** Todas las zonas definidas dentro del mapa de seguridad de la compañía deben contar con:

    - Políticas y niveles de seguridad de la zona.
    - Requisitos de seguridad, acceso y controles a la zona.
    - Nivel de riesgo tolerable alcanzado.
    - Alcance de la zona.
    - Inventario de Activos por zona.
    - Estructura organizativa.
    - Roles y responsabilidades.
    - Riesgos asociados a la zona: amenazas y vulnerabilidades.
    - Estrategia de seguridad por zona.

Una vez han sido establecidas las zonas a proteger, da paso la implementación de las zonas especiales o conductos cuya responsabilidad es proteger la comunicación entre zonas, en otras palabras, podría definirse como las penetraciones o vías de comunicación segura entre

zonas que permite asegurar que la información de cada zona viaja protegida asegurando la confidencialidad de la información que transporta mediante la implementación de los siguientes requisitos:

- **Protección** de los canales que contienen vínculos con activos TO.
- Dispositivos de red (switches, routers, firewalls), servidores o pasarelas de comunicaciones para conversión de protocolos.
- **Características del conducto:** Todos los conductos definidos dentro del mapa de seguridad de la compañía deben contar con:
    - Políticas y niveles de seguridad del conducto.
    - Requisitos de seguridad, acceso y controles del conducto.
    - Nivel de riesgo tolerable alcanzado.
    - Alcance del conducto
    - Inventario de Activos por conducto.
    - Estructura organizativa.
    - Roles y responsabilidades.
    - Riesgos asociados al conducto: amenazas y vulnerabilidades.
    - Estrategia de seguridad por conducto.

Según el estándar los criterios iniciales para la diferenciación entre Zonas y Conductos quedan definidos en los siguientes puntos a tratar para lograr alcanzar la protección deseada por la compañía:

- Los **activos TI y TO** deben pertenecer a agrupaciones o Zonas diferentes. La principal causa de dicha separación entre entornos es que los sistemas industriales pueden ocasionar impacto en la salud de las personas, así como en el medio ambiente. Además, la posibilidad de generar una perdida en la producción de la planta dañaría a la compañía no solo a nivel productividad, la imagen de la empresa quedaría dañada a nivel corporativo.

- Existe una diferenciación a nivel funcional teniendo en cuenta que los **roles y responsabilidades** de cada una de las áreas suele recaer en personas diferentes. En el caso de las PYMES se ha de contemplar la existencia de roles que comparten cargo para activos relacionados con la información de negocio y control industrial. En tal caso, serían implementados roles compartidos por zonas, contemplando el volumen de la empresa.

- **Sistemas Instrumentados de Seguridad**, o sistemas encargados de llevar a cabo la ejecución automática de acciones que garantizan el estado seguro de la planta deben formar parte de una misma zona. Los SIS son aquellos sistemas que cuentan con los siguientes componentes:

    - Sensores encargados de detectar alteraciones de procesos.
    - Dispositivos lógicos que determinan acciones peligrosas y envían señales de aviso.
    - Dispositivos de control que implementan acciones correctivas en caso de aviso por fallo o error.

- **Dispositivos de conexión temporal**, zona diferente: dispositivos de almacenamiento, herramientas de análisis.

- **Comunicaciones inalámbricas**, deben estar en una zona separada de las comunicaciones cableadas.

De este modo, en la definición de las políticas aplicables a zonas y conductos, deben quedar documentados cada uno de estos puntos, en función de la división establecida en la compañía:

- Identificación de zona y/o conducto.
- Perímetro lógico aplicable.
- Perímetro físico aplicable.
- Accesos a las zonas y conductos, regulación de dichos accesos, por rol y necesidad de conocer.
- Flujo de información entre los accesos definidos.
- Interconexión entre zonas y conductos.
- Nivel de ciberseguridad establecido.
- Procedimientos y políticas de ciberseguridad aplicables por zona y conducto.
- Dependencias de zonas y conductos con diferentes zonas establecidas.

4.2.3.1 Recomendaciones para la detección de incidencias

La fase de detección se centra en las diferentes actividades concernientes a la identificación de la ocurrencia de un evento de ciberseguridad. De este modo, dicha fase permite el descubrimiento de las diferentes funcionalidades relacionadas con la ciberseguridad en la compañía.

Por tanto, la idea principal a seguir queda definida en la identificación de diferentes anomalías y eventos, que cuentan con impacto potencial en la operación de los sistemas, un incremento en las capacidades de monitoreo continuo de ciberseguridad que permite verificar la efectividad de las medidas de protección a nivel de red, así como protección física se establece como premisa a seguir.

Para mantener la operación de planta dentro del nivel tolerable de riesgo, es necesario implementar una estrategia basada en la detección de anomalías y cambios en el entorno de la empresa contemplando los sistemas de operación y los de información.

Los objetivos de detección son los siguientes:

- Conocer posibles incidentes o anomalías en los procesos que involucren activos.
- Conocer las posibles vulnerabilidades que podrían afectar a los sistemas TI/TO.
- Identificar amenazas que comprometen a la compañía.
- Obtener conocimiento sobre la efectividad de las medidas de ciberseguridad.
- Poseer herramientas, tecnologías y/o estrategias automatizadas que permitan ofrecer la información requerida en el contexto apropiado y en el periodo que se desea.

La automatización de procesos de seguimiento para acontecimientos que ocurren en las redes, puede llevarse a cabo por medio de sistemas de detección de intrusiones (IDS), así como, con sistemas de prevención de intrusiones (IPS), software encargado del control de acceso a las redes informáticas para proteger los sistemas de posibles ataques.

De este modo, el tratamiento ofrecido a los sistemas de control industrial ha de ser activamente monitorizado, preferentemente por un servicio especializado en la detección de incidencias.

Por otro lado, las compañías deben identificar, comunicar y recuperar el estado de operación ante vulnerabilidades encontradas, por medio de herramientas de identificación de

vulnerabilidades conocidas en hosts y redes de sistemas. Además de, herramientas para la gestión de parches. Gracias al uso de estas herramientas es posible identificar, de un modo rápido y sencillo el software fuera de fecha, cumplimientos de políticas y generar alertas e informes sobre las vulnerabilidades encontradas.

La detección de malware permite la identificación sobre la presencia de virus, troyanos, software espía, así como diferente código malicioso. La compañía debe contar con mecanismos de detección de malware en las entradas y salidas de los sistemas a proteger, bien sea con contrafuegos, servidores de correo electrónico, servidores web, servidores proxy, servidores de acceso remoto, así como, en estaciones de trabajo, dispositivos removibles y todos aquellos puntos de acceso que cuenten con algún tipo de comunicación con los activos a proteger.

4.2.4 FASE IV: RESPUESTA

4.2.4.1 Copias de seguridad de sistemas y equipos.

La identificación de la información que se desea guardar va ligada de la identificación de los activos a proteger. De este modo, una vez han sido definidos los activos, se ha de evaluar la información que manejan cada uno de ellos y la importancia de mantener dicha información.

Considerando la posibilidad de pérdida de información por diferentes situaciones, como pueden ser robos, fallos en el sistema bien a nivel físico o lógico, catástrofes naturales y/o medioambientales, contar con un registro de información periódico sobre el estado del sistema es una acción de obligado cumplimiento para la compañía.

Para la implementación de las copias de seguridad, siguiendo las recomendaciones de INCIBE (INCIBE, 2015) aconseja la realización de cuatro prácticas para el proceso completo de implementación de copias de seguridad:

- **Identificación de la información a salvaguardar.**

  Para realizar una correcta identificación de la información a salvaguardar se propone realizar las siguientes preguntas:

  - ¿Qué información queremos proteger?
  - ¿Qué información es crítica para el negocio?
  - ¿Es relevante registrar esta información?
  - ¿Cómo afecta su pérdida en la continuidad de negocio?

- **Establecimiento de la metodología para el proceso de copiado.**

  En relación a los tipos de copia existentes, hay tres tipos de copia: incrementales, totales o diferenciales. La compañía debe analizar que tipo de copia se adapta mejor a las características de la empresa.

  Otra de las cuestiones a tener en cuenta, se trata de la periodicidad de realización de las copias de seguridad. Conforme la definición del tipo de copia a realizar es definida la periodicidad de la misma, la política de copias de seguridad ha de ser coherente, no es necesario realizar copias de seguridad totales diarias, si el periodo de actualización de la información es mensual.

- **Ubicación de almacenamiento de la copia de seguridad.**

  Debe ser definido un soporte de almacenamiento, bien sea disco duro portátil, cabina de discos, servicio de almacenamiento en la nube (en caso de servicio de almacenamiento en la nube se deben tener en cuenta como está implementada la metodología en su definición de zonas y conductos, teniendo en cuenta las características de este sistema de almacenamiento).

  En función del soporte de almacenamiento elegido deben ser definidas políticas para la realización del proceso de copia de seguridad y su almacenamiento seguro, teniendo en cuenta que la recuperación ante desastre es uno de los componentes clave en la estrategia de seguridad de una empresa.

- **Plan periódico para la restauración de las copias de seguridad.**

  Con un periodo temporal definido por parte de la compañía, se debe verificar el correcto almacenaje de la información, así como, la verificación de que la información almacenada es la que debe de ser.

De este modo, en caso de necesidad de recuperación de la información almacenada, tener la certeza de que han sido registrados los valores correctos para volver al sistema como se encontraba antes de la incidencia sufrida.

De este modo, debe usarse un sistema replicado, mediante el cual es posible realizar la restauración a valores iniciales de la información contenida, así como la verificación de que la recuperación es posible llevarla a acabo en el tiempo estimado. Así, se certifica la recuperación para la vuelta a operación, sin perdidas de información no esperadas. En caso contrario, se debe realizar un estudio para la resolución de los problemas encontrados en el mínimo tiempo posible.

4.2.5 FASE V: RECUPERACIÓN

4.2.5.1 Proceso de recuperación.

El proceso de recuperación ante un ataque, varia en función de cómo está implementado el sistema de ciberseguridad de la compañía. Así, la protección de la información relevante estará basada en tres fases principales.

En primer lugar, es necesario obtener información a cerca de lo ocurrido en la compañía ante un incidente en la ciberseguridad de los sistemas, por lo que se procede recopilar pruebas para documentar el suceso ocurrido y definir la estrategia a seguir:

- ¿Quién ha tenido acceso a la información?
- ¿Cuál ha sido la brecha de acceso a la información?
- ¿Por qué se pudo acceder?
- ¿Qué metodología se siguió para el acceso?

De este modo, teniendo en cuenta la cada vez mayor influencia de malware en las redes y la corrupción de la información que genera este programa malicioso en los archivos, la recopilación de toda la información posible a cerca del incidente en el menor tiempo posible, ayuda a que el proceso de recuperación se minimice alcanzando así el modo operacional en el menor tiempo posible.

A continuación, la realización del análisis de la información y por consiguiente investigación del suceso ocurrido para realizar la respuesta al incidente. Los centros de operaciones de

seguridad o SOC de las compañías que pueden costearlo, son los encargados de dar respuesta a las preguntas definidas en la recopilación de información anteriormente realizada.

En el caso de la pequeña y mediana empresa, para aquellas compañías que económicamente no pueden financiar el coste de un SOC, deben de tener desinadas responsabilidades de seguridad, bien mediante contratación de servicios forenses o servicios de validación de terceros, que certifiquen que no ha habido colusión o negligencia, además del personal para la protección de las zonas establecidas en el modelo de ciberseguridad basado en zonas y conductos (IEC, 2013).

Las preguntas que deben obtener respuesta están relacionas con los siguientes conceptos:

- ¿Cuándo y cómo tuvo lugar el incidente de seguridad?
- ¿Siguen obtenido información los atacantes tras el indecente de seguridad?
- ¿Han dejado información en el sistema?
- ¿Es posible detener el ataque o el sistema sigue siendo vulnerable?
- ¿Hay infiltrados dentro de la compañía?

La capacidad de identificación y recuperación de la información en el menor tiempo posible sobre el suceso ocurrido, garantiza la implementación de mecanismos de recuperación con mayor velocidad.

Por tanto, las compañías deben examinar y aprovechar las diferentes herramientas que están a su alcance, para implementar un plan de soporte al análisis de las incidencias producidas por ciberataques. Además, la cooperación entre los diferentes roles involucrados en la ciberseguridad de la compañía desde personal de seguridad, desarrolladores, operación y dirección.

En definitiva, se ha de invertir el escenario de desastre a un escenario de operación en el menor tiempo posible, mediante un plan estratégico de seguridad, así como la cooperación del personal de la empresa.

4.2.5.2 Ciberresiliencia

Se define ciber-resiliencia como la capacidad de una compañía para adaptarse y continuar con sus funciones, así como su trabajo en situaciones de riesgo. De este modo, trata de como se ha de actuar y gestionar la situación de una forma eficiente afectando lo mínimo posible al desempeño de la empresa.

En relación a los ICS (Sistemas de Control Industrial) se abarcan varios tipos de control industrial e instrumentos asociados, que son utilizados para el control de procesos industriales, dichos dispositivos son ejecutados en redes dedicadas mediante protocolos específicos. Las soluciones de ciberresiliencia son implementadas mediante monitorización de manera pasiva, se contempla que la rigidez de los procesos operacionales y su cumplimiento de patrones por medio de "machine learning", es decir, el software aprende cual es el funcionamiento optimo para en caso de anomalía y fallo del sistema, envía alarma del sistema para actuar mediante los protocolos de actuación definidos.

De este modo, la monitorización de red pasiva (NMS), trata de una metodología para la recolección de tráfico de red, a través del puerto de duplicación de tráfico en los conmutadores, dichos elementos no tienen capacidad para bloquear o evitar las comunicaciones.

Las redes TI o redes de tecnologías de la información y las redes TO dedicadas a comunicar los conmutadores, estas dos redes tienen que estar separadas dado que cuentan con un comportamiento diferente.

Las redes TI cuentan con un flujo de información no determinístico, es decir, es difícil saber cuanta información está circulando, sin embargo, las redes TO son más determinísticas dado que se trata de un comportamiento más ordenado dentro de la red, los comportamientos de las redes TO repiten la manera de regular el tráfico.

Dentro de los procesos, se encuentran las ordenes de producción programadas, la intervención del ser humano es menor, se trata de ordenes predeterminadas para procesos industriales, por lo que las ordenes quedan fijas en cualquiera de los procesos preestablecidos.

Características red TI:

- Cientos de sistemas usando cientos de aplicaciones.
- Comportamiento de los dispositivos difícil de predecir.
- Cambio frecuente en los patrones de comportamiento.

Características red TO:

- Número limitado de sistemas.
- Repetición de las operaciones una y otra vez.
- Pocos cambios y planificados por adelantado.

De este modo, las prioridades en las redes TI son diferentes que en las redes TO, contemplando una mayor importancia la **confidencialidad** para el entorno TI, en contraposición al entorno TO cuyas prioridades son la **disponibilidad** e **integridad:**

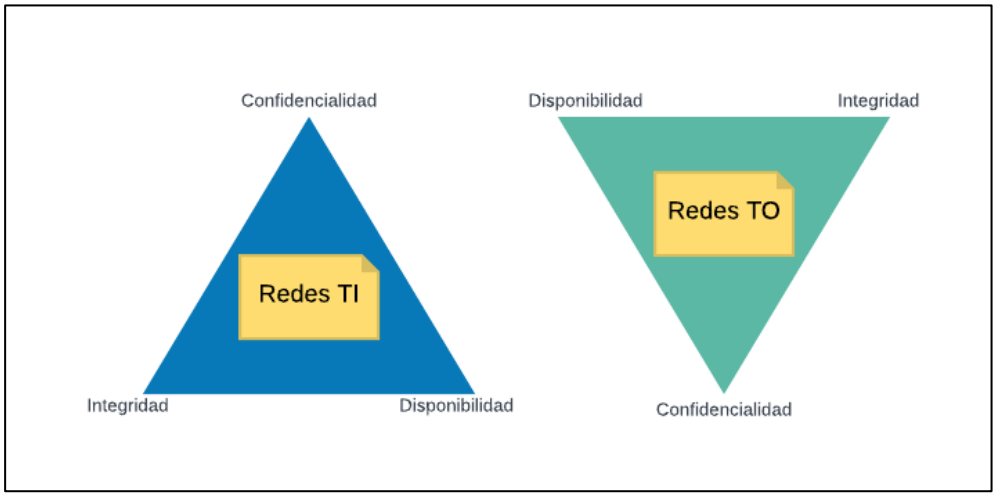

Figura 16. Prioridades redes TI y TO. Fuente: elaboración propia.

Otra de las diferencias entre el mundo TI y TO son las prioridades, en el mundo TI cobra mayor importancia la confidencialidad, es decir, que la información que se transmite no sea mostrada. Sin embargo, en TO, la disponibilidad es la premisa principal teniendo en cuenta que se está estableciendo en base a los procesos que suceden, en tiempo real, y las pérdidas que pueden generarse.

Cuando se va a implementar una solución de seguridad, es necesario saber cuántas redes hay en la organización, equipos, responsables, roles de la compañía, que tengan la visión completa de las políticas que hay en los dos mundos TI y TO.

Los propietarios de los activos:

- Establecimiento de procedimientos de adquisición adecuados.
- Contemplar los riesgos a la hora de interconectar equipos.
- Recuperación ante fallos en diferentes puntos de la infraestructura tecnológica.

De este modo, se debe documentar y actualizar las anomalías encontradas en los sistemas, no depender únicamente de que sea el sistema operativo actual, la segmentación de redes y la concienciación a nivel de entrenamiento.

4.2.5.3 Medidas para alcanzar la Ciber-Resiliencia

La implementación de diagramas de redes industriales que componen la planta, como se estableció anteriormente por medio de la disgregación entre zonas y conductos teniendo en cuenta que en el ámbito industrial no existe una red única.

De este modo, obtener el conocimiento a cerca de cuales y cuantas redes están definidas en la planta, las zonas establecidas, cuantas DMZ son requeridas para una protección apropiada de los activos establecidos por zona en función de la sensibilidad de los mismos, es un plan estratégico para volver a la estabilidad del sistema, en caso de que éste haya sufrido algún tipo de perturbación, contemplando la disposición física y mediante políticas de normativa aplicable en relación a las redes de la compañía.

Por otro lado, en el recorrido hacia la ciberresiliencia se debe tener en cuenta el ámbito de aplicación de dicha metodología, un entorno industrial en el cual muchos de sus dispositivos de operación cuentan con las mismas características que décadas atrás. Así, otro de los inconvenientes que puede encontrar la compañía trata sobre la obsolescencia de las plataformas que tienen implementadas.

Un ejemplo de este problema podría encontrarse en una planta que cuenta con un servidor para la gestión de las operaciones en una plataforma Solaris, los discos duros comienzan a dar errores, contemplando la edad de los dispositivos, la técnica de ciberresiliencia aplicada trata del remplazo de dichos componente teniendo en cuenta que en la actualidad la comercialización de dichos dispositivos no existe por tratarse de tecnología obsoleta.

Además, una de las premisas de mayor importancia para alcanzar una alta capacidad de respuesta y recuperación ante incidentes, trata del conocimiento del personal de la planta en relación a las competencias relacionadas con la seguridad de la misma. De este modo, la compañía desde diferentes niveles jerárquicos es capaz de interpretar y aplicar medidas de seguridad correctivas y preventivas para la ciberresiliencia de la empresa.

4.2.6 FASE VI: EVALUACIÓN CONTINUA

4.2.6.1 Auto evaluación

Una vez realizada la evaluación de los sistemas, redes e instalaciones, se ha de implementar el ejercicio de la auto-evaluación en el cual son propuestas recomendaciones para los sistemas existentes, bien sea mediante contramedidas para la mejora de la ciberseguridad de la planta.

De este modo, el análisis regular del nivel establecido en relación a la ciberseguridad ayuda a la compañía a conocer el grado de exposición, la evaluación periódica permite identificar áreas vulnerables, posibles riesgos y agujeros de seguridad antes de que estos se produzcan. Por lo que, la gestión de forma unificada de accesos, dispositivos y aplicaciones contribuye a mejorar la seguridad de la compañía.

Por otro lado, mediante el ejercicio de auto-evaluación se pretende valorar la capacidad de reacción ante incidentes, muchas veces las compañías no son consientes de que no han evaluado apropiadamente los riesgos o bien, no cuentan con la capacidad para tomar una posición reactiva ante incidentes.

Además, debe de contemplarse la evolución continua de la infraestructura tecnológica de la empresa, teniendo en cuenta que debe adaptarse a las regulaciones y nuevas metodologías de trabajo que conllevan las ultimas plataformas tecnológicas. De este modo, buenas prácticas consideradas en años anteriores pueden que a día de hoy no lo sean. Así, las evaluaciones de riesgos periódicas ayudan a la pro actividad de la compañía por medio de actualizaciones continuas que permites una elevada adaptación a los cambios de las nuevas tecnologías.

Por otro lado, teniendo en cuenta el “talón de Aquiles” que suponen los dispositivos móviles, correos electrónicos y archivos, por ser elementos en manos de cualquier empleado que suponen un canal de entrada al sistema, formación y entrenamiento del personal deben ser tareas esenciales para la prevención de futuros ataques, además de dotar con herramientas de reacción de manera adecuada ante una amenaza de ciberseguridad a todos los trabajadores de la planta, según su cargo y responsabilidad.

Una compañía con una buena preparación de ciberseguridad cuenta con alta capacidad de respuesta ante situaciones de peligro de diversa índole. Por tanto, para implementar los correctos mecanismos y funcionalidades de protección deben ser evaluados los riegos a los que está expuesta la compañía, teniendo en cuenta que en el entorno de ciberseguridad, no

existe una garantía total. Así, la implementación de un plan de ciberseguridad bajo las ordenes de un equipo con una formación adecuada ayuda a la protección de la planta y por tanto, evitar los peores escenarios posibles.

5. Evaluación de la metodología: caso práctico y validaciones de experto.

En el presente caso de aplicación, se expone una situación que podría darse en una compañía del sector industrial, sirve de utilidad para observar los pasos a seguir para la implementación de la metodología NUTRIA.

El objetivo fundamental del caso de aplicación trata de mostrar un marco de trabajo en el cual se van desarrollando y cerrando los escenarios que surgen en función de las características de la compañía.

De este modo, el caso de aplicación ha de servir como guía para el cumplimiento con las especificaciones definidas anteriormente.

5.1 Caso de aplicación de la metodología NUTRIA en una compañía.

5.1.1 Estudio inicial de la compañía de mecanizado

Una empresa de mecanizado, capaz de atender fabricaciones en serie de componentes mecánicos de alta complejidad y elevada precisión para piezas de aluminio, acero inoxidable, titanio, plásticos técnicos y otro tipo de aleaciones no férricas pretende adaptar sus procesos y tecnologías a la Industria 4.0.

De este modo, la compañía ha decidido implementar una metodología de mejora continua en la planta, realizar acciones formativas a todos los roles involucrados en la producción para tomar conciencia de la nueva era que la compañía comienza, así como la incorporación de nuevas tecnologías que permitan incrementar la autonomía y la producción de la compañía.

En primer lugar, se parte de la recopilación de la información, a través de entrevistas con el personal de la empresa de mecanizado, punto de partida para el análisis e implementación de ciberseguridad.

La siguiente tabla, muestra una síntesis del estudio realizado en la planta, a través de la realización de cuestionarios de seguridad como el ANEXO I, así como, documentación por parte de la compañía.

Tabla 2. Síntesis información obtenida. Fuente: elaboración propia

INFORMACION SOLICITADA	APORTADO (SI/NO/PARTE)
Esquemas de red.	SI
Inventario de los diferentes sistemas involucrados, tanto TI como TO.	SI
Planes de direccionamiento en la interconexión de redes.	SI
Políticas y procedimientos: contratación, formación continua, auditoria interna, reevaluación y revisión de las políticas.	PARTE
Información, esquemas, planos de la instalación.	SI
Comunicación y distribución con terceras partes.	SI
Histórico de seguridad de la compañía.	SI
Procedimientos de actuación en caso de incidentes.	NO

La implementación de la metodología se inicia identificando diferentes áreas de proceso dentro del **Sistema Bajo Consideración**:

- **Fabricación:** El taller de mecanizado cuenta con tornos de cabezal móvil, tornos automáticos de decoletaje, tornos multitarea con herramientas mecanizadas ofreciendo alta precisión y cortes ajustados, para reducir necesidades de manipulación y operaciones secundarias.

- **Acabado y Calidad:** Tras el proceso de mecanizado de la pieza, la compañía cuenta con procesos como el cincado, galvanizado, pintura, anodizado, pulido, chorreado con circonio, micro-esfera de vidrio o corindón, tratamientos térmicos, electro-pulido y pasivado.

- **Almacenamiento:** Una vez acabadas la piezas, son almacenadas para transportarlas al cliente final, embaladas y etiquetadas apropiadamente.

- **Gestión de stock y red corporativa de la empresa:** Los procesos de gestión de stock, ventas, compras e inventario de materiales son realizadas en está área de proceso.

A continuación, se muestra la situación inicial a nivel de red de la planta, se trata de una única red corporativa que ofrece servicio a todos los servicios y procesos de la planta. Así, la topología utilizada es de anillo central, a través de toda la planta, contando con un enrutador de tráfico de capa 3.

Por otro lado, la segmentación lógica se encuentra implementada utilizando VLAN teniendo en cuenta la posibilidad de gestión de los switches que forman parte del anillo. Así, de los switches centrales dependen otros switches de acceso de capa 2 (no son descritos en la figura por simplificar la representación).

Dentro de las diferentes áreas de proceso, PLCs y sistemas HMI están vinculados a las fases anteriormente descritas para la supervisión y control de los procesos. Además, existe un centro de control con un sistema SCADA desplegado para la supervisión y control de los procesos de fabricación.

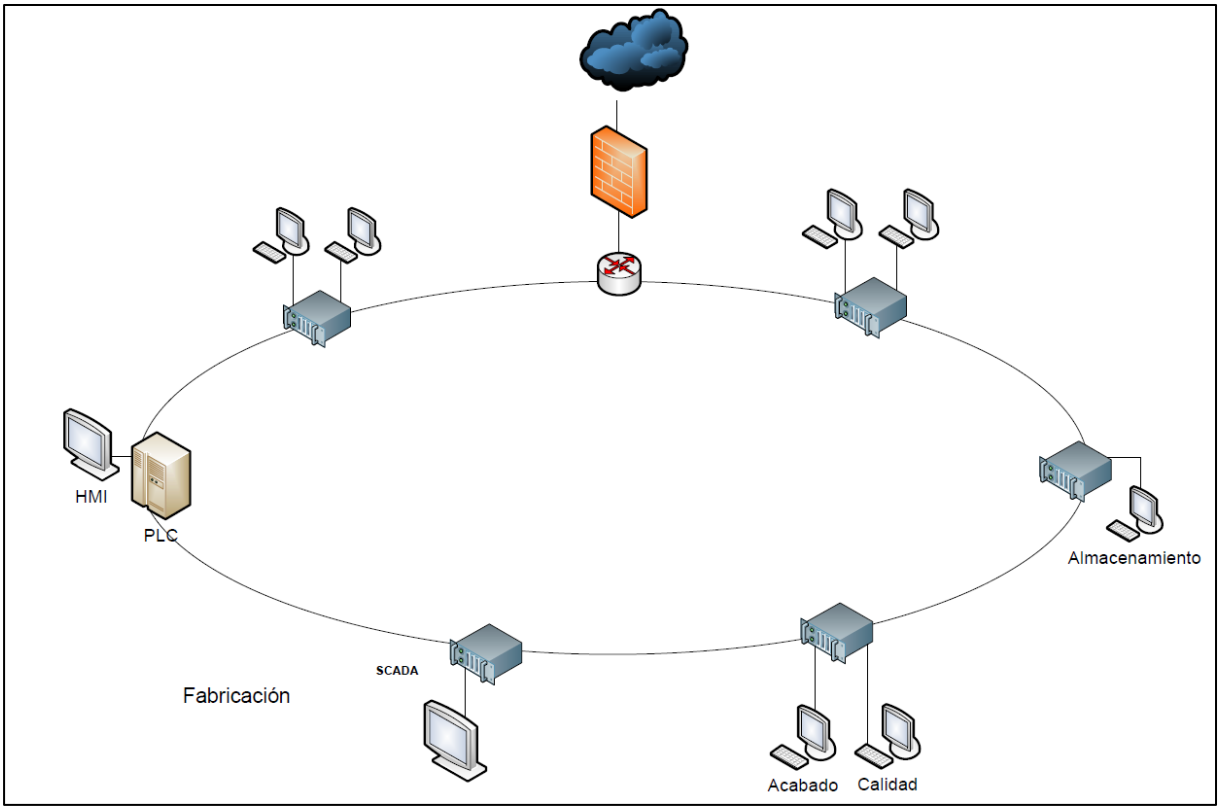

Figura 17. Situación inicial de la compañía de mecanizado, Fuente: elaboración propia.

El rendimiento de la compañía, debido a la existencia de una única red multi-servicio, se ha visto afectado en relación a la estimación temporal de los procesos de fabricación. La compañía cuenta con un cortafuegos con firmas activadas para la detección de intrusos. De este modo, se reduce el riesgo de malware o denegación de servicio.

Sin embargo, se ha de tener en cuenta que la inexistencia de segmentación física, podría producir un ataque mediante phising como vector de ataque o uso de algún dispositivo extraíble la infección de la red que se propagaría de forma inmediata y afectaría a toda la red de la empresa.

5.1.2 Propuesta de mejora

Una vez se ha definido el contexto de la fabrica, se procede a la identificación de las zonas y conductos siguiendo los aspectos y recomendaciones fijadas por la metodología basada en la IEC 62443. Así, tras la realización de la correspondiente evaluación de riesgos se procede al establecimiento de tres zonas diferenciadas.

ZONA 1: Zona TI con los activos TI, así como gestores transaccionales del tipo ERP o CRM, para mantener bases de datos en un estado conocido, centro de datos corporativo, estaciones de trabajo, etc. Cuenta con segmentación física de red, además de cortafuegos separando la Zona 1 de Zona 2.

CONDUCTO 1 en ZONA 1: Se trata de la red TI, además de canal de confianza entre zona 1 y zona 2 donde están incluidos los activos cuya información tiene que ser compartida entre la zona 1 y la zona 2. De este modo, dicho conducto esta formado por un dispositivo de enrutamiento y diferentes switches gestionables.

ZONA 2: Zona desmilitarizada o DMZ, se trata de la red intermedia entre las dos redes principales, es establecida entre dos cortafuegos con objetivo de evitar el tráfico y acceso entre las dos redes principales, pero permitiendo el flujo de información seguro entre ellas.

Dicha zona incluye un servidor de aplicación MES para la gestión de las funciones de lógica de negociación y de acceso a los datos de las aplicaciones y el servidor que tiene una réplica del entorno Cloud para hacer mas eficiente el acceso y consulta de datos de los procesos de producción.

CONDUCTO 2 en ZONA 2: Dicho conducto trata de la red DMZ, formado por dos switches gestionables de capa 2.

ZONA 3: Teniendo en cuenta las diferentes operaciones que se llevan a cabo en la compañía se establecen sub-zonas en función de los procesos llevados a cabo y los requisitos de seguridad que requieren. De este modo se procede a establecer tres sub-zonas:

- **Sub-zona Fabricación:** Contempla los activos correspondientes al proceso de fabricación. Una vez realizado el análisis de riesgo, se contempla dicha sub-zona como área de procesos críticos teniendo en cuenta que cualquier alteración y/o interrupción de los procesos acarrearía perdidas económicas elevadas a la compañía.

De este modo, se procede a la incorporación de cortafuegos industriales DPI, es un cortafuegos que se despliega físicamente entre los sistemas SCADA, HMI y los dispositivos de campo como los PLCs para bloquear malware teniendo en cuenta la posibilidad de segmentación específica por protocolo industrial, como las reglas de segmentación por Funtion Codes especificas de protocolos como Modbus o Ethernet IP.

Así, se asegura la comunicación entre los PLCs y el sistema SCADA sobre el protocolo Modbus, obligando a que su realización sea siempre sobre este protocolo y la autenticación de la IP y MAC de los dispositivos.

- **Sub-zona Acabado y calidad:** Contempla el registro de datos correspondiente a las diversos controles de calidad, así como el registro de los materiales acabados que pasan a la sub-zona de almacenamiento, así como la trazabilidad del proceso de producción de cada pieza realizada.

- **Sub-zona Almacenaje**: Sub-zona encargada de la gestión de los productos finalizados, así como de la organización por pedidos, dicha información es transmitida por medio de un canal de confianza entre la Zona 2 y la Zona 3, teniendo en cuenta la necesidad de comunicación final con la Zona 1,TI de gestión corporativa.

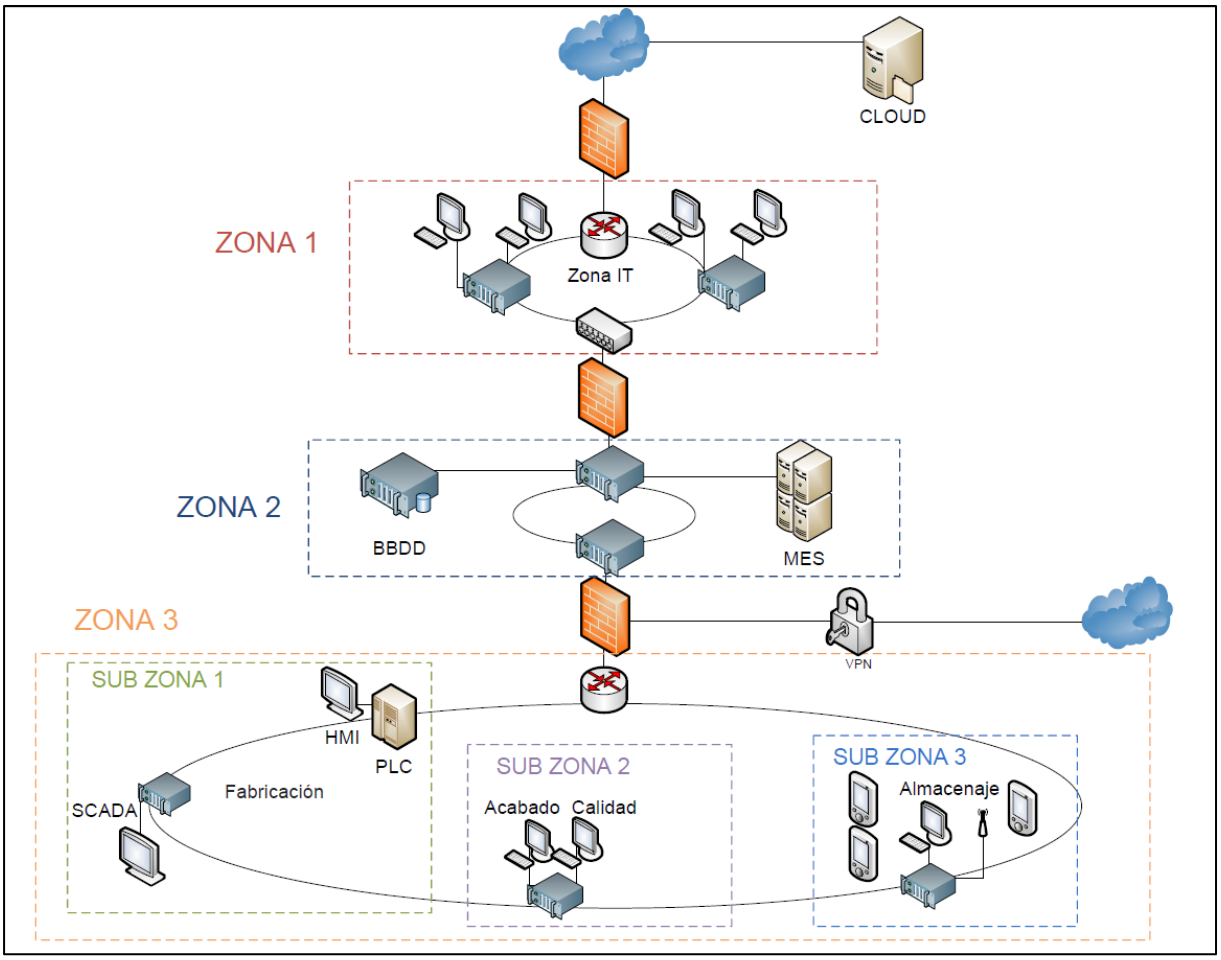

Figura 18. Establecimiento de zonas y conductos para la fabrica de mecanizado. Fuente: Elaboración propia.

Se procede a la identificación de funciones y responsables, proponiendo el siguiente organigrama, en relación a los nuevos roles establecidos en planta:

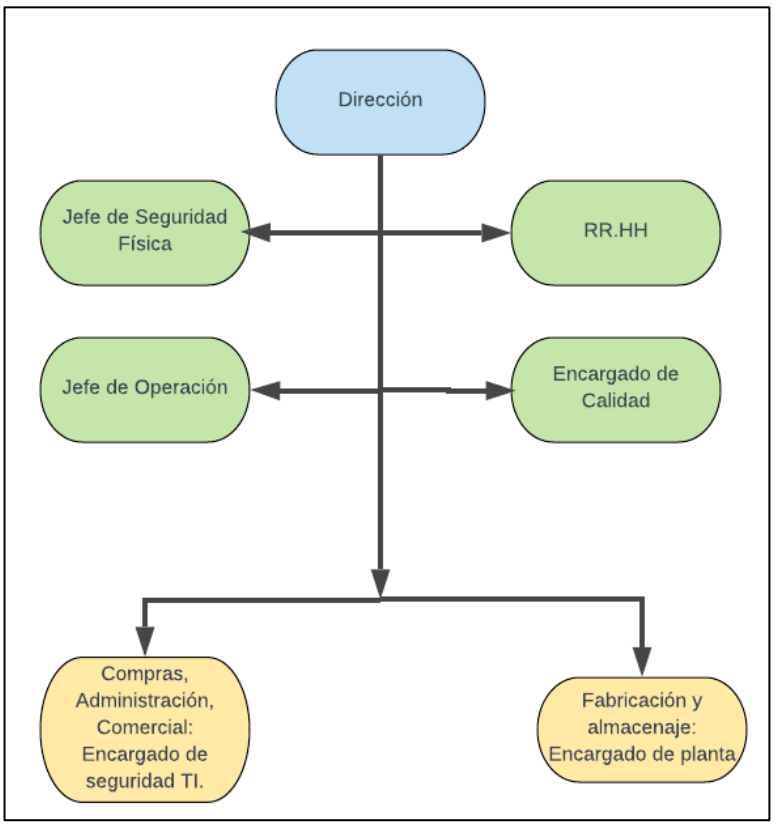

Figura 19. Organigrama empresa de mecanizado.

- **Dirección:** Responsable de la ciberseguridad de la empresa de mecanizado y del cumplimiento de las políticas definidas.

- **Jefe de Seguridad Física:** Responsable de las situaciones de riesgo, así como planificación y programación de actuaciones relacionadas con servicios de ciberseguridad. Encargado de Zona II

- **RR.HH:** Servicio subcontratado a consultoría externa, encargado de las acciones formativas, así como de la contratación de personal, con contrato de confidencialidad definido por la empresa de mecanizado, estableciendo políticas y controles de ciberseguridad.

- **Calidad:** Control y gestión de la documentación y registros del sistema de calidad, realización de auditorias internas, seguimiento de los procedimientos, así como de las no conformidades que puedan surgir. El encargado de calidad también lleva a cabo la tarea de informar a la plantilla de modificaciones o cambios que surgen en la planta y definir los contenidos, para el plan interno de formación junto con la consultoría externa.

- **Encargado de seguridad TI:** Administrador de procesos relacionados con compras, administración y área comercial, encargado del cumplimiento de políticas, estándares, normas y procedimientos establecidos por la compañía en el área TI. Encargado de Zonas I y II, así como de Conductos I y II.

- **Encargado de seguridad de planta TO:** Administrador de procesos TO en el área de fabricación, calidad y almacenaje. Encargado de Zona III y sub-Zonas I, II y III.

5.2 Validaciones de expertos

Una vez realizado el Trabajo Fin de Master: NUTRIA: "Una metodología de Ciberseguridad para Pymes en entornos industriales" para verificar la viabilidad de la metodología, expertos en el área de ciberseguridad evaluaron el trabajo realizado aportando las siguientes validaciones:

- **Gonzalo Porlán Moreno**, Ingeniero de Telecomunicaciones, especializado en redes y Sistema de Comunicación, cuenta con experiencia en el desarrollo de sistemas de comunicaciones y evaluaciones de productos IT, según la norma Common Criteria (ISO/IEC 15408), FIPS 140-2 y auditorías EMVco, participando en más de 50 proyectos.

  En la actualidad, director técnico para Common Criteria, en los laboratorios de Applus, especialistas en evaluación de seguridad de EAL1 a EAL6 tanto de software como smartcards, circuitos integrados y cajas de seguridad.

  "Con respecto a la metodología NUTRIA, se destacarán -de forma resumida- los aspectos más importantes de cada área genérica:

  - ***Identificación**: recogida en las fases I y II, describe la identificación tanto de los procedimientos existentes, como de los activos y las necesidades. Es destacable cómo dentro del análisis se incluyen aspectos concretos como es el estudio del tráfico de red con objeto de identificar los flujos principales de comunicación. Esto es especialmente relevante en la industria manufacturera, donde el tiempo de reacción es muy importante e identificar y proteger estos flujos puede suponer una ventaja estratégica.*

  - ***Actuación**: descrita en las fases III, IV y V, supone la utilización de un criterio sistemático que permite la segregación del problema en conjuntos más pequeños, contribuye a acotar las medidas de seguridad que son de aplicación para cada conjunto y ser más eficiente en la cobertura de las necesidades identificadas. Además, el considerar escenarios catastróficos (se considera que el sistema fallará y por tanto se considera la inclusión de medidas paliativas y de recuperación), lejos de suponer una desconfianza en las medidas de seguridad, supone un acercamiento al escenario más real posible y considerar todas las posibilidades.*

- ***Evaluación:*** *descrita en la fase VI, la formación se incluye como un aspecto a considerar desde el primer momento, puesto que los medios humanos suelen ser el eslabón más débil del sistema de seguridad, mientras que los medios técnicos pueden ser perfectamente conocidos y controlados. La evaluación incluye tanto evaluación del propio personal como evaluación del propio sistema y la efectividad de las medidas implementadas con respecto al análisis que se realizó para el caso.*

La definición de la metodología NUTRIA es correcta desde el punto de vista formal, puesto que incluye las fases más importantes de toda metodología. Además, esta metodología está diseñada para analizar y dar respuesta al problema concreto de la seguridad TO en la pequeña y mediana empresa, para lo que incluye los mecanismos y procedimientos necesarios para abarcar dicho problema."

Propuesta de mejora

Teniendo en cuenta que la seguridad es un aspecto cambiante, tal y como se dice en la introducción, donde van evolucionando las técnicas de ataque y defensa, se debería modificar el esquema para que fuera un esquema circular y definir un periodo de validez. Quizá estas sucesivas iteraciones se podrían contemplar como un sistema de auditorías internas que fuera más ligero que una vuelta inicial, que se entiende que se realizaría en más profundidad.

Sugiero que la metodología incluya el establecimiento de un esquema/organigrama responsable del mantenimiento y la toma de decisiones relativos a la seguridad, como resultado de la aplicación de la metodología. En ese esquema inicial se podrían identificar las responsabilidades genéricas de cada rol".

- **José A. Rivas**, matemático especializado en ciencias de la computación y seguridad informática. Actualmente es el responsable del Laboratorio de Seguridad en Madrid para Applus+ Laboratories. Ha realizado evaluaciones de seguridad a diferentes dispositivos/soluciones, principalmente bajo la norma Common Criteria.

  Presidente del Subcomité 6 integrado en el Comité Técnico Nacional 320 – Ciberseguridad y Protección de Datos Personales – en UNE y miembro activo de OWASP Madrid. Participa de otros grupos de trabajo internacionales (OWASP IoT Project, GlobalPlatform…).

  > *"La presente metodología – NUTRIA – divide a lo largo de 6 fases, las diferentes tareas que una empresa (pequeña – mediana) debe ejecutar para lograr un sistema ciber-robusto en un entorno industrial.*
  >
  > *Se describen acciones esenciales para la correcta protección de los activos de dicho sistema. Acciones que van desde el conocer tu propio sistema e identificar los distintos elementos que lo componen, análisis de vulnerabilidades, respuesta ante incidentes o recuperación ante incidentes.*
  >
  > *Todo ello contrastado bajo estándares (ISO/IEC 62443) o recomendaciones de entidades (INCIBE o CCI) del sector industrial. Lo que permite afirmar que la metodología está en línea con las demandas/intereses del sector.*

  Propuesta de mejora

  - *Atendiendo al nombre de la fase 6 – Evaluación Continua – tendría sentido modificar el diagrama de fases de la metodología para que fuera un esquema cíclico.*
  - *Según la descripción de la Fase 1 – Preparación – y la Fase 2 – Identificación y análisis del entorno – se podrían contemplar como una única fase, en lo referente a la recopilación de la información de protección de la seguridad de las instalaciones.*
  - *La fase 4 – Respuesta –Se debería considerar la realización de un análisis forense, listado y revisión de los activos afectados, mecanismos que encajarían en este tipo de situaciones.*
  - *Un check-list de auditoria basado en esta metodología podría ser un añadido de valor al trabajo."*

- **Sergio González de Castro**, Graduado en Ingeniería Informática por la Universidad Politécnica de Madrid. Cuenta con más de 5 años de experiencia profesional directa en ciberseguridad, en una gran índole de proyectos. Como referente técnico de ciberseguridad industrial de Applus+ Laboratories, ejecuta evaluaciones de sistemas y dispositivos para diversos tipos de dispositivos de control industrial, incluyendo sistemas de edificación inteligente.

  "Análisis de la metodología NUTRIA:

  - ***Identificación**: La metodología detalla las fases y pasos a tratar de una forma detallada pero flexible para poder acoger diferentes tipologías de sectores, empresas y realidades del entorno evaluado. Las técnicas de ciberseguridad para sistemas con comunicaciones más recomendables se ven reflejadas, no detectándose carencias evidentes en la misma. La criticidad de las telecomunicaciones en el mundo de Industria 4.0 se encuentra adecuadamente reflejada.*

  - ***Actuación**: el desglosado en subtareas favorece la comprensión en profundidad del sistema objetivo, realizando los debidos análisis de riesgos para establecer una protección adecuada para los distintos activos. La catalogación de activos y redes, así como la creación de un adecuado plan de continuidad de negocio, en base a la salvaguarda de los respaldos de seguridad imponen una introspección sobre la resiliencia del sistema al operador del mismo importante para garantizar la continuidad de cualquier PYME ante un ciberataque.*

  - ***Evaluación:** ejercitando la introspección, la evaluación continua permite a la PYME continuar refinando el resultado de la última iteración de NUTRIA, mejorando procesos, análisis, formaciones, y los demás aspectos de la metodología, de una forma más madura. Este acercamiento a ISO9001 en los procesos de mejora continua resulta crucial en el cambiante mundo de la ciberseguridad, y permite asumir los cambios que pueda traer la adopción de la industria 4.0.*

  La acertada aproximación a los elementos más distinguidos de otras metodologías permiten a NUTRIA gozar de una robustez poco habitual para una metodología naciente.

Propuesta de mejora

1. *Una propuesta que aumentaría la usabilidad de la metodología sería el incluir una evaluación completa de un sistema, con todos los componentes y sub-fases. Esto permitiría a PYMES con recursos más limitados intentar comprender el valor de la metodología, y permitir que se comprendan conceptos que pueden ser más complejos para implementadores poco versados en ciberseguridad,*
2. *En línea con la propuesta anterior, la inclusión de unas plantillas para los elementos más reiterativos sería de interés para las PYMES que adopten la metodología, simplificando el proceso inicial de tareas como pueda ser el inventariado, los planes de formación, esquemas y direccionamientos de red, y otros similares.*

6. Conclusiones y trabajo futuro

6.1 Conclusiones

En la actualidad, están siendo desarrolladas e implementadas numerosas iniciativas de ciberseguridad para las Tecnologías de la Información, no tantas en relación a los sistemas de control industrial, a nivel nacional o bien por medio de diferentes instituciones.

Si además se contempla el direccionamiento tecnológico de la industria, tanto a nivel de grandes empresas como la pequeña y mediana empresa, hacia la hiper-conectividad, donde se observa el retraso en relación a la protección de sistemas industriales con respecto a las tecnologías de la información.

En muchas compañías, los sistemas industriales no fueron diseñados contemplando su conexión a internet, con la llegada de la Industria 4.0, las empresas del sector industrial deben conocer y tener consciencia, de los riesgos y pérdidas económicas que acarrea un ciberataque.

Además, deben obtener los medios para implementar medidas de ciberseguridad para el objetivo principal del entorno industrial, prevenir, monitorizar y mejorar la resiliencia de los sistemas industriales ante acciones hostiles y/o optimizar la resiliencia ante amenazas en la producción.

Así, las lecciones aprendidas mediante la realización de la metodología, han quedado centradas, en el estudio de iniciativas de protección sobres sistemas industriales y la relación entre las tecnologías de la información y las tecnologías de operación, para la realización de un método, basado en estándares aplicables vigentes, que permita implementar medidas de ciberseguridad eficaces y eficientes en la Pequeña y Mediana Empresa.

6.1.1 Contribución realizada

A continuación, se resaltan las principales aportaciones realizadas en este trabajo de investigación:

En el **Capítulo II** se expone el análisis del estado del arte actual, en relación a la ciberseguridad en los Sistemas de Control Industrial, así como de las PYMES en entornos industriales, en relación al conocimiento e implementación de medidas de ciberseguridad, contemplando los ataques específicos en el área de las Tecnologías de la Operación y los estándares, normativa y buenas prácticas publicadas hasta el momento.

El **Capítulo IV** constituye el núcleo central de las aportaciones realizadas, definiendo una metodología que permite a las PYMES, adelantarse a la problemática que conlleva la implementación de la Industria 4.0 en las compañías del sector industrial que carecen de medidas de ciberseguridad en gran parte.

Ante este riesgo, las PYMEs necesitan adelantarse al problema proactivamente, ya que si se actúa una vez la seguridad de la empresa ha sido comprometida, el coste económico será mucho mayor debido a la pérdida de disponibilidad.

Así, mediante la implementación de la metodología NUTRIA se definen una serie de fases a realizar, tomando como punto clave para su implementación, el conocimiento por parte de trabajadores y propietarios, de cuál es la realidad a la que se enfrentan, así como técnicas, controles y modificaciones para evitar y/o mitigar ataques y/o incidencias.

Partiendo de los fundamentos teóricos expuestos en el estado del arte y tomando como referencia el marco NIST, para la gestión de la ciberseguridad industrial, se construyó una metodología que permite servir de guía para la implementación de un modelo de ciberseguridad industrial para la pequeña y media empresa.

La metodología NUTRIA consta de seis fases diferenciadas:

- **Fase I: Preparación:** Realización del estudio previo para obtención de conocimiento del estado del entorno de la compañía y su seguridad, la información es validada mediante una visita a las instalaciones. En esta fase se obtiene la información relacionada con: Funciones y responsabilidades actuales, procedimientos, nivel de formación tanto de empleados como de gerencia, planos de la instalación así como, toda información de valor para proceder al análisis.

- **Fase II: Identificación y análisis:** Tras la obtención de la información en la FASE I, se procede a identificar el "Sistema bajo Consideración", como la infraestructura completa bajo análisis. La evaluación de la documentación existente y de los activos es llevada a cabo en esta fase, para el establecimiento de la metodología a seguir en función de la definición del "SuC".
  Así, son estudiadas funcionalidades de la ciberseguridad como la seguridad física, el tráfico entre los activos definidos y el análisis de las amenazas y vulnerabilidades del sistema a proteger. Una vez se obtiene la evaluación global, son definidos los nuevos roles y responsabilidades así como la formación del personal en el nivel que sea necesario.

- **Fase III: Defensa y detección:** El análisis realizado ofrece unos resultados para implementar las técnicas de protección en función de la empresa, bajo el contexto de zonas y conductos definido por ISA99/IEC6443 (IEC, 2013). Son ofrecidas recomendaciones para la detección de incidencias relacionadas con eventos de ciberseguridad.

- **Fase IV: Respuesta:** La fase de respuesta queda centrada en buenas prácticas y controles para la realización de copias de seguridad de los sistemas bajo protección, teniendo en cuenta el carácter industrial de estas compañías, la prioridad siempre es el trabajo con máquinas y dispositivos, es decir, la disponibilidad de estos. Por tanto, la obtención de copias de seguridad de estados anteriores, para la recuperación en caso de perdida de disponibilidad cobra una gran importancia.

- **Fase V: Recuperación:** La recuperación queda centrada en la resiliencia de la empresa, es decir, en la capacidad que debe adquirir para adaptarse y continuar con sus funciones en situaciones de riesgo. Esta fase estudia como se ha de actuar y gestionar las situaciones de forma eficiente para optimizar el rendimiento de la compañía en caso de ataque o incidente.

- **Fase VI: Evaluación Continua:** La última fase define la auto evacuación que debe realizar la compañía una vez implementada la metodología, para analizar regularmente los controles y medidas establecidas teniendo en cuenta el avance de las tecnologías actuales, por lo que la metodología deberá de ir adaptándose a las necesidades de la compañía.

6.1.2 Validación de la metodología

Para la corroboración de la metodología, se acudió a la validación de expertos en ciberseguridad, que evaluaron la metodología para identificar las habilidades y competencias del modelo expuesto, sirviendo de consideración ante las necesidades del sector industrial.

Las validaciones obtenidas refuerzan el modelo a implementar, los expertos mediante el estudio de las fases definidas en la metodología, realizaron una aportación formal contemplando los puntos de valor, así como las mejoras que podrían realizarse, obteniendo un veredicto final positivo por parte de los tres expertos que han participado en la evaluación de NUTRIA.

Por otro lado, fue realizado un caso de aplicación contemplando dicha actividad como una técnica para la captura de los requisitos potenciales de la nueva metodología, proporcionando un escenario de una compañía de mecanizado en el que se indica cómo se debería actuar para conseguir los objetivos específicos definidos en la metodología NUTRIA.

De este modo, mediante un caso de uso que contempla una secuencia de iteraciones entre el sistema bajo estudio y los roles implicados, se pudo establecer un caso práctico para ilustrar los requerimientos de la metodología y cómo reacciona ante diferentes situaciones en función de los controles y requerimientos establecidos en la compañía.

De este modo, validar de modo práctico teórico las capacidades de la metodología NUTRIA como sistema para implementar y/o optimizar controles de seguridad en la pequeña y mediana empresa.

6.2 Líneas de trabajo futuro

Como trabajo futuro a desarrollar, se llevará a cabo la implementación de la metodología descrita por parte de una compañía (PYME) como prueba práctica, implementando cada una de las fases propuestas de la metodología NUTRIA, así como la obtención de información sobre la implantación, análisis, éxitos y mejoras para la optimización de la misma.

En base a las recomendaciones de los expertos, una vez haya sido implementada la metodología, será mejorado el esquema en función de los resultados obtenidos, para la creación de un esquema circular definiendo un periodo de validez del mismo.

Por otro lado, la optimización del establecimiento de esquema/organigrama para la identificación de responsabilidades, variará en función de la industria bajo estudio, una vez hayan sido realizadas varias implementaciones de la metodología, serán optimizadas las funciones y responsabilidades catalogándolas en función de la industria evaluada y los resultados obtenidos.

Además, será llevado a cabo el desarrollo o adaptación de los controles de ciberseguridad de la metodología, de cara a que la compañía que la implemente, obtenga el conocimiento exhaustivo de los controles de ciberseguridad que podría llevar a cabo sin recurrir a otras guías, mediante la metodología NUTRIA.

Otra de los trabajos futuros que pueden llevarse a cabo, son la creación de un foro donde las diferentes empresas del sector comparten experiencias en relación a la metodología NUTIRA, así como propuestas de mejora.

La implementación de un software mecanizado de seguimiento para las compañías, pudiendo así, monitorizar los controles implementados periódicamente, para la realización de modificaciones, acciones correctivas o preventivas basadas en datos de la planta.

Además, siguiendo las recomendaciones de mejora obtenidas en la sección **5.2 Validaciones** de expertos será incluida una evaluación completa de un sistema, con todos los componentes y sub-fases.

Por otro lado, se contrastará la implementación de la metodología NUTRIA en Pymes contra grandes empresas, para poder obtener una validación de hasta donde es capaz de implementarse la metodología, que necesita incrementar o mejorar.

Una vez la metodología adquiera madurez, se estudiará la aplicación de la misma en Smart City o Ciudades Inteligentes, teniendo en cuenta que, éste nuevo modelo de ciudad obliga a que elementos de urbanismo, infraestructuras, transportes y servicios evolucionen a plataformas inteligentes.

De este modo, se trata de ciudades instrumentadas que cuentan con una compleja red de sensores mediante los cuales es recabada información para el análisis y control de los sistemas, con necesidad de implementar medidas de ciberseguridad.

7. Bibliografía

Verizon. (2018). 2018Data Breach Investigations Report.

Williams, T. J. *The Purdue Enterprise Reference Architecture and Methodology (PERA)*. Institute for Interdisciplinary Engineering Studies Purdue University 1293 Potter Center, West Lafayette, IN 47907-1293 USA,.

UNE ISO/IEC 27001:2013. (2014). *UNE ISO/IEC 27001:2013*. AENOR. Madrid: AENOR

Ayerbe, A. (12 de Marzo de 2019). *www.realinstitutoelcano.org*. Recuperado el 25 de junio de 2019, de www.realinstitutoelcano.org/wps/portal/rielcano_es/contenido?WCM_GLOBAL_CONTEXT=/elcano/elcano_es/zonas_es/ari33-2019-ayerbe-hablemos-de-la-ciberseguridad-industrial

Ackerman, P. (2017). *Industrial Cibersecurity*. Packt.

Bill Lydon, I. (2019). *Reference Architectural Model for Industrie 4.0*. Obtenido de https://www.isa.org/intech/20190405/

Caldentey, D. (05 de Febreto de 2019). Por qué la ciberseguridad en la Industria 4.0 ya es tan necesaria y estratégica. *unirrevista* .

CCI. (2019). *Centro de Ciberseguridad Industrial*. Obtenido de https://www.cci-es.org/

CCI. (2019). *El Centro de Ciberseguridad Industial*. Obtenido de https://www.cci-es.org/mision

CCI. (2014). *Guía para la construcción de un SGCI, Sistema de Gestión de la ciberseguridad industrial 2014*. Guia, CCI.

CISCO. (Febrero de 2018). Cisco 2018. Reporte Anual de Ciberseguridad. *Reporte* .

CISCO. (2018). *Pequeño y poderoso. Cómo fortifica el mercado de empresas medianas y pequelas sus defensas contra las amenzas actuales*.

Europea, C. (2013). *Estrategia de ciberseguridd de la Unión Europea: Un ciberespacio abierto, protegido y seguro*. Consejo de la Unión Europea, Bruselas.

ENISA. (2019). Obtenido de https://www.enisa.europa.eu/about-enisa

ENISA. (2011). *Protecting Industrial Control Systems*. ENISA.

IEC. (2013). Industrial communication networks - Network and system security - Part 3-3: System security requirements and security levels. En IEC, *IEC 62443-3-3:2013* .

IEC. (2010). ISA/IEC 62443-2-1 Establishing an IACS Security Program.

INCIBE. (31 de Marzo de 2015). Recuperado el 2019 de abril de 24, de La importancia de las copias de seguridad de tus datos : https://www.incibe.es/protege-tu-empresa/blog/importancia-copias-seguridad

INCIBE. (15 de Septiembre de 2015). *Amenazas en los Sistemas de Control Industrial*. Recuperado el 18 de Marzo de 2019, de https://www.incibe-cert.es/blog/amenazas-sci

INCIBE. (08 de Abril de 2016). *BlackEnergy y los sitemas críticos*. Recuperado el abril de 2019, de INCIBE: https://www.incibe-cert.es/blog/blackenergy-sistemas-criticos

INCIBE. (15 de Octubre de 2015). *Ciberseguridad en la Industria 4.0*. Recuperado el 24 de marzo de 2019, de https://www.incibe-cert.es/blog/ciberseguridad-industria-4-0: https://www.incibe-cert.es/blog/ciberseguridad-industria-4-0

INCIBE. (13 de Julio de 2015). *Diferencias entre TI y TO*. Recuperado el 23 de Mayo de 2019, de https://www.incibe-cert.es/blog/diferencias-ti-to: https://www.incibe-cert.es/blog/diferencias-ti-to

INCIBE. (25 de Agosto de 2015). IEC 62443: Evolución de la ISA 99. *Blog INCIBE* .

INCIBE. (04 de Julio de 2018). *Tendencias en la industria, mejoras en la ciberseguridad*. Recuperado el 23 de abril de 2019, de https://www.incibe-cert.es/blog/tendencias-industria-mejoras-ciberseguridad: https://www.incibe-cert.es/blog/tendencias-industria-mejoras-ciberseguridad

ISA. (2019). *ISA99, Industrial Automation and Control Systems Security*. Obtenido de https://www.isa.org/isa99/

Jay Lee, B. B. (2015). A Cyber-Physical Systems arquitecture for Industry 4.0-based manufacturing systems. NSF Industry/University Cooperative Research Center on Intelligent Maintenance Systems (IMS), University of Cincinnati, Cincinnati, OH, United States.

Kushner, D. (26 de Febrero de 2013). The Real Story of Stuxnet. *IEEESPECTRUM* .

Nelson, N. (2016). *The Impact of Dragonfly Malware on Industrial Control Systems*. SANS Institute. Information Security Reading Room. SANS.

NIST. (2015). *Guide to Industrial Control Systems (ICS) Security*. Special Publication 800-82, USA, U.S Department of Commerce.

NIST. (16 de Abril de 2018). *Marco para la mejora de la seguridad cibernética en infraestructuras críticas*. Obtenido de https://www.nist.gov/sites/default/files/documents/2018/12/10/frameworkesmellrev_20181102mn_clean.pdf

MAPFRE. (30 de Enero de 2019). ¿Qué importancia tiene la ciberseguridad en la Industria 4.0?

Marcelo Guato Burgos, P. V. (20 de Febrero de 2019). Un breve resumen de los que son los CPS (Cyber Physical Systems) sus implicaciones y los desafíos futuros. *https://www.ticportal.es/expert/cps-cyber-physical-systems-implicaciones-desafios-futuros* .

Martín, M. F. (11 de Marzo de 2016). Por qué debe plantearse la convergencia entre sistemas OT e IT. *Computerworld* .

Mathias Uslar 1, S. R. (2019). *Applying the Smart Grid Architecture Model for Designing and Validating System-of-Systems in the Power and Energy Domain: A European Perspective*. Energies .

McAfee. (2016). *www.mcafee.com*. Obtenido de https://www.mcafee.com/enterprise/es-mx(assets/executive-summaries/es-hacking-skills-ahortage.pdf

PIC. (2011). *Ley 8/2011, por la que se establecen medidas para la protección de las infraestructuras críticas*. Jefatura del Estado. BOE.

Ralf Spenneberg, M. B. (2016). *Blackhat*. Recuperado el 2019, de https://www.blackhat.com/docs/us-16/materials/us-16-Spenneberg-PLC-Blaster-A-Worm-Living-Solely-In-The-PLC-wp.pdf: https://www.blackhat.com/docs/us-16/materials/us-16-Spenneberg-PLC-Blaster-A-Worm-Living-Solely-In-The-PLC-wp.pdf

Roccia, T. (08 de Noviembre de 2018). *Triton Malware Spearheads Latest Generation of Attacks on Industrial Systems*. Recuperado el 23 de Febrero de 2019, de McAfee: https://securingtomorrow.mcafee.com/other-blogs/mcafee-labs/triton-malware-spearheads-latest-generation-of-attacks-on-industrial-systems/

Symantec Security Response. (2011). W32.Stuxnet Dossier. *https://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/w32_stuxnet_dossier.pdf , 1.4*.

SANS INSTITUTE. (2019). *ICS Layered Threat Modeling*.

8. ANEXO I: CUESTIONARIO DE CIBERSEGURIDAD INDUSTRIAL

CUESTIONARIO DE CIBERSEGURIDAD INDUSTRIAL

Entidad: _____

Nombre: _____ **Cargo:** _____ **Fecha:** _____

Firma: _____

Con el siguiente cuestionario se pretende obtener información sobre el alcance de la evaluación de los controles y políticas establecidas en la compañía relacionadas con la ciberseguridad. De este modo, se parte de la documentación e información con la que cuenta la empresa con el fin de optimizar la evaluación para la implementación de la metodología de protección de entornos industriales.

INVENTARIO DE DISPOSITIVOS (hardware)	
PREGUNTAS	**RESPUESTAS**
¿Existe inventario?	
Información que aporta: identificación, política, propiedad del activo, ubicación, equipamiento de red	
Actualización: Fecha y periodicidad de la actualización	
Trazabilidad del activo desde su entrada en producción	
Roles involucrados: realización, edición y aprobación	
¿Existe inventario por zona y/o conducto?	
Políticas de detección y/o restricción	

de acceso a dispositivos físicos	
Política de gestión y mantenimiento de inventario	
Comentarios	

INVENTARIO SOFTWARE	
PREGUNTAS	**RESPUESTAS**
¿Existe inventario?	
Información que aporta: identificación, política, propiedad del activo, ubicación, equipamiento de red	
Relación entre inventario hardware y software	
Trazabilidad del activo desde su entrada en producción	
Roles involucrados: realización, edición y aprobación	
¿Existe inventario por zona y/o conducto?	
Políticas de detección y/o restricción de acceso a dispositivos físicos	
Política de gestión y mantenimiento de inventario	
Guías de instalación y bastionado	
Herramienta para impedir instalar software no autorizado: nombre, fabricante y versión	
Política de revisión de software	
Política de instalación segura	
Comentarios	

ANALISIS Y REMEDIACION DE VULNERABILIDADES	
PREGUNTAS	**RESPUESTAS**

¿Se dispone de herramientas para identificación de vulnerabilidades?	
Conocimiento de los anuncios de defectos de fabricante	
Periodicidad del análisis de vulnerabilidades	
Política para análisis y resolución de vulnerabilidades y/o defectos de seguridad	
Plazo de resolución de defectos y seguimiento	
Política de parcheo	
Herramientas de parcheo	
Comentarios	

PERMISOS DE ADMINISTRACIÓN Y/O OPERACION	
PREGUNTAS	RESPUESTAS
Política de gestión de privilegios	
Restricción de privilegios según necesidad de conocer	
Inventario cuentas administración	
Uso de contraseñas por defecto	
Acceso a internet	
Política de cuentas, ¿Cuentas nominativas?	
Política de control de accesos, físicos y lógicos	
Política de registro de actividad TO y TI	
Mecanismos de autenticación: Para las cuentas de administración, si se utilizan contraseñas (longitud mínima, vigencia máxima y mínima, requerimientos de complejidad, histórico de contraseñas recordadas)	

Auditoria y control del uso de las cuentas con privilegios: registro de actividad, alertas automáticas, mecanismos de los administradores para evitar que los propios administradores modifiquen registros.	
Comentarios	

MANTENIMIENTO Y MONITORIZACIÓN (REGISTROS DE INFORMACIÓN)	
¿Cómo se registra la actividad de los sistemas?	
¿Quién es el encargado de los registros?	
¿Qué información aporta el registro?	
¿Quedan registradas las actividades exitosas como las que no lo son?	
¿Dónde se almacenan los registros?	
¿Quién tiene acceso?	
¿Se realizan copias de seguridad de los registros?	
Comentarios	

DISPOSITIVOS REMOVIVLES, USO Y CONFIGURACIÓN SEGURA	
¿Procedimiento de bastionado de los sistemas previo a su entrada en operación?	
¿Qué tipo de dispositivos están permitidos?	
Antes de puesta en servicio de nuevos sistemas, ¿Se realiza análisis de vulnerabilidades,	

pruebas de penetración?	
¿Se realizan pruebas periódicas para la verificación de que la configuración actual no ha sufrido modificaciones no autorizadas?¿Monitorización en tiempo real?	
Comentarios	

CUMPLIMIENTO DE LA NORMATIVA LEGAL VIGENTE	
¿Se dispone de políticas de seguridad documentadas?	
¿Han sido asignados roles y responsabilidades en función del área de la compañía a tratar en aspectos de seguridad?	
¿Se cuenta con registros de entrada y salid de diferentes áreas bajo evaluación, ordenes de trabajo y procedimientos que ofrecen trazabilidad en relación a la actividad realizada en planta.	
Comentarios	

Calificación final

9. ANEXO II: Infografía metodología NUTRIA.

"Una metodología de Ciberseguridad para Pymes en entornos industriales"

Fase I

PREPARACIÓN

- Conocimiento del entorno
- Identificación de funciones y responsabilidades
- Formación y sensibilización con la ciberseguridad industrial

Fase II

IDENTIFICACIÓN Y ANÁLISIS

- ¿Qué es necesario proteger?
- Análisis de la información documentada
- Estudio de activos TI y TO, interconexión y diferencias
- Análisis de amenazas y vulnerabilidades en Sistemas Industriales
- Evaluación de riesgo

Fase III

DEFENSA Y DETECCIÓN

- Establecimiento de Zonas y Conductos
- Recomendaciones para la detección de incidencias

Fase IV

RESPUESTA

- Copias de seguridad para asegurar la disponibilidad
- Repercusión de la pérdida de información en la continuidad de negocio

Fase V

RECUPERACIÓN

- Proceso de recuperación
- Ciberresiliencia, ¿Cómo obtenerla?

Fase VI

EVALUACIÓN CONTINUA

- Recomendaciones para la autoevaluación

10. ANEXO III: Glosario, términos, acrónimos y definiciones.

Término	Definición
Anodizado	Se denomina anodización al proceso electrolítico de pasivación utilizado para incrementar el espesor de la capa natural de óxido en la superficie de piezas metálicas.
Antitampering	Controles a prueba de manipulación que dificulta a un atacante implementar modificaciones.
APT	Una amenaza persistente avanzada, también conocida por sus siglas en inglés, APT (por Advanced Persistent Threat), es un conjunto de procesos informáticos sigilosos y continuos, a menudo orquestados por humanos, dirigidos a penetrar la seguridad informática de una entidad específica.
Big Data	Los macrodatos, también llamados datos masivos, inteligencia de datos, datos a gran escala o big data (terminología en idioma inglés utilizada comúnmente) es un término que hace referencia al concepto relativo a conjuntos de datos tan grandes y complejos como para que hagan falta aplicaciones informáticas no tradicionales de procesamiento de datos para tratarlos adecuadamente.
Botnet	Término que hace referencia a un conjunto o red de robots informáticos o bots, que se ejecutan de manera autónoma y automática. El artífice de la botnet puede controlar todos los ordenadores/servidores infectados de forma remota.
Bots	Un bot (aféresis de robot) es un programa informático que efectúa automáticamente tareas repetitivas a través de Internet, cuya realización por parte de una persona sería imposible o muy tediosa
BYOD	Bring your own device («trae tu propio dispositivo» en inglés), abreviado BYOD, es una política empresarial consistente en que los empleados lleven sus propios dispositivos personales (portátiles, tabletas, móviles…) a su lugar de trabajo para tener acceso a recursos de la empresa tales como correos electrónicos, bases de datos y archivos en servidores así como datos y aplicaciones personales.
CCI	Centro Cibeseguridad Industrial.

Chip	Circuito integrado.
Ciber-delincuencia	Cualquier tipo de actividad en la que se utilice Internet, una red privada o pública o un sistema informático domestico con objetivos como destruir o dañar ordenadores, medios electrónicos y redes de Internet
Ciberamenzas	Uso de la red, los teléfonos móviles u otras tecnologías telemáticas para intimidar a otro con el anuncio de la provocación de un mal grave para él o su familia.
Cibercrimen	Delito informático, delito cibernético o ciberdelito es toda aquella acción antijurídica que se realiza en el espacio digital o de internet. Ante el extendido uso y utilización de internet en todas las esferas de la vida (economía, cultura, industria, ciencia, educación, información, comunicación etc) y el creciente número de usuarios, la delincuencia también se ha expandido a esta dimensión.
Ciberdelencuencia	cualquier tipo de actividad en la que se utilice Internet, una red privada o pública o un sistema informático domestico con objetivos como destruir o dañar ordenadores, medios electrónicos y redes de Internet.
Cincado	El cincado es el recubrimiento de una pieza de metal con un baño de zinc para protegerla de la oxidación y de la corrosión, mejorando además su aspecto visual.
Cloud	La computación en la nube, conocida también como servicios en la nube, informática en la nube, nube de cómputo, nube de conceptos o simplemente «la nube», es un paradigma que permite ofrecer servicios de computación a través de una red, que usualmente es Internet.
CMM	El Modelo de Madurez de Capacidades o CMM (Capability Maturity Model), es un modelo de evaluación de los procesos de una organización.
CPS	Un sistema ciberfísico es un mecanismo controlado o monitorizado por algoritmos basados en computación y estrechamente integrados con internet.

Crimeware	Crimeware es un tipo de software que ha sido específicamente diseñado para la ejecución de delitos financieros en entornos en línea.
CRM	La customer relationship management, más conocida por sus siglas CRM, puede tener varios significados: Administración basada en la relación con los clientes, un modelo de gestión de toda la organización, basada en la satisfacción del cliente.
CVSS	El sistema de puntuación de vulnerabilidad común es un estándar de la industria libre y abierto para evaluar la gravedad de las vulnerabilidades de seguridad del sistema informático.
DCOM	El Modelo de Objetos de Componentes Distribuidos es una tecnología propietaria de Microsoft para desarrollar componentes de software distribuidos sobre varias computadoras y que se comunican entre sí.
DCS	Un Sistema de procesos Distribuido o SCD, más conocido por sus siglas en inglés DCS, es un sistema de control aplicado a procesos industriales complejos en las grandes industrias.
Decoletaje	La fabricación de piezas de revolución mecanizando material en barra o en rollo por arranque de viruta mediante una herramienta de corte y para una fabricación en serie.
Desbordamientos de búfer	Error de software que se produce cuando un programa no controla adecuadamente la cantidad de datos que se copian sobre un área de memoria reservada a tal efecto (buffer): Si dicha cantidad es superior a la capacidad preasignada, los bytes sobrantes se almacenan en zonas de memoria adyacentes, sobrescribiendo su contenido original, que probablemente pertenecían a datos o código almacenados en memoria
DFKI	Centro Alemán de Investigación para la Inteligencia Artificial
DMZ	Una zona desmilitarizada (conocida también como DMZ, sigla en inglés de demilitarized zone) o red perimetral es una red local que se ubica entre la red interna de una organización y una red externa, generalmente en Internet.

DNP3	DNP3 (acrónimo del inglés Distributed Network Protocol, en su versión 3) es un protocolo industrial para comunicaciones entre equipos inteligentes (IED) y estaciones controladores, componentes de sistemas SCADA.
DoS	Un ataque de denegación de servicio, también llamado ataque DoS (por sus siglas en inglés, Denial of Service), es un ataque a un sistema de computadoras o red que causa que un servicio o recurso sea inaccesible a los usuarios legítimos.
ERP	Los sistemas de planificación de recursos empresariales son los sistemas de información gerenciales que integran y manejan muchos de los negocios asociados con las operaciones de producción y de los aspectos de distribución de una compañía en la producción de bienes o servicios.
Ethernet IP	Protocolo de red industrial que adapta el protocolo industrial común a Ethernet estándar. n cortafuegos es la parte de un sistema informático o una red informática que está diseñada para bloquear el acceso no autorizado, permitiendo al mismo tiempo comunicaciones autorizadas.
Firewall	Un cortafuegos es la parte de un sistema informático o una red informática que está diseñada para bloquear el acceso no autorizado, permitiendo al mismo tiempo comunicaciones autorizadas.
Gusano	Malware que tiene la propiedad de duplicarse a sí mismo.
Híper-conectividad	Concepto que sintetiza la situación actual del ser humano en la cual vive conectado permanentemente a la información a través de diferentes dispositivos.
HMI	HMI (Human-Machine Interface) es una 'interfaz hombre-máquina', un panel de control diseñado para conseguir una comunicación interactiva entre operador y proceso/máquina, con la función de transmitir ordenes, visualizar gráficamente los resultados y obtener una situación del proceso/máquina en tiempo real.
ICS	Sistema de Control Industrial.

INCIBE	El Instituto Nacional de Ciberseguridad es un organismo dependiente del Ministerio de Economía y Empresa de España a través de la Secretaría de Estado para el Avance Digital.
IoT	Internet de las Cosas
Log	n informática, se usa el término log, historial de log o registro, se refiere a la grabación secuencial en un archivo o en una base de datos de todos los acontecimientos (eventos o acciones) que afectan a un proceso particular (aplicación, actividad de una red informática, etc.).
MAC	En las redes de computadoras, la dirección MAC (siglas en inglés de Media Access Control) es un identificador de 48 bits (6 bloques de dos caracteres hexadecimales (4 bits)) que corresponde de forma única a una tarjeta o dispositivo de red. Se la conoce también como dirección física, y es única para cada dispositivo.
Machine learning	El aprendizaje automático o aprendizaje automatizado o aprendizaje de máquinas (del inglés, machine learning) es el subcampo de las ciencias de la computación y una rama de la inteligencia artificial, cuyo objetivo es desarrollar técnicas que permitan que las computadoras aprendan.
Malware	El malware, en inglés, malicious software, programa malicioso, o programa maligno (también llamado badware, código maligno, softwaremaligno, software dañino o software malintencionado) hace referencia a cualquier tipo de software maligno que trata de afectar a un ordenador, a un teléfono celular u otro dispositivo.
MES	Los sistemas de ejecución de fabricación (MES, por sus siglas en inglés) son sistemas computarizados utilizados en la fabricación para rastrear y documentar la transformación de materias primas en productos terminados. MES proporciona información que ayuda a los responsables de la toma de decisiones de fabricación a comprender cómo se pueden optimizar las condiciones actuales en la planta para mejorar la producción.
Modbus	Modbus es un protocolo de comunicaciones situado en los niveles 1, 2 y 7 del Modelo OSI, basado en la arquitectura maestro/esclavo (RTU) o cliente/servidor (TCP/IP), diseñado en 1979 por Modicon para su gama de controladores lógicos programables (PLCs). Convertido en un protocolo de comunicaciones estándar de facto en la industria, es el que goza de mayor disponibilidad para la conexión de dispositivos electrónicos industriales.
NMS	Network Management System: El software de administración de red es un software que se utiliza para aprovisionar, descubrir, monitorear y mantener redes de computadoras.

OPC UA	OPC Unified Architecture es un protocolo de comunicación máquina a máquina para automatización industrial desarrollado por la Fundación OPC.
Open Platform Communications	El OPC es un estándar de comunicación en el campo del control y supervisión de procesos industriales, basado en una tecnología Microsoft, que ofrece una interfaz común para comunicación que permite que componentes de software individuales interactúen y compartan datos.
Pasivado	La pasivación es la formación de una película relativamente inerte sobre la superficie de un material, que lo enmascara en contra de la acción de agentes externos.
Phishing	Phishing, conocido como suplantación de identidad, es un término informático que denomina un modelo de abuso informático y que se comete mediante el uso de un tipo de ingeniería social, caracterizado por intentar adquirir información confidencial de forma fraudulenta
PLC	Un controlador lógico programable, más conocido por sus siglas en inglés PLC o por autómata programable, es una computadora utilizada en la ingeniería automática o automatización industrial
PYME	Pequeña y Mediana Empresa.
RBAC	En la seguridad de los sistemas informáticos, el control de acceso basado en roles o la seguridad basada en roles es un enfoque para restringir el acceso del sistema a usuarios autorizados.
Resiliente	Capacidad de los seres humanos para adaptarse positivamente a situaciones adversas.
Resina epoxy	Una resina epoxi o poliepóxido es un polímero termoestable que se endurece cuando se mezcla con un agente catalizador o «endurecedor».

Router	Se trata de un producto de hardware que permite interconectar computadoras que funcionan en el marco de una red. Su función: se encarga de establecer la ruta que destinará a cada paquete de datos dentro de una red informática.
RTU	Una Unidad Terminal Remota (UTR o, mas conocida por sus siglas en inglés, RTU) es un dispositivo basado en microprocesadores, el cual permite obtener señales independientes de los procesos y enviar la información a un sitio remoto donde se procese.
SCADA	SCADA, acrónimo de Supervisory Control And Data Acquisition es un concepto que se emplea para realizar un software para ordenadores que permite controlar y supervisar procesos industriales a distancia.
SCM	El término SCM (gestión de la cadena de suministro, del inglés Supply Chain Management) se refiere a las herramientas y métodos cuyo propósito es mejorar y automatizar el suministro a través de la reducción de las existencias y los plazos de entrega.
SD	Secure Digital (SD) es un dispositivo en formato de tarjeta de memoria para dispositivos portátiles.
Servidor proxy	Un proxy, o servidor proxy, en una red informática, es un servidor —programa o dispositivo—, que hace de intermediario en las peticiones de recursos que realiza un cliente (A) a otro servidor ©.
Servidor web	Un servidor web o servidor HTTP es un programa informático que procesa una aplicación del lado del servidor, realizando conexiones bidireccionales o unidireccionales y síncronas o asíncronas con el cliente y generando o cediendo una respuesta en cualquier lenguaje o Aplicación del lado del cliente. El código recibido por el cliente es renderizado por un navegador web.
SIS	Sistemas instrumentados de Seguridad.
SNMP v3	El Protocolo simple de administración de red o SNMP es un protocolo de la capa de aplicación que facilita el intercambio de información de administración entre dispositivos de red.

SOC	Un Centro de Operaciones de Seguridad, es una central de seguridad informática que previene, monitorea y controla la seguridad en las redes y en Internet.
Stock	Bienes poseídos por una empresa para su venta o transformación en el curso ordinario de la explotación.
Switches	Conmutador (switch) es el dispositivo digital lógico de interconexión de equipos que opera en la capa de enlace de datos del modelo OSI.
TI	Tecnologías de la Información
TO	Tecnologías de la Operación.
Troyano	En informática, se denomina caballo de Troya, o troyano, a un malware que se presenta al usuario como un programa aparentemente legítimo e inofensivo, pero que, al ejecutarlo, le brinda a un atacante acceso remoto al equipo infectado.
Virus	Un virus o virus informático es un software que tiene por objetivo de alterar el funcionamiento normal de cualquier tipo de dispositivo informático, sin el permiso o el conocimiento del usuario principalmente para lograr fines maliciosos sobre el dispositivo.
VLAN	Una VLAN, acrónimo de virtual LAN (red de área local virtual), es un método para crear redes lógicas independientes dentro de una misma red física.
WirelessHART	WirelessHART es una tecnología de redes de sensores inalámbricas basada en el Protocolo de Transductor Remoto Direccionable de Carretera.

Zigbee	Zigbee es el nombre de la especificación de un conjunto de protocolos de alto nivel de comunicación inalámbrica para su utilización con radiodifusión digital de bajo consumo, basada en el estándar IEEE 802.15.4 de redes inalámbricas de área personal.