www.ismsforum.es

Guía para la gestión de la ciberseguridad en el entorno industrial de una PYME

Una iniciativa de

isms forum

isms EUSKADI

Junio 2023

Guía para la gestión de la ciberseguridad en el entorno industrial de una PYME

AUTORES

COORDINADORES	Hugo Llanos
PARTICIPANTES	Aníbal Díaz
	Carlos Morell
	Edorta Echave
	Iago Fortes
	Itzcoatl Mendoza
	Iván Rivas
	Joan Figueras
	Joel Espunya
	Jorge Márquez
	José Israel Nadal
	José Luis Jiménez
	Ramón Ortiz
	Santi Minguito
	Santiago R. Urbano
	Vicente Campayo
REVISORES	Miembros de la Junta Directiva del Capítulo Regional de ISMS Forum Euskadi
GESTIÓN DEL PROYECTO	Beatriz García
DISEÑO/MAQUETACIÓN	Cynthia Rica Gómez

CONTENIDOS

1 CIBERSEGURIDAD INDUSTRIAL ¿NECESIDAD O MODA?

1.1 Tecnología en entornos industriales

No cabe duda de que la tecnología es el resorte que está permitiendo que el mundo cambie a un ritmo trepidante.

El entorno industrial no se encuentra fuera de esta revolución, y la aplicación de la tecnología ha permitido que los procesos de producción dispongan actualmente de unos coeficientes de rendimiento y optimización muy elevados, disminuyendo los costes y mejorando la productividad de las empresas.

A la evolución de los propios componentes físicos asociados a los procesos de fabricación, el factor fundamental que hay que sumar es la introducción generalizada de tecnología en los entornos de planta.

Si hubiera que determinar cuál es la tecnología que más ha influido para alcanzar esta situación actual, podríamos apuntar, sin lugar a duda, a la evolución de las comunicaciones. El despliegue masivo de tecnologías provenientes del mundo IT en sustitución de tecnologías propietarias de uso exclusivo en comunicaciones de campo industriales, más costosas y con un despliegue menos flexible, han agilizado la conexión de las líneas de producción, lo que ha permitido mejorar tanto su operación como la extracción de datos operacionales que permiten mejorar la efectividad de los propios procesos.

Se podría decir que se ha pasado de un escenario de "máquina isla", operada de forma manual y con un funcionamiento aislado con respecto al resto de máquinas presentes en la línea de producción, a un conjunto de máquinas interconectadas que conforman una infraestructura con altos niveles de automatización, en el que la fábrica trabaja como un conjunto armonizado, monitorizado y optimizado.

Pero esta "hiperconectividad" tiene un precio: la exposición en las redes de sistemas o componentes que antes no lo estaban, incrementa notablemente la probabilidad de ocurrencia de un incidente que provenga, precisamente, de la propia red. Y a esto contribuyen dos factores principales:

1. Que la "modernización" de la planta se ha realizado sin realizar una adecuación de la red de planta con una configuración adecuada desde la perspectiva de ciberseguridad.

2. Y dado que las tecnologías ethernet en planta son relativamente recientes, una parte importante de los elementos industriales conectados a las redes de planta no se encuentran diseñados específicamente para esta conectividad, por lo que la ausencia de medidas de seguridad que presentan de forma nativa que puedan limitar la ocurrencia de un incidente son o nulas o muy escasas.

1.2 La transformación digital como palanca de la ciberseguridad

La transformación digital y la ciberseguridad se encuentran íntimamente ligadas. La necesidad de una mejora continua de los procesos productivos supone, en ocasiones, la extracción y tratamiento de datos operacionales que, posteriormente, se explotan en entornos en la nube, lo que expanden el alcance de las redes de las empresas hasta niveles que se escapan de los propios límites físicos de las redes empresariales.

Un ciberataque que se produzca en un entorno industrial puede causar un grave impacto, no solo con consecuencias en la propia producción, sino también en la propia integridad de las personas y sistemas físicos que operan y soportan el proceso industrial.

Por lo tanto, la ciberseguridad se antoja como una necesidad fundamental para proteger los sistemas y procesos industriales.

1.3 Que es la ciberseguridad industrial

La ciberseguridad industrial, también conocida como ciberseguridad OT (del inglés Operational Technologies – Tecnologías de Operación), es una rama de la ciberseguridad que se focaliza en la protección de los sistemas y procesos que se utilizan en la producción, fabricación y otros tipos de actividades industriales frente a las amenazas cibernéticas.

Fuente: Centro de Ciberseguridad Industrial (CCI)

Si tomamos la pirámide de automatización, basada en el modelo Purdue, como referencia, el ámbito de actuación del entorno OT incluiría los niveles 0, 1 y 2, como puramente industriales, y un nivel 3 que podría considerarse como de interconexión con el nivel 4, asignado generalmente a lo que se conoce como entorno IT (del inglés Information Technologies – Tecnologías de la Información).

Las diferencias funcionales y operacionales, así como los requisitos de ciberseguridad existentes entre los entornos IT y OT son palpables, y no siempre se pueden aplicar las mismas medidas de ciberseguridad indistintamente en ambos entornos, considerando:

- Las diferencias en cuanto a concepto, uso y requerimientos funcionales de los equipos y sistemas que se localizan en ambos entornos.
- Las generalmente reducidas posibilidades de intervención, debido a los tiempos de fabricación.
- Y principalmente la necesidad de asegurar la producción frente a cambios que pudieran interferir en el correcto funcionamiento de esta.

La ciberseguridad industrial implica la implementación de medidas de ciberseguridad tanto en el ámbito técnico, como en el organizativo y procedimental. Entre otras: la protección de las redes y los dispositivos finales, la identificación y mitigación de vulnerabilidades, la implementación de controles de acceso, el establecimiento de roles encargados de la ciberseguridad, la formación y capacitación de los empleados, etc.

1.4 Porqué es necesaria

Considerando que, de forma general, las medidas de protección ante amenazas de seguridad existentes en los entornos industriales tienen un nivel de madurez mu bajo, podemos llegar a la conclusión de que si un ciberataque consigue alcanzar este entorno las consecuencias serán imprevisibles.

Por otro lado, y al margen del propio interés de la organización en llevar a cabo un esfuerzo en la securización del entorno OT, existen otros factores que pueden ser un extra de motivación como: la necesidad de cumplimiento de normativas, bien sectoriales o exigidas por clientes, la presión de compañías aseguradoras, etc.

Pero sin duda, el aumento exponencial de los incidentes de ciberseguridad que se están produciendo a lo largo de todo el mundo, invita a reflexionar seriamente sobre la capacidad de resiliencia de nuestras organizaciones en caso de materialización de un ciberincidente.

—1.4.1 Panorama actual: "la tormenta perfecta"

El contexto de las amenazas cambia continuamente, debido a la intensa actividad de los atacantes, que crean, propagan, mutan y explotan las vulnerabilidades o debilidades de los activos esenciales de los sistemas de información de una organización, como son:

- Las personas, expuestas permanentemente a amenazas de ingeniería social son los vectores de entrada de los atacantes o, bien, y en muchos casos, se convierten en una amenaza interna cuando actúan deliberadamente para causar daño a los activos de la organización.

- La información, objetivo de ataques cada vez más sofisticados, dirigidos y persistentes, para su acceso no autorizado o para su cifrado, con el objetivo de extorsionar a la organización y obtener beneficios ilícitos, cuando no para su destrucción.

- Los servicios externalizados, cada vez más extendidos, en cuyos proveedores la organización delega las medidas de seguridad que se deben gestionar continuamente para evitar la pérdida de su control o la materialización de las amenazas que afectarán directamente a los servicios que presta y/o la información que maneja la organización.

- El software, que es el activo más cambiante, por no decir más volátil, en cuanto a las vulnerabilidades que presenta continuamente y cuya explotación impactará en la organización, su negocio y reputación.

En este panorama de ciberlucha desigual se encuentra inmersa la PYME pues gestiona siempre recursos escasos, frente a los recursos ilimitados de los atacantes fruto de sus operaciones ilícitas en el ecosistema de ciberseguridad.

La amenaza, en "mayúsculas", afecta por igual a todos los sectores de actividad, donde la PYME utiliza la tecnología para desarrollar sus operaciones y, en consecuencia, como medio clave para lograr la competitividad en el mercado, cuando no la supervivencia.

En particular, lo anterior se convierte en crítico o una "tormenta perfecta"[1] cuando la actividad de la PYME es industrial y los procesos productivos se monitorizan, ejecutan, controlan y protegen mediante sistemas OT o de automatización, antes aislados de Internet, pero hoy interconectados con sistemas de gestión expuestos, en consecuencia, a todas las amenazas del ecosistema.

—1.4.1 Panorama actual: "la tormenta perfecta"

El ransomware (del inglés "ransom" + "ware", diminutivo y sufijo de software) es un tipo de malware (software malicioso) que cuando infecta un dispositivo o una organización entera, bloquea el acceso a la información (archivos y sistemas) -normalmente mediante cifrado- para luego pedir el pago de un rescate (ransom) a cambio de devolver el acceso a la información. Es decir, es un ataque a la disponibilidad.

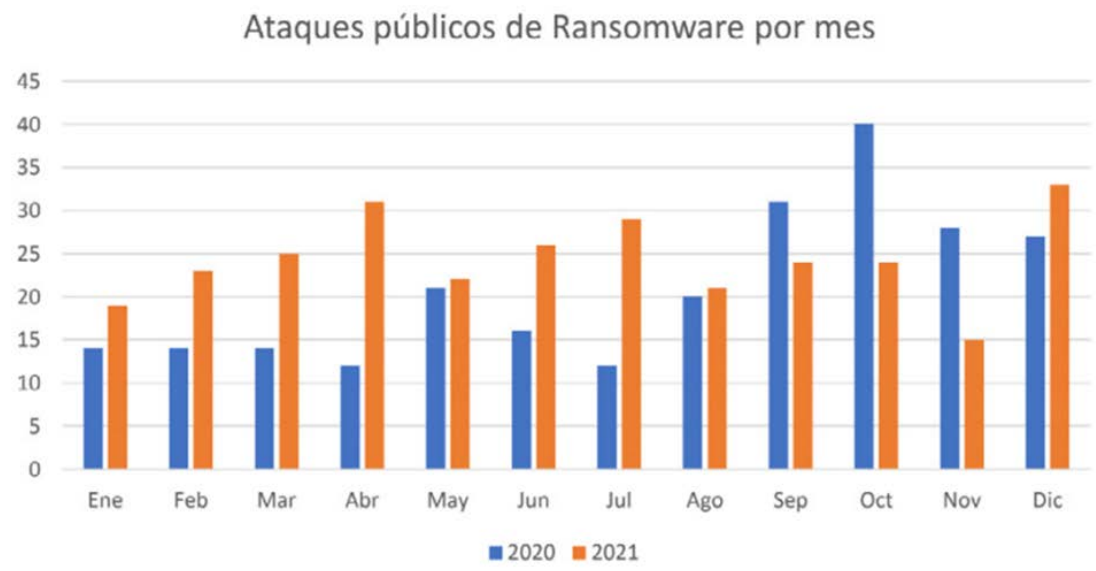
Lo más habitual es que el pago del rescate se solicite en bitcoins (u otra criptomoneda), por ser un medio de pago anónimo y por lo tanto muy difícil, por no decir imposible, de rastrear.

El ransomware afecta a todo tipo de empresas: pequeñas, medianas y grandes; también a empresas de servicios (únicamente con entorno IT) pero también a organizaciones industriales. Podríamos citar un gran número de empresas conocidas que han sido atacadas con este tipo de malware y que son casos públicos.

1 The perfect storm https://www.pmi.org/learning/library/perfect-storm-emerging-technology-7291

Desde hace unos años, los ataques por ransomware se han vuelto todavía más perjudiciales para las empresas ya además de la extorsión para recuperar los datos del cifrado, se suma la petición de un rescate para evitar ("chantaje y amenaza") la revelación de la información, bien publicándola abiertamente en Internet o subastándola en la deep web, con el consiguiente daño a la empresa y sus clientes (información confidencial de clientes, propiedad industrial intelectual, ...), proveedores o trabajadores, incluyendo el riesgo de multas, por ejemplo, en el caso de que se trate de datos personales.

En la siguiente gráfica se aprecia el aumento de ataques ransomware de 2020 a 2021:



Del último informe del CCN-Cert (de Ciber Amenazas y Tendencias) del 2022

1.5 Estándares, marcos de referencia y cumplimiento normativo

Las PYMEs que operan en el entorno industrial disponen de marcos de referencia y normativas específicas de seguridad, como la NIST, ISA/IEC-62443, entre otras. Estos marcos de referencia ayudan a las organizaciones a cumplir las normativas específicas de su ámbito de aplicación, pero a veces no son suficientes para aliviar la presión regulatoria. Si bien es cierto que existen normativas especificas orientadas a proteger "única y exclusivamente el entorno Industrial", debemos de tener en cuenta que en la mayoría de veces no son entornos aislados y que conviven infraestructura IT junto con infraestructura OT, y que un ciberataque en cualquiera de los dos entornos puede llevarnos a comprometer no solo la planta industrial si no que puede llevar a que se produzca una fuga de datos personales, sensibles o confidenciales dependiendo del sector de la PYME.

En España, y en el ámbito europeo, existen regulaciones vigentes que establecen requisitos y estándares para garantizar la protección de los sistemas y datos en diferentes sectores, como en alimentación, manufactura, transporte, automoción, etc. El cumplimiento adecuado de estas normativas es esencial para evitar sanciones financieras y proteger la reputación de las empresas. A continuación, se realiza un breve repaso de las principales regulaciones en ciberseguridad en España y Europa:

Cumplimiento de regulaciones en España

1. Las PYMEs deben cumplir con la Ley Orgánica de Protección de Datos Personales y garantía de los derechos digitales (LOPDGDD), que establece las obligaciones y medidas de seguridad que deben implementarse para proteger la información personal y asegurar su confidencialidad e integridad. Además, se recomienda seguir las directrices de la Agencia Española de Protección de Datos (AEPD) en relación con la protección de datos y la ciberseguridad. Un ataque por Ransomware podría atentar contra esta Ley.

2. Asimismo, la Ley de Propiedad Intelectual (LPI) y la Ley de Marcas (17/2001) son relevantes para proteger la propiedad intelectual y los derechos de autor. Un Ciberataque por Ransomware o una fuga de datos ocasionada por un ciberataque, podría atentar contra esta Ley.

3. La Estrategia de Seguridad Nacional es el marco de referencia para la política de Seguridad Nacional, una política de Estado que parte de una concepción amplia de la seguridad. La Estrategia actual, que cuenta con el informe favorable del Consejo de Seguridad Nacional de 18 de noviembre, y aprobada por el Gobierno mediante Real Decreto, profundiza en algunos de los conceptos y líneas de acción definidos en 2017 y avanza en la adaptación de dicha Política y los instrumentos y recursos del Estado que la conforman ante nuevos desarrollos de un entorno de seguridad en cambio constante.

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

5. La Ley 8/2011 tiene por objeto "establecer las estrategias y las estructuras adecuadas que permitan dirigir y coordinar las actuaciones de los distintos órganos de las Administraciones Públicas en materia de protección de infraestructuras críticas, previa identificación y designación de las mismas, para mejorar la prevención, preparación y respuesta de nuestro Estado frente a atentados terroristas u otras amenazas que afecten a infraestructuras críticas.

6. El Real Decreto 311/2022 que tiene por objeto regular el Esquema Nacional de Seguridad (ENS), que establece la política de seguridad en la utilización de medios electrónicos en el ámbito de la Administración Electrónica y se constituye como un instrumento al servicio de la interoperabilidad.

Cumplimiento de regulaciones en Europa

1. Las PYMEs deben cumplir con el Reglamento General de Protección de Datos (RGPD), que establece un marco de protección de datos uniforme en la Unión Europea. Un ataque por Ransomware podría atentar contra esta Ley.

2. La Directiva NIS (Directiva sobre la seguridad de las redes y la información) es una normativa europea que establece requisitos para garantizar la seguridad de las redes y los sistemas de información en diversos sectores. Esta directiva afecta a sectores considerados como "infraestructuras críticas", como la energía, el transporte, la sanidad, los servicios financieros, la gestión del agua y la alimentación, entre otros. Su objetivo es fortalecer la ciberseguridad y mejorar la capacidad de respuesta ante incidentes cibernéticos, promoviendo la cooperación entre los Estados miembros y estableciendo medidas de protección y notificación de incidentes en dichos sectores.

3. Directiva NIS2. La Directiva NIS-2 será de obligado cumplimiento para empresas de más de 250 empleados y con un volumen de facturación anual de 50 millones de euros en adelante. Al mismo tiempo, también estarán obligados a su cumplimiento los operadores que presten servicios esenciales y los proveedores de servicios digitales que operan en la Unión Europea. Estos servicios incluyen, entre otros, servicios energéticos, transporte, salud, banca y finanzas, y servicios de telecomunicaciones.

Es de aplicación tanto para la administración como para las medianas y grandes empresas de ciertos sectores, como pueden ser la gestión de residuos, las industrias química, farmacéutica y alimentaria, la fabricación de maquinaria pesada, los servicios postales, vehículos, etc.

En esta norma, entra un nuevo factor y es que tienen que atenerse a ella no sólo las empresas que proporcionan productos o servicios, sino también toda su cadena de suministro. Esto produce que el número de organizaciones que tendrán que seguirla es enorme.

La Directiva se publicó el 27 de diciembre de 2022 en el Diario Oficial de la Unión Europea y los países dispondrán de 21 meses para su trasposición a normativa local.

1.6 Ejemplos de incidentes en PYMES españolas

A pesar de que existen varios casos de PYMES u organizaciones de menor tamaño con incidentes de seguridad conocidos -casos públicos que han sido publicados en prensa, en foros y demás-, en esta guía comentaremos algunos relevantes, pero sin citar ningún dato identificativo directo de las empresas afectadas.

El primer caso que destacamos es de 2012, con un phishing (email falso y fraudulento con un gancho, técnica empleada para el engaño a las personas) a un ayuntamiento típico de la España vaciada con tan solo 2000 habitantes, y sin embargo se materializó en un robo de 200.000€ (el saldo total de la cuenta bancaria del ayuntamiento), aproximadamente 100€ por habitante. A través del phishing el atacante se hizo con las claves bancarias.

El segundo caso que destacamos es una empresa industrial del sector la alimentación, que siendo víctima de un ransomware se encontró sin acceso a la información de fábrica y con los sistemas de producción completamente parados. El impacto para la organización de tener la producción parada con el riesgo de no servir el producto al cliente y de desperdicio de materia prima (perecedera rápidamente) era tan alto, que cedieron al chantaje y realizaron el pago para poder recuperar el acceso a la información y poder reiniciar la producción. El pago se realizó en bitcoins y superaba los 70.000 euros al cambio. Posteriormente tuvieron que revisar en profundidad los sistemas, hacer limpieza y establecer medidas de seguridad adecuadas para prevenir la repetición de este tipo de ataques y otros riesgos.

En un tercer caso, destacamos un caso ocurrido en plena pandemia, a finales del 2020, cuando una organización en España, del sector de automoción, fue víctima de otro ransomware denominado Revil. En este caso, se había producido el robo de información supuestamente sensible. Se estima que el impacto no fue tan alto -además de la falta de garantías- como para ceder al chantaje y realizar el pago de un rescate. Sin embargo, la organización tuvo que responder ante la opinión pública y especialmente ante algunos clientes descontentos y preocupados por la gravedad del incidente y con la necesidad de conocer si han sido afectados colateralmente de alguna forma. Como noticia reciente de finales de marzo de 2023, se desarticuló una organización cibercriminal con la detención de 25 personas, que realizó estafas telemáticas a unas 100 empresas por un importe total de más de 5 millones de euros. El principal ataque era el "fraude del CEO", en el que se roba y suplanta al gerente de una PYME (con poder de decisión sobre pagos) para ordenar pagos ilícitos a cuentas de la organización criminal. Nuevamente el engaño al usuario como medio para la realización del delito.

Cabe destacar que en el "Informe sobre la cibercriminalidad en España 2021" la importancia de la Cibercriminalidad va creciendo año tras año. Hemos pasado del año 2017, donde nos situábamos en el 5,7%, al año 2021 con el 15,6%, sobre el total de infracciones penales.

Otros ejemplos de grandes empresas industriales representativos

Por supuesto podríamos mencionar el caso de Stuxnet (2010-2012) en el que cabe destacar que precisamente con una vulnerabilidad IT se ataca a dispositivos OT (2 modelos de PLC de un gran fabricante del ámbito industrial), impactando en el mundo físico mediante el deterioro y desgaste acelerado de los rotores de centrifugadoras.

Otros ejemplos más recientes y conocidos son las paradas de producción de una empresa de distribución de gas (gaseoductos) y de una empresa cárnica, ambas estadounidenses con un gran impacto en operaciones y muy mediáticos a mediados de 2021, originadas por el cifrado provocado por un ransomware que provoca la parada de la producción. Lo más destacable de estos dos casos es que realizaron el pago del "rescate" en bitcoins de sumas muy altas que han ascendido a varios millones de USD.

En el caso de la empresa estadounidense de oleoductos en 2021 que mencionábamos, el ataque fue llevado a cabo por el grupo Darkside y, por un lado, paralizó la actividad del sistema de oleoductos durante seis días; y por otro, realizaron el robo de más de 100Gb de información.

En un último caso, y para mostrar la importancia de la ciberseguridad en la cadena de suministro, el ataque impactó a una empresa pequeña que proporcionaba piezas a una gran marca de automoción en 2022. El ataque también fue un ransomware que paralizó el sistema de gestión de suministros de dichas piezas y afectó a las 14 plantas de producción del fabricante de vehículos, sumando 28 líneas de producción en total. Esto causó que se parase la producción de coches durante un día, perdiéndose el 5% del total de la producción de esta marca (10.000 unidades).

2 INTRODUCCIÓN A LA GUÍA

2.1 Seguridad IT vs. Seguridad OT

Recordemos que en el ámbito de la Seguridad de la Información se definen fundamentalmente tres principios básicos: Confidencialidad, Integridad y Disponibilidad, conocidos también como la "tríada CIA" (por sus iniciales en inglés).

- La **Confidencialidad** permite limitar el acceso a los datos de modo que sólo las personas (o recursos) autorizados puedan acceder a la información.
- La **Integridad** garantiza que la información sea correcta, sin errores y que no pueda ser modificada sin permiso.
- La **Disponibilidad** asegura que la información está accesible en un momento preciso y para las personas que la necesitan.

En los sistemas IT corporativos, como el ERP o la base de datos de clientes, la puesta en práctica de los principios de la tríada CIA viene cumpliéndose en ese mismo orden de importancia: Confidencialidad, Integridad, Disponibilidad. Al plantear un plan de seguridad IT, es habitual que una de las primeras medidas a implementar esté relacionada con el cifrado de datos, medida directamente relacionada con la Confidencialidad.

Ahora bien, en el ámbito de la seguridad de los Sistemas de Control Industrial (SCI) la perspectiva puede ser diferente. Los sistemas SCI están formados por dispositivos y redes que controlan los procesos industriales. En el caso de una Infraestructura Crítica como Energía o Transportes, debe primar el principio de Disponibilidad para garantizar que el proceso operativo no se detiene.

Esto tiene que ver, en parte, con que los SCI muchas veces también incluye a los sistemas responsable de la Safety o seguridad física de los procesos productivos. Esta dependencia entre los sistemas de Security y Safety es clave a la hora de diseñar un sistema OT. Como se puede imaginar, una caída en estos sistemas podría causar daños a los trabajadores de la planta o incluso su muerte.

Tradicionalmente, el área de OT ha vivido aislada del área de IT (y viceversa), pero en la actualidad, en la era de la hiperconectividad, sistemas "Smart", IoT, etc. se está produciendo una aproximación entre ambas áreas en lo que se denomina "Convergencia IT/OT". Esta convergencia no es tarea fácil y uno de los retos a superar es la diferente visión de los principios de seguridad según el punto de vista de cada área. Si para los equipos de IT (de soporte al negocio) prima la Confidencialidad sobre los otros principios de seguridad, para los ingenieros o técnicos de OT, el orden de importancia de la tríada CIA es justo lo opuesto: Disponibilidad, Integridad, Confidencialidad. No obstante, esta afirmación no puede ser considerada como un axioma, y hay que considerar las particularidades de cada escenario industrial, porque ¿es asumible por una empresa primar la fabricación sobre una fabricación no adecuada (falta de integridad en el proceso de fabricación)?

El gráfico representa la inversión de las prioridades en cuanto a seguridad según se trata del área de Sistemas de IT o de Sistemas de OT. Para los responsables de OT lo más importante es mantener el proceso industrial en funcionamiento, ya se trate de una cadena robotizada de producción; una red de suministro de energía, o de agua potable; o del sistema de control de una red de semáforos inteligentes. La carencia de Disponibilidad podría derivar en una pérdida de control sobre el proceso o que se detuvieran las operaciones, con los consiguientes riesgos que ello implicaría tanto para la seguridad del sistema como para la seguridad física de las personas o los efectos en el medioambiente.

2.2 Qué es un SGCI

—2.2.1 Qué es un sistema de gestión

Un sistema de gestión es una estructura organizativa y un marco de trabajo que permite a las organizaciones administrar sus actividades para conseguir unos objetivos específicos. Algunos sistemas de gestión se basan en estándares reconocidos internacionalmente, como la norma ISO 9001 para un Sistema de Gestión de la Calidad, la norma ISO 14001 para un Sistema de Gestión Medioambiental, o la norma ISO 27001 para un Sistema de Gestión de Seguridad de la Información.

El objetivo principal de un sistema de gestión es proporcionar un marco integral que permita a la organización planificar, implementar, monitorizar y mejorar sus procesos. Esto implica que el sistema debe contar con una serie de procesos, políticas, procedimientos y normativas que describan cómo se articulan las actuaciones de las personas interesadas (clientes, empleados, colaboradores, socios, accionistas, reguladores…) para lograr los objetivos y metas fijados. En este sentido, es importante identificar bien los roles y responsabilidades de los implicados en el sistema de gestión.

Un sistema de gestión eficaz también implica el establecimiento de indicadores de rendimiento clave para evaluar el progreso y la conformidad con los estándares establecidos.

Todos los elementos de un sistema de gestión quedan reflejados en un marco normativo o marco documental. Entre los principales elementos del marco normativo tenemos:

- **Políticas:** Documento de alto nivel que refleja la intención y el compromiso de los órganos de dirección de la organización para cumplir con los objetivos derivados del sistema de gestión. Suele ser un documento breve y que perdura en el tiempo. Por ejemplo, una "Política de Ciberseguridad Industrial".

- **Procedimientos:** Documento que establece cómo se van a aplicar las políticas para dar cumplimiento a las distintas áreas de actuación del sistema de gestión. Un procedimiento es un documento a más bajo nivel que una política, con mayor detalle, y centrado en una actividad concreta. Debe disponer de un mecanismo de control de versiones ya que deben mantenerse actualizados en todo momento con el fin de reflejar la realidad de los procesos de la organización. Por ejemplo, un "Procedimiento de Copias de Seguridad", un "Procedimiento de Gestión de Contraseñas" o un "Procedimiento de altas y bajas de usuarios".

- **Instrucciones Técnicas:** Son documentos operativos que describen con todo detalle cómo se llevan a cabo las tareas descritas en los procedimientos. Es como el "manual de instrucciones" para una determinada actividad. Por ejemplo, de un "Procedimiento de Copias de Seguridad" puede derivarse una "Instrucción Técnica para la realización de copias del SCADA en la red" o una "Instrucción Técnica para la restauración de las configuraciones de los sistemas de control".

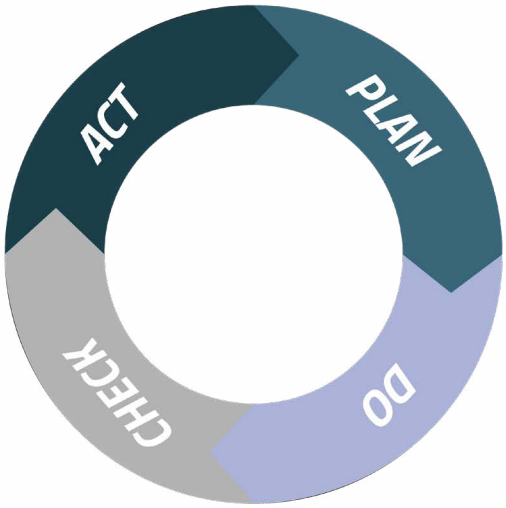
Una característica común de todos los sistemas de gestión es que cuentan con un enfoque basado en la mejora continua, esto es, un ciclo de retroalimentación constante con acciones para resolver posibles deficiencias y optimizar el desempeño. A continuación, se describe el ciclo de mejora continua o ciclo PDCA.

—2.2.2 Ciclo PDCA

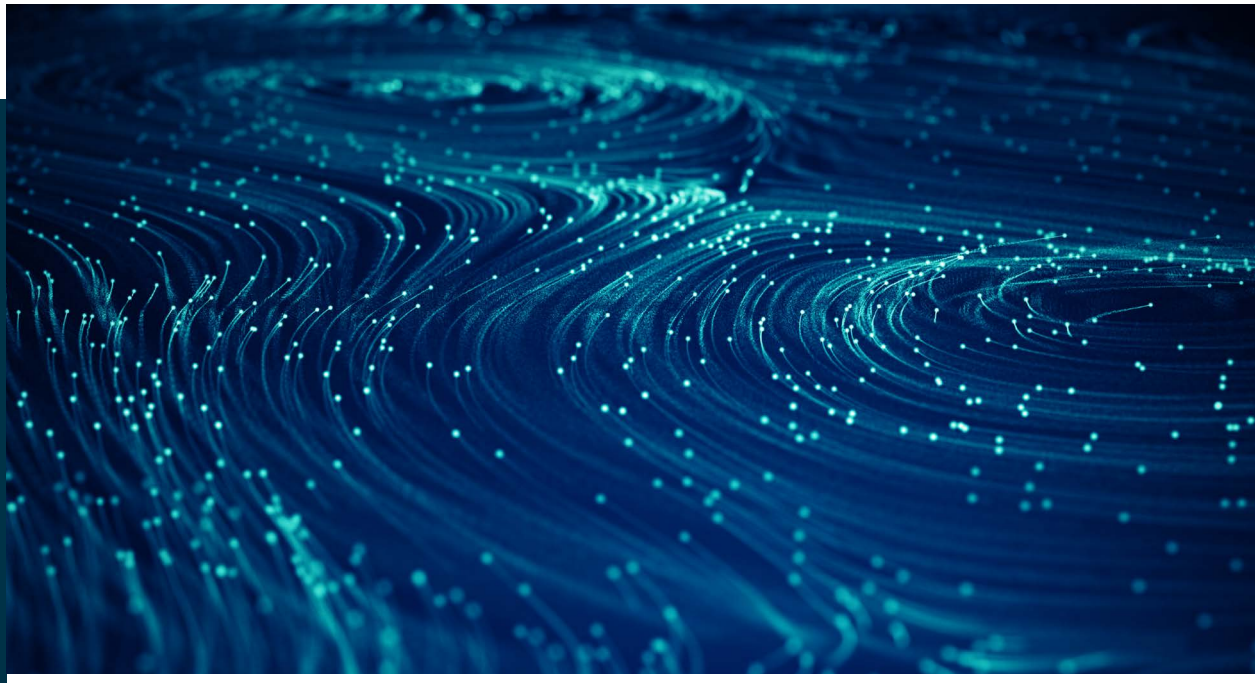
El ciclo de mejora continua, también conocido como ciclo PDCA (acrónimo de las iniciales en inglés de Planificar, Hacer, Verificar y Actuar), o también ciclo de Deming (en honor al estadístico estadounidense Edwards Deming) es una metodología ampliamente utilizada en los sistemas de gestión para impulsar la mejora y el perfeccionamiento de los procesos.

El ciclo se compone de cuatro etapas en bucle:

- **Planificar (Plan):** se fijan los objetivos, se identifica a las partes interesadas, se establecen los recursos necesarios y se diseñan los planes para conseguir dichos objetivos.
- **Hacer (Do):** se implementan los planes y se llevan a cabos las actividades planificadas.
- **Verificar (Check):** se monitorizan y se evalúan los resultados comparándolos con los objetivos establecidos. Se identifican las desviaciones y se analizan las causas raíz.
- **Actuar (Act):** se toman medidas correctivas, preventivas o proactivas para mejorar continuamente los procesos.



Al final de las etapas PDCA, el ciclo vuelve a iniciar en una nueva iteración, utilizando los resultados y lecciones aprendidas del ciclo anterior permitiendo con ello que las organizaciones puedan adaptarse y responder de manera efectiva a los cambios. Esto es especialmente importante en el ámbito de la ciberseguridad industrial, donde impera un escenario cambiante ya sea con motivo de la adopción de nuevos retos tecnológicos, o por la aparición de un nuevo panorama de amenazas y riesgos.



—2.2.3 Qué es un Sistema de Gestión de la Ciberseguridad Industrial

Un Sistema de Gestión de la Ciberseguridad Industrial (SGCI) es el sistema de gestión implementado por una organización para garantizar la adopción de buenas prácticas en ciberseguridad respecto a los sistemas de control y automatización industrial (entorno OT).

El SGCI incluirá el conjunto de políticas, procedimientos y medidas de seguridad implementadas en la organización para proteger los sistemas y activos pertenecientes al ámbito de OT.

De forma genérica, se pueden identificar los siguientes elementos en un SGCI:

- Alcance del SGCI
- Roles y responsabilidades
- Evaluación de riesgos
- Plan de acción
- Marco normativo de la seguridad
- Implementación de medidas de seguridad
- Monitorización
- Mejora continua

En el apartado 3 de esta guía se describe con detalle el proceso de desarrollo e implementación del SGCI considerando estos elementos.

2.3 Diferencias entre un SGSI y un SGCI

Aunque un Sistema de Gestión de Seguridad de la Información (SGSI) y un Sistema de Gestión de la Ciberseguridad Industrial (SGCI) son sistemas muy parecidos y comparten el objetivo de proteger los activos, gestionar los riesgos y promover la mejora continua en términos de seguridad, hay que tener en cuenta las diferencias entre ambos en los siguientes aspectos:

- Ámbito de aplicación: el SGSI se enfoca en la protección de la información en general, abarcando todos los activos de información de una organización, incluyendo datos confidenciales, sistemas de TI, procesos y recursos asociados. El SGCI se centra específicamente en la protección de los sistemas de control industrial y los entornos OT. Estos sistemas de control son responsables de supervisar y controlar los procesos industriales y, por lo tanto, tienen requisitos de ciberseguridad específicos.

- Amenazas y riesgos: en el SGSI, se consideran una amplia gama de amenazas y riesgos de seguridad de la información, incluyendo ciberataques, malware, acceso no autorizado, pérdida de datos, revelación de información confidencial, fuga de datos personales, etc. En el SGCI, se pone énfasis en las amenazas y riesgos específicos que afectan a los sistemas de control industrial. Estos pueden incluir ataques dirigidos a sistemas SCADA, sistemas de control distribuido (DCS), protocolos de comunicación industrial, equipos de campo y otros componentes críticos en entornos industriales.

- Normativas y estándares: para el SGSI, hay varios marcos y normas reconocidos internacionalmente, como la norma ISO 27001 y normas derivadas, o marcos de referencia como el NIST CSF, incluso normas de rango legal de obligado cumplimiento como el Reglamento General de Protección de Datos (RGPD) o la Directiva de Seguridad de Redes y Sistemas (NIS), entre otras. En el caso del SGCI, el principal estándar utilizado es la norma ISA/IEC 62443, que se centra específicamente en la ciberseguridad industrial. Proporciona una guía detallada y requisitos específicos para la protección de los sistemas de control industrial, aunque también hay que considerar las normativas sectoriales específicas, como la regulacion de la ciberseguridad en sistemas ferroviarios, en sistemas de producción y distribución de energía eléctrica, etc. o, la normativa de protección de infraestructuras críticas de cada país, que establece obligaciones para los operadores de infraestructuras críticas.

2.4 ¿Un SGCI para una PYME?

Si bien las regulaciones y normativas en materia de ciberseguridad industrial tienen un enfoque orientado a grandes empresas, las PYME no están exentas de sufrir un incidente de seguridad que afecte a sus entornos OT. Por este motivo, es esencial que las empresas tengan en cuenta los requisitos de seguridad industrial y los ajusten según las características particulares de sus entornos de control y automatización industrial.

En particular, como cualquier sistema de gestión, un SGCI posee la flexibilidad y capacidad de personalización necesarias para adaptarse eficazmente a las particularidades y necesidades específicas de las PYME.

A medida que las PYME adoptan procesos de digitalización industrial como IoT, automatización o robótica, sus sistemas industriales se vuelven más interconectados, lo que a menudo los hace más vulnerables a ciberataques. Los ataques a sistemas OT pueden causar daños significativos en la producción, el suministro y la reputación de las PYME, lo que puede resultar en pérdidas financieras y una disminución de la confianza de los clientes. Por lo tanto, la implementación de medidas de ciberseguridad industrial es esencial para proteger los activos empresariales y garantizar la continuidad de las operaciones, así como para cumplir con las regulaciones y estándares de seguridad exigidos por los socios comerciales y las autoridades gubernamentales.

Del mismo modo que la dirección de una organización suele tener preocupación por la seguridad de sus sistemas de información, y suele prestar su apoyo para la puesta en marcha de un SGSI que garantice la seguridad de los datos corporativos, una PYME industrial debería apostar por contar con un SGCI que establezca los requisitos y controles de seguridad OT de la organización. El SGCI permitirá minimizar los riesgos de ciberseguridad en la operación o producción, al mismo tiempo que permite fijar las suficientes garantías en cuanto a la continuidad del negocio.

Además de los riesgos financieros y operativos, un SGCI es crucial para proteger la propiedad intelectual y la información confidencial de las PYME. Estas organizaciones a menudo poseen conocimientos técnicos especializados y secretos comerciales valiosos que pueden ser el objetivo de ciberdelincuentes. La pérdida o el robo de dicha información puede tener un impacto devastador en la competitividad y la sostenibilidad de las PYME. Hay que tener presente que, aunque las grandes empresas puedan parecer más atractivas para los ciberdelincuentes, las PYME son vistas como objetivos más fáciles debido a sus posibles deficiencias en cuanto a medidas de seguridad. Los ataques dirigidos a las PYME pueden tener consecuencias devastadoras, como pérdida de datos, interrupción de las operaciones comerciales, daño a la reputación y costos financieros considerables.La implantación de in SGCI en la PYME permite dotar a la organización de una sólida postura de ciberseguridad industrial fortaleciendo la confianza de clientes y socios comerciales, lo que puede abrir nuevas oportunidades de negocio y fomentar el crecimiento a largo plazo para las PYME.

Finalmente, no hay que olvidar que las PYME suelen formar parte de cadenas de suministro más grandes, donde la seguridad de la información y la ciberseguridad industrial son aspectos críticos. Si una PYME se convierte en una puerta de entrada para los ciberataques, puede poner en peligro la seguridad de toda la cadena de suministro, afectando a terceros. Los ciberdelincuentes son conscientes de que el ataque a una PYME, con menores capacidades de protección, puede abrirles la puerta para atacar empresas más grandes bien sea suplantando al personal de la PYME u obteniendo datos que les facilite el acceso. Las grandes empresas y multinacionales están cada vez más interesadas en trabajar con proveedores y socios comerciales que cumplan con altos estándares de ciberseguridad, lo que implica que las PYME deben adoptar medidas de seguridad adecuadas para mantener relaciones comerciales sólidas.

2.5 Que aporta un SGCI

Como ya hemos comentado en el apartado 2.2, un Sistema de Gestión de Ciberseguridad Industrial (SGCI) es una herramienta que permite a las empresas implementar y mantener un enfoque estructurado y sistemático para la gestión de la ciberseguridad en los entornos industriales.

Entre los beneficios que podemos identificar y que ofrece una implantación adecuada de un SGCI se encuentran:

1. Visión permanente del nivel de riesgo: un SGCI permite identificar y evaluar los riesgos de ciberseguridad a los que está expuesta la empresa en relación a los sistemas y procesos industriales. Por lo tanto, si se conocen los riesgos asociados a escenarios de amenaza, es posible poner en marcha medidas de protección adecuadas en función de la criticidad de los procesos industriales que queremos proteger.

2. Aseguramiento de la producción: la identificación y el tratamiento de los riesgos disminuye la probabilidad de materialización de una amenaza, lo que permite minimizar la ocurrencia de una interrupción de la producción debido a un ciberataque.

3. 3Cumplimiento de requerimientos normativos: un SGCI permite cumplir con los requerimientos normativos relacionados con la ciberseguridad industrial, tanto los basados en marcos normativos más generales (IEC 62443, por ejemplo) como en aquellos de ámbito sectorial.

4. Ventaja competitiva: poder demostrar que la empresa se encuentra comprometida con la ciberseguridad en sus procesos productivos es, actualmente, un aspecto que puede posicionarla en una mejor posición en el mercado.

2.6 Factores de éxito a considerar

—2.6.1 Factores críticos

A continuación, se presentan algunos de los factores de éxito a considerar en la gestión de la ciberseguridad en el entorno industrial de una PYME.

PUNTO CRÍTICO	DESCRIPCIÓN
Apoyo de la Dirección	El primer factor crítico para el éxito en la gestión de la ciberseguridad en una PYME es el apoyo de la dirección. La alta dirección debe comprender la importancia de la seguridad de la información y estar dispuesta a invertir en medidas de ciberseguridad que protejan la empresa. Esto significa que la dirección debe asignar presupuesto, recursos y tiempo para desarrollar una estrategia de ciberseguridad y un plan de acción que se adapte a las necesidades específicas de la empresa. En definitiva, el principal espónsor interno de la puesta en marcha de un SGCI debe ser la propia Dirección.
Cultura de ciberseguridad: formación y concienciación	Otro factor importante para el éxito en la gestión de la ciberseguridad es crear una cultura de ciberseguridad en la empresa. Esto implica educar y concientizar a todo el personal sobre las amenazas de seguridad y la importancia de proteger la información. La cultura de ciberseguridad también implica la implementación de políticas y prácticas de seguridad que se apliquen de manera consistente en toda la organización. Esto puede incluir medidas como la autenticación de dos factores, el cifrado de datos, la gestión de contraseñas y la implementación de firewalls. Es fundamental que todo el personal de la empresa ¡incluyendo los operarios que trabajan exclusivamente en la planta! reciba formación y capacitación continua sobre ciberseguridad. La formación puede incluir la identificación de phishing y otros ataques de ingeniería social, la gestión de contraseñas seguras y la adopción de buenas prácticas de seguridad de la información, la manipulación de dispositivos de almacenamiento extraíble, la conexión de equipamiento de terceros a las redes corporativas, ... También se debe fomentar la cultura de ciberseguridad a través de simulaciones y ejercicios de respuesta a incidentes de seguridad.
Identificación del riesgo	La identificación de los riesgos es otro factor crítico para el éxito en la gestión de la ciberseguridad. Para lograr una gestión efectiva de la ciberseguridad, es necesario entender las amenazas y los riesgos que enfrenta la empresa. Esto incluye la identificación de vulnerabilidades en los sistemas, procesos y aplicaciones de la empresa. Una vez que se han identificado los riesgos, es posible establecer medidas de seguridad adecuadas para proteger los activos críticos de la empresa.
Monitorización y detección de amenazas	La Monitorización y la detección de amenazas son fundamentales para la ciberseguridad industrial en una PYME. Las empresas deben disponer de los medios que les permitan detectar actividades sospechosas en sus sistemas y redes. Esto puede incluir la implementación de sistemas de detección de intrusiones (IDS), sistemas de información y eventos de seguridad (SIEM), etc.

—2.6.2 Servicios de SOC: un pilar fundamental

Considerando el conocimiento experto que requiere la implantación y uso de estas herramientas, y la falta de recursos TIC que generalmente presenta una PYME, siempre es aconsejable valorar la externalización de este servicio en un servicio de SOC experto (Centro de Operaciones de Seguridad). Un servicio de SOC brinda numerosas ventajas para una PYME en la vigilancia y monitorización de ciberataques en un entorno industrial:

1. **Detección temprana de amenazas:** un servicio de SOC cuenta con herramientas y tecnologías avanzadas para detectar de manera temprana actividades sospechosas o maliciosas en los sistemas y redes de la empresa. Esto permite identificar y responder rápidamente a posibles ciberataques antes de que puedan causar daños significativos.

2. **Monitorización continua:** el SOC ofrece una monitorización continua de los sistemas y redes de la empresa, las 24 horas del día, los 7 días de la semana. Esto asegura una protección constante contra amenazas y la identificación de patrones o comportamientos anómalos que podrían indicar una intrusión o un ataque en curso.

3. **Respuesta y gestión de incidentes:** un servicio de SOC no solo detecta amenazas, sino que también brinda una respuesta rápida y eficiente ante incidentes de seguridad. Esto incluye la coordinación y gestión de la respuesta al incidente, la contención de la amenaza, la recuperación de sistemas y datos, y la implementación de medidas correctivas para prevenir futuros ataques.

4. **Experiencia y conocimientos especializados:** el equipo de un SOC está compuesto por expertos en seguridad cibernética que poseen conocimientos y experiencia en la detección y mitigación de ciberataques. Estos profesionales están capacitados para interpretar y analizar los datos recopilados por las herramientas de monitorización, identificar patrones de ataque y aplicar las mejores prácticas de seguridad.

5. **Ciberinteligencia de amenazas:** Mientras las tecnologías de ciberseguridad cuentan con la inteligencia de amenazas proporcionada por los fabricantes, los SOC suelen contar con un conjunto de indicadores de amenazas mayor, ya que se encuentran suscritos a servicios de ciberinteligencia o, en los casos más avanzados, cuentan con analistas de inteligencia que, mediante la correlación anonimizada de los incidentes, extraen indicadores antes incluso de que los ataques sucedan en los clientes.

6. **Reducción de riesgos y pérdidas:** al contar con un servicio de SOC, una PYME puede reducir significativamente los riesgos y las pérdidas asociadas con los ciberataques. La detección temprana y la respuesta rápida permiten minimizar el impacto de los incidentes de seguridad, reducir el tiempo de inactividad y evitar posibles robos de datos o daños a la reputación de la empresa.

7. **Cumplimiento normativo:** un servicio de SOC puede ayudar a las PYMEs a cumplir con las regulaciones y normativas específicas de ciberseguridad. Al contar con una monitorización constante y una respuesta efectiva a los incidentes, las empresas pueden demostrar su compromiso con la seguridad y el cumplimiento de los requisitos legales.

—2.6.3 ¿Y si no tengo en cuenta lo anterior?

Hasta aquí hemos enumerado algunos de los principales Factores de éxito a considerar en la gestión de la ciberseguridad en el entorno industrial, pero ¿cuáles podrían ser las consecuencias de no tener en cuenta estas consideraciones?

Pongamos un ejemplo o caso de uso sobre la consecuencia o no de aplicar estas consideraciones descritas anteriormente en una PYME. Imaginemos una PYME que se dedica a la producción de bienes de consumo y que recientemente ha comenzado a utilizar sistemas automatizados para controlar sus procesos de producción. La empresa ha reconocido la necesidad de implementar medidas de ciberseguridad para proteger sus sistemas y datos, y ha abordado un proyecto de ciberseguridad industrial considerando los factores críticos de éxito que hemos mencionado anteriormente.

La empresa ha recibido el apoyo de la dirección, que ha proporcionado el presupuesto necesario para implementar medidas de seguridad adecuadas. Se ha creado una cultura de ciberseguridad dentro de la empresa y se ha realizado una evaluación de riesgos para identificar los activos críticos y los riesgos a los que se enfrentan. Con esta información, se han implementado medidas de seguridad específicas para proteger los sistemas automatizados y los datos de la empresa.

Además, la empresa ha llevado a cabo una evaluación de proveedores y terceros para asegurarse de que los proveedores también cumplan con los requisitos de seguridad necesarios. La empresa ha identificado las normativas y regulaciones específicas que se aplican a su industria y ha implementado medidas para cumplir con estas regulaciones. La empresa también ha establecido un plan de actualización de sistemas y aplicaciones, así como un plan de Monitorización y detección de amenazas.

En este escenario, la empresa ha logrado implementar medidas de seguridad efectivas que protegen sus sistemas y datos contra las vulnerabilidades conocidas y desconocidas. La empresa puede operar con confianza, sabiendo que está protegida contra ataques cibernéticos y que ha implementado medidas para minimizar el impacto en caso de que ocurra un incidente de seguridad.

Por otro lado, si la empresa no hubiera abordado el proyecto de ciberseguridad industrial considerando los factores críticos de éxito, se puede enfrentar a consecuencias imprevisibles en caso de materialización de un ciberincidente. Por ejemplo, la empresa podría haber sido víctima de un ciberataque que resultara en la pérdida de datos sensibles, esenciales o críticos para el negocio, la interrupción de la producción y la pérdida de reputación. Además, la empresa podría haber enfrentado sanciones financieras y legales por no cumplir con las regulaciones y normativas de seguridad aplicables a su industria.

2.7 Descripción del caso de uso

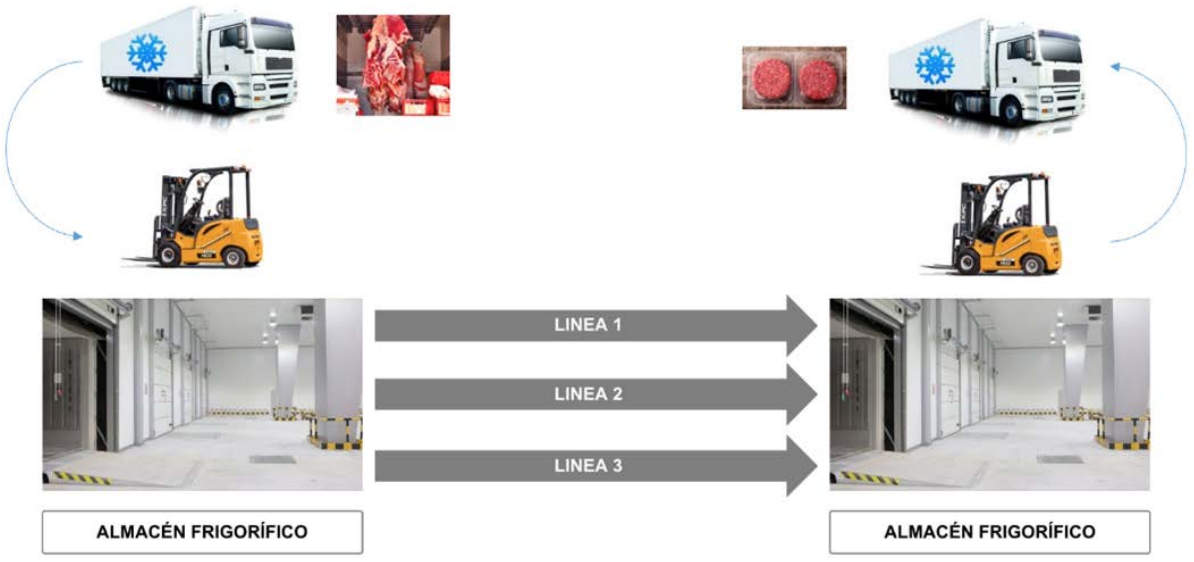
El capítulo 3 de la presente guía desarrolla una serie de actividades enfocadas a la puesta en marcha de un SGCI en una PYME. Para ilustrar de forma práctica estas actividades, se ha desarrollado un caso de uso ficticio sobre el que se detallarán ejemplos concretos.

—2.7.1 La empresa

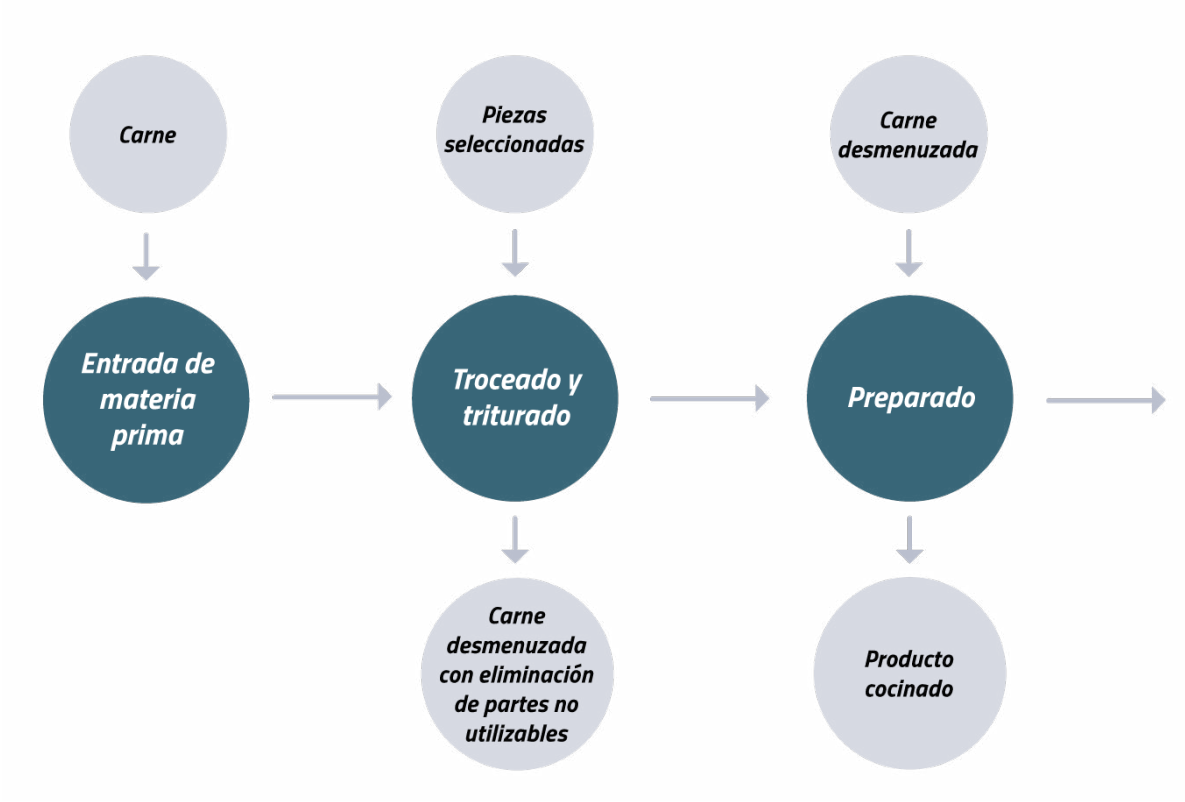
La empresa ACME, dedicada a la preparación de preparados cárnicos en el sector alimentario, se encuentra en la necesidad de implementar un Sistema de Gestión de Ciberseguridad Industrial. Dado que ACME es una PYME ubicada en España, con una facturación de 3 millones de euros en el año 2022 y un equipo de 35 empleados (10 en oficinas y 20 en planta), es crucial garantizar la seguridad de su infraestructura tecnológica tanto en IT como en OT, especialmente considerando el nivel medio-alto de automatización de sus procesos industriales y la importancia de la cadena de frío y la trazabilidad en su producción.

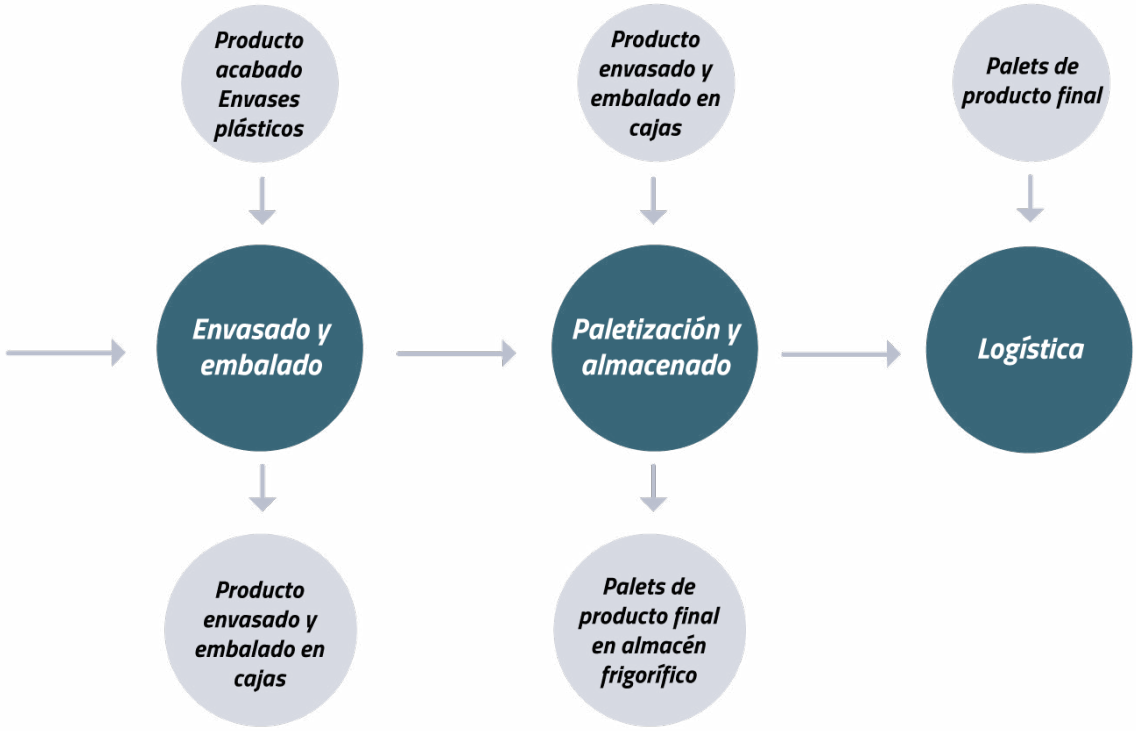
—2.7.2 Descripción del contexto y entorno industrial

ACME cuenta con un horario de producción de lunes a viernes, con dos turnos, y dispone de tres líneas de fabricación independientes.



Cada una de estas líneas pasa por diferentes etapas en la cadena de producción, que incluyen la entrada de materia prima, troceado y triturado, preparado, envasado y embalado, paletización, almacenado y logística. Estos pasos son críticos para el correcto funcionamiento de la empresa y requieren de una gestión eficiente y segura de los sistemas informáticos y los datos asociados.





PROCESO	DESCRIPCIÓN
ENTRADA DE MATERIA PRIMA	▪ Entrada de material en camiones frigoríficos (descarga manual). ▪ Monitorización y registro continuo de condiciones de almacenes frigoríficos. ▪ Registro de trazabilidad de cada pieza de carne que entra a la planta (manual, lectura código barras con pistola). ▪ Almacenamiento (manual) de la materia prima en armarios frigoríficos. ▪ Ordenación de materia prima (manual dentro de los almacenes frigoríficos) en función de sus características.
TROCEADO Y TRITURADO	▪ Registro de trazabilidad de cada pieza de carne que entra a la cadena (manual, lectura código barras con pistola). ▪ Retirada manual de partes de grasa de piezas enteras (manual). ▪ Entrada de piezas de carne enteras en máquina troceadora (automatizado, tornillo sinfín). ▪ Entrada de trozos de carne en trituradora (automatizado, cinta sinfín). El nivel de trituración en función de tipo de producto final a obtener.
PREPARADO	▪ En función del tipo de lote a fabricar, la materia prima se coloca en moldes –bandejas- específicos (proceso manual). ▪ Preparación de la carne en horno industrial (automatizado). ▪ Enfriamiento de la carne preparada (automatizado) en zona de enfriado mediante aire.
ENVASADO Y EMBALADO	▪ Proceso de envasado (automatizado) donde cada lote requiere de los envases de plástico específicos. La materia prima se coloca en el molde (volcado) y se cierra con plástico transparente mediante termosellado. ▪ Impresión de pegatina de datos de trazabilidad y pegado en el envase (automatizado). Lectura automática de la etiqueta mediante escáner (automatizado). ▪ Colocación de los envases en cajas (manual). Las cajas empleadas son universales para todo tipo de lotes. ▪ Impresión de etiqueta de caja y pegado en lateral de la misma (automatizado).
PALETIZACIÓN Y ALMACENADO	▪ Apilamiento de cajas (manual) en palets y colocación (manual) en paletizadora. ▪ Cubrimiento de plástico en paletizadora (automatizado). ▪ Impresión de etiqueta con contenido de palets (albarán) y pegado en exterior (automatizado). Lectura automática de la etiqueta mediante escáner. ▪ Transporte de palets a almacén frigorífico de lotes finalizados (manual). ▪ Monitorización y registro continuo de condiciones de almacenes frigoríficos.
LOGÍSTICA	▪ Extracción de palets a zona de expediciones (manual). ▪ Carga de palets en camiones frigoríficos, previa lectura (manual) del código de barras (albarán).

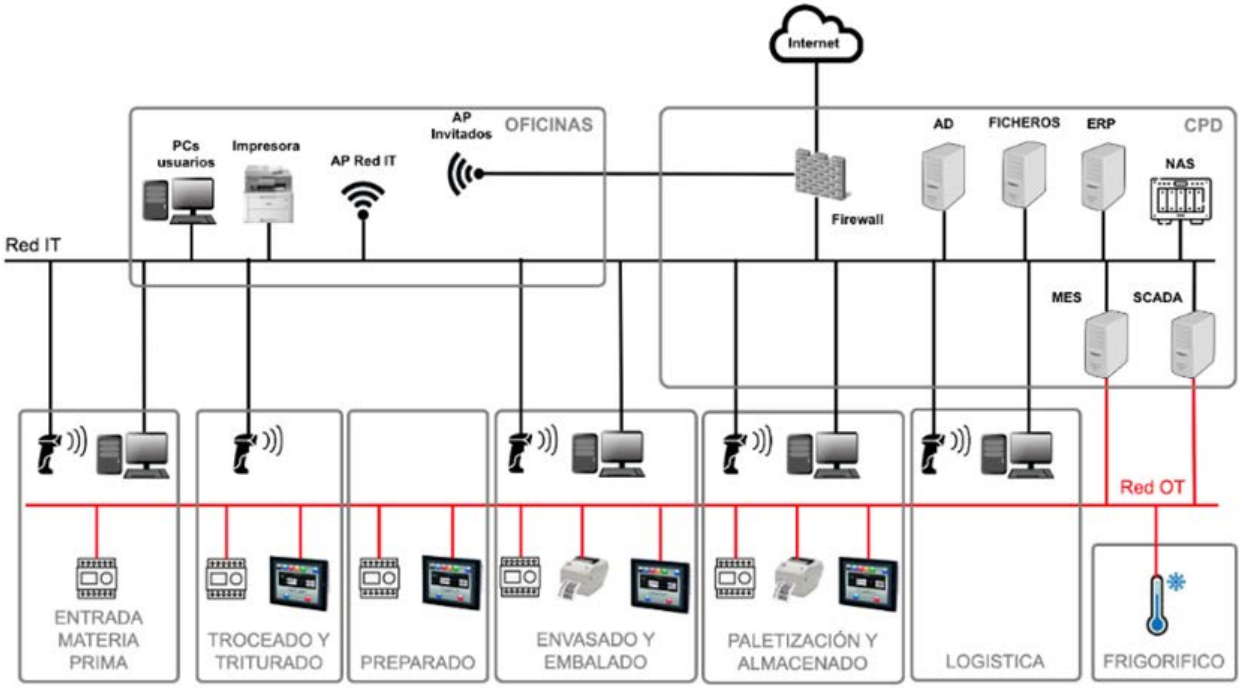
—2.7.3 Desafíos y riesgos

Dada la creciente amenaza de ataques cibernéticos en el entorno industrial, es fundamental que ACME esté preparada para hacer frente a posibles riesgos de seguridad. Algunos de los desafíos y riesgos específicos que enfrenta ACME en su entorno industrial incluyen:

- **Riesgo de interrupción de la cadena de producción:** un ciberincidente podría afectar negativamente las operaciones de las líneas de producción, lo que podría provocar retrasos en la producción, pérdida de ingresos, pérdida de lotes de producción debido a la ruptura de la cadena de frío, imposibilidad de disponer de una trazabilidad adecuada de los lotes fabricados, etc.
- **Riesgo de acceso no autorizado a los sistemas y datos:** los datos sensibles relacionados con la cadena de frío y la trazabilidad de los productos podrían ser comprometidos si un atacante logra acceder a los sistemas de ACME sin autorización.
- **Riesgo de manipulación de datos:** si un atacante logra acceder y manipular los sistemas de ACME, podría introducir cambios no autorizados en los registros de producción, lo que podría afectar la calidad y seguridad de los productos.
- **Riesgo de robo de propiedad intelectual:** ACME podría enfrentar amenazas de robo de su propiedad intelectual, como recetas y procesos de producción, que podrían ser utilizados por competidores o vendidos en el mercado negro.
- **Riesgo en la calidad final del producto:** Los sistemas interconectados en cualquier red disponible en ACME pueden ser víctimas de un ataque para comprometer el proceso de cualquiera o todas las líneas de producción, por ejemplo, alterando el funcionamiento de los frigoríficos, el proceso de enfriamiento por aire, e incluso datos erróneos impresos en las pegatinas.

—2.7.4 Infraestructura tecnológica existente

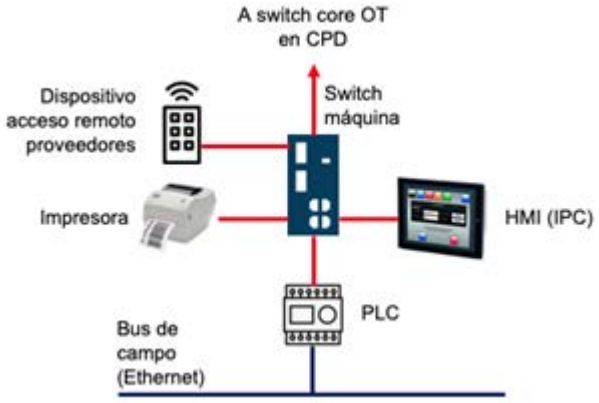
A día de hoy, ACME cuenta con la siguiente infraestructura:



ENTORNO IT

PROCESO	DESCRIPCIÓN
Red	▪ Único direccionamiento para todos los elementos de la red alámbrica y para la red inalámbrica corporativa. ▪ Dos switches core en -stack- en CPD del que nacen los enlaces físicos a los puestos de oficinas y servidores del CPD ▪ La electrónica de red no se ha actualizado ni modificado desde su instalación hace ya tres años.
Tipología de elementos conectados a red corporativa	▪ PCs de personal de oficinas (Dirección, Administración, Comercial). ▪ PCs de personal de producción, incluyendo los puestos del personal de mantenimiento. ▪ PCs en planta para acceso a ERP, correo, etc. ▪ Impresoras de oficina. ▪ Servidores IT y OT (éstos con una interfaz también en OT –dual homed-). ▪ Pistolas y lectores de códigos de barras físicamente en la planta.
Cortafuegos	▪ Únicamente filtrado de la conexión a Internet, pero sin limitaciones en cuando a destinos/servicios. ▪ Se emplea como medio de acceso remoto (VPN) al personal interno a la red de la oficina en teletrabajo y en puestos itinerantes (Dirección, Comercial). Usuario + Contraseña de dominio. Acceso ANY:ANY una vez conectado.
Red inalámbrica corporativa	▪ Únicamente filtrado de la conexión a Internet, pero sin limitaciones en cuando a destinos/servicios. ▪ Se emplea como medio de acceso remoto (VPN) al personal interno a la red de la oficina en teletrabajo y en puestos itinerantes (Dirección, Comercial). Usuario + Contraseña de dominio. Acceso ANY:ANY una vez conectado.
Red inalámbrica invitados	▪ Únicamente filtrado de la conexión a Internet, pero sin limitaciones en cuando a destinos/servicios. ▪ Se emplea como medio de acceso remoto (VPN) al personal interno a la red de la oficina en teletrabajo y en puestos itinerantes (Dirección, Comercial). Usuario + Contraseña de dominio. Acceso ANY:ANY una vez conectado.
Puestos	▪ Antivirus comercial (EPP, no EDR) con licencia vigente. Se actualizan directamente desde Internet. ▪ Todos los equipos son Windows 10 u 11, con actualizaciones automáticas desde Internet. ▪ Los usuarios son administradores locales. ▪ No hay control sobre los dispositivos USB que se pueden conectar a los puestos.
Servidores	▪ Sistema de virtualización formado por dos servidores. o La versión del sistema de virtualización no se ha actualizado desde su instalación hace ya tres años. o El sistema de virtualización dispone de la posibilidad de balanceo automático de las VM en caso de caída de un nodo, pero se encuentra deshabilitado y requiere intervención manual. ▪ Directorio Activo: o Todos los equipos IT, incluidos servidores, dentro del dominio corporativo. o Política de caducidad, longitud, complejidad de contraseñas habilitada para usuarios. o Los administradores de dominio no tienen política de contraseñas y no se ha cambiado desde su despliegue.
Copias de seguridad	▪ Existe una NAS en la que diariamente (de forma automática) se realiza una copia de las VMs del sistema de virtualización. ▪ Debido a las limitaciones del espacio de almacenamiento, se mantienen en la NAS únicamente copias que permiten restaurar a una semana atrás. ▪ Cada semana (el fin de semana) se obtiene una copia (no cifrada) de los datos de la NAS en un disco USB externo (dos discos que se van alternando cada lunes), y que se guardan en un armario localizado en las propias oficinas (en esta ubicación está el disco de la semana siguiente, encontrándose conectado a la NAS el de la semana en curso). ▪ La NAS no se ha actualizado desde su puesta en marcha desde hace 3 años.
Servicios	▪ Existe una NAS en la que diariamente (de forma automática) se realiza una copia de las VMs del sistema de virtualización. ▪ Debido a las limitaciones del espacio de almacenamiento, se mantienen en la NAS únicamente copias que permiten restaurar a una semana atrás. ▪ Cada semana (el fin de semana) se obtiene una copia (no cifrada) de los datos de la NAS en un disco USB externo (dos discos que se van alternando cada lunes), y que se guardan en un armario localizado en las propias oficinas (en esta ubicación está el disco de la semana siguiente, encontrándose conectado a la NAS el de la semana en curso). ▪ La NAS no se ha actualizado desde su puesta en marcha desde hace 3 años.

ENTORNO OT

PROCESO	DESCRIPCIÓN
Red	▪ Un único direccionamiento para todos los elementos conectados a la red de planta. ▪ La red de planta no dispone de conexión a Internet de ningún tipo. ▪ En el CPD hay un switch core al que se encuentran conectada una interfaz de los servidores OT y del que nacen los enlaces a los switches de máquina (formato DIN Rail, no gestionables).
Máquinas presentes en la red OT	▪ Las líneas pueden producir cualquier producto final, con modificaciones (estimado en 4h). ▪ Cada proceso de fabricación de cada línea está asociado a una máquina. ▪ Cada máquina ha sido proporcionada por una ingeniería distinta, aunque con una estandarización en cuanto a fabricantes de automatismos. ▪ La arquitectura común de la conectividad de las máquinas es la siguiente:  Los enlaces en color rojo disponen de direccionamiento en la red de planta. Los enlaces en color azul se corresponden con el bus de campo (red interna) de la máquina. Cada ingeniería ha empleado un direccionamiento no acordado (de hecho, las dos máquinas que emplean el mismo).
Accesos remotos	▪ Tanto el personal de mantenimiento como los proveedores disponen de acceso a los PLC a través de la VPN corporativa. ▪ En alguna máquina, y por petición expresa del proveedor, se dispone de un dispositivo de acceso remoto (propiedad y gestionado por el propio proveedor, encendido de forma permanente) para poder acceder de forma remota a la máquina. Este dispositivo requiere conexión a Internet y se proporciona mediante una tarjeta SIM disponible en el propio dispositivo.
Componentes en red de planta	▪ El despliegue de los PLC se ha hecho "por defecto", y no se han configurado medidas nativas de seguridad en los mismos. ▪ Los HMI están basados en un visor del SCADA que se ejecuta sobre un sistema operativo Windows 7. Estos puestos se inician con un autologon con un usuario sin privilegios. No disponen de ningún tipo de protección de seguridad y no se encuentran actualizados.
Servidores	▪ Servidores OT en configuración dual-homed: una interfaz en IT y otra en OT. ▪ Sistema operativo MS Windows 2019. ▪ Actualizaciones automáticas deshabilitadas. ▪ Sin protección de seguridad de ningún tipo (firewall de host desactivado).
Acceso a PLCs desde estaciones de ingeniería en red IT	▪ Se dispone del entorno de programación de los PLC en el servidor con el SCADA. ▪ El personal de mantenimiento inicia sesión vía RDP en el SCADA con su usuario de dominio.
Copias de seguridad	▪ No se dispone de copias de seguridad de los HMI (IPC), aunque únicamente llevan SO + visualizador SCADA. ▪ Los programas de los PLC se encuentran en el servidor SCADA (donde se encuentra el entorno de programación), aunque en algunos casos han perdido la trazabilidad de los programas en caso de que el proveedor haya estado realizando modificaciones frecuentes.

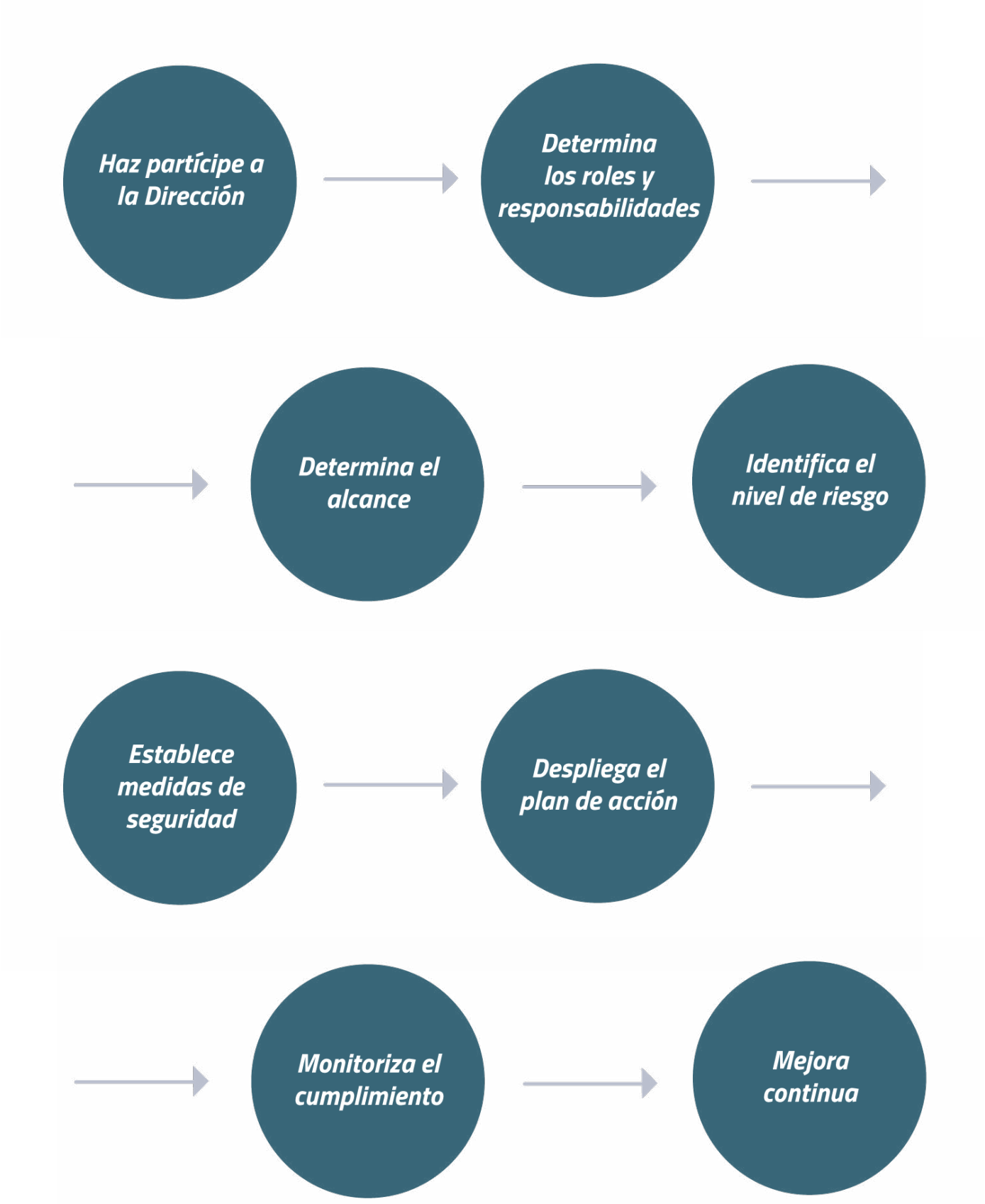
—2.7.5 Contexto de la situación

A continuación, se detallan los puntos relevantes que ponen de manifiesto la necesidad de abordar un proyecto que permita comenzar a gestionar la ciberseguridad:

PUNTO CRÍTICO	DESCRIPCIÓN
Falta de formación y concienciación en ciberseguridad para los empleados	La empresa no ha proporcionado ninguna capacitación o información sobre ciberseguridad tanto para los empleados de IT (Tecnología de la Información) como para los de OT (Tecnología Operación). Esto implica que los empleados no están familiarizados con las mejores prácticas de seguridad y no están conscientes de los riesgos asociados con las amenazas cibernéticas.
Ausencia de auditorías de seguridad	La empresa nunca ha llevado a cabo auditorías de seguridad de ningún tipo. La falta de evaluaciones periódicas de seguridad pone en riesgo la integridad de los sistemas y los datos, ya que no se identifican las vulnerabilidades o posibles brechas de seguridad existentes
Carencia de conocimientos de ciberseguridad del personal a cargo de las infraestructuras IT	La persona encargada de gestionar las infraestructuras IT y los puestos de cliente no posee conocimientos adecuados en ciberseguridad. Para tareas más complejas, se depende de una empresa de IT local, pero solo se solicita su ayuda cuando se necesita un servicio específico. Esto implica que no se cuenta con una persona interna capacitada para manejar adecuadamente los aspectos de seguridad en la infraestructura de IT y OT.
Falta de conocimientos de ciberseguridad por parte del personal de mantenimiento	El personal de mantenimiento no tiene conocimientos en ciberseguridad y, aunque los sistemas OT no están conectados a Internet, existe la posibilidad de que puedan ser vulnerables a ataques internos o incidentes de seguridad causados por descuidos o negligencia.
Fraude sufrido por el CEO debido a la falta de formación	Recientemente, la empresa experimentó un fraude al CEO, aunque el importe no fue significativo. Sin embargo, este incidente podría haberse evitado fácilmente si el usuario del departamento de Administración hubiera recibido una mínima formación sobre cómo reconocer y evitar estafas o ataques de phishing.
Detección de malware a través del antivirus, pero fallos en el entorno cloud	El antivirus logró detectar y detener un malware conocido que se encontraba adjunto a un correo electrónico enviado por un cliente. Sin embargo, el entorno cloud en el que se encuentra el correo permitió el paso del archivo adjunto, lo que indica una falta de medidas de seguridad adecuadas en el entorno en la nube.
Problemas debido a fallos físicos y falta de respaldo del código en el servidor corporativo	Debido a un fallo físico en uno de los controladores lógicos programables (PLC), una línea de producción estuvo parada durante tres días debido a la falta de piezas de repuesto. Además, al intentar reiniciar la línea, se encontró que la última versión del código de programación no se encontraba en el servidor corporativo. Esto demuestra una falta de planificación y una deficiente gestión de respaldos, lo que puede resultar en interrupciones prolongadas y pérdida de datos críticos.
Conflictos de IPs en puesta en marcha de nuevos componentes	La excesiva visibilidad en la red de los elementos de planta ha causado algún problema en la puesta en marcha de alguno de los componentes, al introducir en la red dispositivos con IPs que ya se encontraban asignados a otros.
Fallos humanos en modificaciones en PLCs	En alguna ocasión, y por error humano, se han realizado subidas de programas modificados a PLCs que no se correspondían.

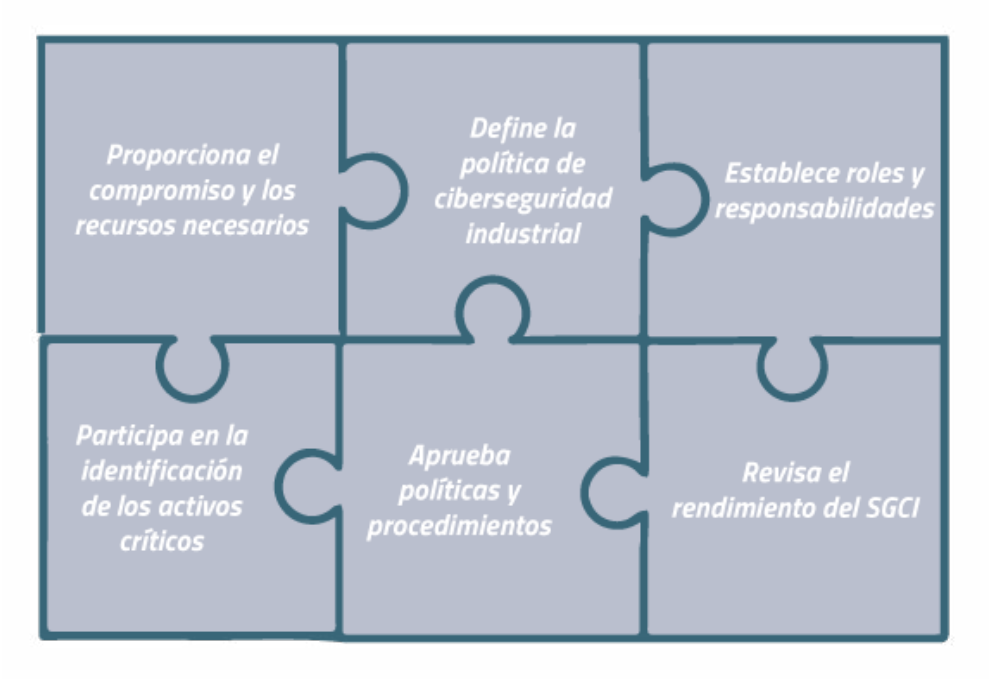
En resumen, la empresa presenta una serie de deficiencias en materia de ciberseguridad, incluyendo la falta de formación y concienciación para los empleados, la ausencia de auditorías de seguridad, la carencia de conocimientos de ciberseguridad en el personal a cargo de las infraestructuras IT, la falta de conocimientos en ciberseguridad del personal de mantenimiento, incidentes de seguridad como el fraude al CEO y la detección de malware, así como problemas causados por fallos físicos y la falta de respaldo del código en el servidor corporativo. Estas deficiencias representan riesgos significativos para la empresa y su capacidad de proteger sus sistemas, datos y operaciones.

3 DESARROLLO DE UN SGCI



3.1 Haz partícipe a la Dirección

La dirección es crucial en el desarrollo del SGCI porque proporciona el compromiso y los recursos necesarios para garantizar que el SGCI sea un éxito. Der forma resumida, la Dirección es necesaria porque:



- Proporciona el compromiso y los recursos necesarios: La dirección es responsable de proporcionar los recursos necesarios para la implementación y mantenimiento del SGCI. Esto incluye recursos financieros, tecnológicos y humanos. Además, la dirección debe demostrar un compromiso claro y visible para asegurar que el SGCI sea un éxito.
- Define la política de ciberseguridad industrial: La dirección es responsable de definir la política de ciberseguridad industrial de la organización. Esta política establece el compromiso de la organización con la ciberseguridad industrial y establece los objetivos y principios básicos del SGCI, asegurándose de está alineada con los objetivos estratégicos de la organización.
- Establece roles y responsabilidades: La dirección es responsable de definir los roles y responsabilidades para la gestión de la ciberseguridad industrial. Esto incluye la designación de un responsable de ciberseguridad industrial y la definición de los roles y responsabilidades de otros miembros del equipo.
- Participa en la identificación de los activos críticos: La dirección debe participar activamente en la identificación de los activos industriales críticos y la evaluación de los riesgos asociados con ellos. Esto incluye identificar los sistemas y datos críticos para el negocio, así como las amenazas y vulnerabilidades que pueden afectarlos.

- Aprueba políticas y procedimientos: La dirección es responsable de revisar y aprobar las políticas y procedimientos de ciberseguridad industrial. Esto asegura que estas políticas y procedimientos estén en línea con los objetivos y principios básicos establecidos en la política de ciberseguridad industrial.
- Revisa el rendimiento del SGCI: La dirección es responsable de revisar regularmente el rendimiento del SGSI y asegurarse de que se estén cumpliendo los objetivos establecidos. Esto incluye la revisión de los informes de auditoría y la realización de revisiones periódicas del SGCI para identificar áreas de mejora.

Aplicación Práctica

La aplicación práctica de este punto implicaría las siguientes acciones:

1) Proporcionar compromiso y recursos necesarios: La alta dirección debe asignar los recursos financieros, tecnológicos y humanos necesarios para implementar y mantener el SGCI. Esto implica asignar un presupuesto adecuado, proporcionar la infraestructura tecnológica requerida y asegurar la disponibilidad de personal capacitado en ciberseguridad.

2) Definir la política de ciberseguridad: La dirección debe elaborar una política de ciberseguridad que refleje el compromiso de la organización con la protección de sus activos críticos. Esta política establecerá los principios, objetivos y lineamientos generales para la gestión de la ciberseguridad en la organización, asegurando que esté alineada con los objetivos estratégicos.

3) Establecer roles y responsabilidades: La dirección debe definir los roles y responsabilidades específicos para la gestión de la ciberseguridad. Esto implica designar un responsable de ciberseguridad o un equipo encargado de liderar las actividades relacionadas con la seguridad de la información y asignar responsabilidades claras a otros miembros del personal.

4) Participar en la identificación de activos críticos: La dirección debe participar activamente en el proceso de identificación de los activos industriales críticos y en la evaluación de los riesgos asociados. Esto implica colaborar con expertos en seguridad para identificar los sistemas y datos más importantes para el negocio, así como las amenazas y vulnerabilidades que podrían afectarlos.

5) Aprobar políticas y procedimientos: La dirección debe revisar y aprobar las políticas y procedimientos específicos relacionados con la ciberseguridad. Esto garantiza que dichas políticas y procedimientos estén alineados con la política de ciberseguridad establecida y que reflejen las mejores prácticas y estándares relevantes.

6) Revisar el rendimiento del SGCI: La dirección debe realizar revisiones periódicas del desempeño del SGCI para evaluar si se están cumpliendo los objetivos establecidos y para identificar áreas de mejora. Esto puede involucrar la revisión de informes de auditoría interna o externa, la realización de revisiones de cumplimiento y la evaluación de incidentes de seguridad pasados.

En resumen, la aplicación práctica de este punto implica que la dirección de la organización asuma un papel activo y de liderazgo en el establecimiento, implementación y supervisión del SGCI, proporcionando los recursos necesarios, definiendo políticas y responsabilidades, participando en la identificación de riesgos y activos críticos, aprobando políticas y procedimientos, y revisando regularmente el desempeño del SGCI. Esto garantiza que la ciberseguridad se aborde de manera integral y efectiva en la organización.

3.2 Determina los roles y responsabilidades

En los entornos IT y OT existen roles y responsabilidades clave que son fundamentales para garantizar que los sistemas se desarrollen, implementen y mantengan de manera segura y eficaz. Algunas de estas funciones y responsabilidades son:

ROL	DESCRIPCIÓN
Responsable de Seguridad	Este rol tratará de garantizar la seguridad de los sistemas de IT y OT. Sus funciones principales serán: identificar y mitigar los posibles riesgos de seguridad, así como las filtraciones de datos y accesos no autorizados. También deberá asegurar de que los sistemas cumplan con los estándares y regulaciones de seguridad y de cumplimiento pertinentes.
Administrador de sistemas y red	Responsable de administrar y mantener los sistemas y las redes de IT y OT. Debe asegurarse de que las redes estén en funcionamiento, que los datos se transmitan correctamente y que cualquier problema de rendimiento y de operativa se resuelva de rápida, oportuna y eficazmente.
Arquitecto de la infraestructura IT/TO	Diseña y desarrolla la arquitectura general de los sistemas de IT y OT, así como sus integraciones. Estará al tanto y comprenderá (o mejor, será experto) de los requisitos de negocio, y de todos los datos que se recopilan y el modo de cómo se integrarán con otros sistemas. Definirá junto con el administrador la escalabilidad de los sistemas utilizados.
Jefe de proyectos	Será el responsable de administrar los proyectos de IT y OT. Su misión es garantizar que cada uno de los proyectos se completen e integren a tiempo, cumpliendo el presupuesto asignado y con cumpliendo los compromisos y estándares de calidad requeridos. Llevará adicionalmente la gestión de los riesgos del proyecto y las expectativas de los departamentos usuarios finales.
Integrador de sistemas	Su rol será integrar los sistemas de IT y OT, asegurando que los sistemas se comuniquen de manera efectiva y que los datos se compartan sin problemas entre ellos. Realizará las pruebas de usabilidad y las verificará y contrastará con las áreas usuarias de la empresa. También deben asegurarse de que los sistemas sean compatibles y definirá playbooks para la resolución de incidencias
Soporte y mantenimiento	Este rol es responsable de proporcionar soporte técnico para los sistemas de IT y OT, y brindar asesoramiento a los usuarios y escalar los problemas al soporte de nivel superior si es necesario. También deben asegurarse de que los sistemas se mantengan y actualicen regularmente para evitar que surjan problemas.

Aplicación Práctica

Para adaptar la definición de roles al caso de uso propuesto (PYME de 20 empleados, con un solo Técnico dedicado específicamente a las tareas IT/OT) la dirección de la empresa, que es la encargada de definir los roles del SGCI tienen la difícil tarea de aunar varios de los roles y disponer por medio de contratación de servicios profesionales de los otros roles o perfiles necesarios.

Así y para este caso concreto, la empresa dispondrá de un responsable de IT con capacidad suficiente para asumir las funciones de Seguridad y Administrador de Red y arquitecto de los sistemas IT/OT. Podrá adicionalmente asumir roles en la tera de formación y concienciación del resto de empleados de la empresa.

Tendrá que contar con el apoyo y los recursos de la gerencia en la tarea de contratar y atender los servicios externos que se encarguen de las nuevas implantaciones y del soporte y mantenimiento de todas las plataformas.

En conjunto con los responsables de negocio colaborará en la atención de la Auditorías de Seguridad necesarias para establecer el Plan para la consecución del SGCI.

3.3 Determina el alcance

El establecimiento del alcance del Sistema de Gestión de la Ciberseguridad Industrial es fundamental para centrar los esfuerzos de acuerdo con las capacidades y recursos disponibles en la organización. El objetivo es identificar con exactitud los procesos industriales que se verán implicados en el desarrollo del SGCI sobre el cual se comenzarán a establecer las medidas a bajo detalle definiendo un modelo de mejora continua.

El alcance del Sistema de Gestión de Ciberseguridad Industrial debe estar alineado con las estrategias corporativas, por lo que los procesos de negocio y sistemas críticos para la organización deben incluirse en el alcance y en la planificación del SGCI, ya que condicionará los niveles de protección a incorporar.

Como recomendación general, es mejor centrarse en desplegar correctamente el SGCI en un ámbito concreto, que tratar de abarcar todos los procesos industriales de una organización, que puede ser contraproducente en cuanto a la necesidad de recursos y medios requeridos.

OBJETIVO

Establecer un alcance bien definido, formalizado y donde se identifiquen claramente los límites del sistema de gestión a aplicar dentro de la Organización, ayudará a definir una metodología de implantación adecuada. Esto facilitará la gestión del SGCI hasta alcanzar un nivel de madurez lo suficientemente adecuado que pueda trasladarse de manera natural a otros procesos industriales que no se hubieran incluido dentro del alcance inicial.

Con esta sistemática también se garantiza la compatibilidad con otros posibles sistemas de gestión implantados, de tal manera que a la hora de priorizar los requerimientos de seguridad todos éstos se alineen parar mejorar la protección sin afectar a la disponibilidad.

Como ya se viene señalando en capítulos anteriores, la gestión de la ciberseguridad industrial debe constar en la política de seguridad corporativa y a mayores reflejar el apoyo de la alta dirección y de los responsables pertinentes, no solo a niveles estáticos de cumplimiento normativo, sino de manera dinámica y de mejora continua a lo largo del tiempo. De esta forma, con la implicación de estas figuras, la gestión de la ciberseguridad industrial se alineará con los objetivos estratégicos, lo que se verá reflejado en el aumento de la madurez del sistema dando el soporte necesario a los responsables del SGCI en la consecución de sus objetivos.

Aplicación Práctica

Es la primera decisión importante que se debe considerar y que delimitará de manera exacta lo que se encuentra protegido en Acme. Considerando la magnitud de la Organización de 35 empleados y una facturación de 3 millones de euros al año, no tendría sentido que el alcance del SGCI incluyese todos o la mayoría de los aspectos de negocio. Se deberá reducir a un conjunto de áreas o ubicaciones que se estime que son esenciales.

Siendo el negocio la preparación de cárnicos, es indispensable que la cadena de producción con sus diferentes etapas se considere como crítico y sean el elemento esencial a incluir en el alcance del SGCI. Por tanto, dispositivos y la información que puedan manejar, que formen parte de cualquiera de las tres líneas de producción que soportan los procesos de entrada de materia prima, troceado y triturado, preparado, envasado y embalado, paletización, almacenado y logística, se incluirán en el alcance.

Teniendo en cuenta lo descrito anteriormente, se incluirá cualquier dependencia que intervenga directa o indirectamente con los procesos, por ejemplo, proveedores externos, mantenimiento, conexiones remotas, etc. Se considerarán los accesos remotos del personal de mantenimiento y proveedores a los PLC a través de la VPN corporativa, al igual que las máquinas habilitadas con internet de manera puntual por proveedores.

Además, se deberá incluir cualquier servidor que contenga información sensible y que pudiese suponer un problema para la pérdida de integridad o confidencialidad, como por ejemplo la doble interfaz IT-OT de los servidores dual-homed con sistemas operativos MS Windows 2019 desactualizados y sin ningún tipo de protección.

De esta forma se abordarían y gestionarían los principales riesgos derivados de las amenazas emergentes que podrían afectar a Acme, como la interrupción de la cadena de producción, accesos no autorizados a los sistemas y datos, manipulación de datos o robos de propiedad intelectual.

3.4 Identifica el nivel de riesgo

El análisis de riesgos es un proceso mediante el cual se identifican y evalúan los daños potenciales de las operaciones de una organización, sus activos o personas con base en la probabilidad de que una amenaza se materialice, el impacto resultante en términos de daños materiales, económicos, prestigio, propiedad intelectual, etc. y las contramedidas adicionales que lo mitigarían.

En la siguiente imagen se puede ver un ejemplo de matriz de riesgos en el que se tienen en cuenta los términos anteriormente descritos:

Probabilidad	Muy probable	Media	Alta	Alta
	Posible	Baja	Media	Alta
	Improbable	Baja	Baja	Media
		Insignificante	Impacto moderado	Grave

Es necesario conocer los riesgos y las amenazas a los que está expuesta nuestra organización, de tal manera que a partir de ese análisis se puedan establecer medidas para reducir el impacto en las operaciones.

Cada organización gestiona de diferente manera los riesgos a los que están expuestos sus activos industriales. Esto se debe a que el mismo dispositivo en diferentes organizaciones, o incluso en diferentes localizaciones dentro de la misma infraestructura, presentan diferentes peligros teniendo en cuenta a los procesos que pueden afectar en caso de que sean comprometidos.

Como base en un análisis de riesgos y que una PYME, como por ejemplo en el caso de uso, debería abordar para conocer los riesgos a los que está expuesta la Organización, debería incluir la siguiente lista de acciones:

- Definir las personas que estarán involucradas en el análisis. De las personas que forman la empresa, identificar las personas responsables y conocedoras de los procesos, tanto de planta como gente que podría intervenir de oficinas.
- Definir el grupo de activos que ejecutan procesos automatizados u otros que impacten sobre los procesos y que se deban incluir en el análisis. Se debe tener en cuenta que el nivel de automatización es medio/alto y priorizar en el análisis de riesgos los activos que intervengan en los procesos críticos de cadena de frío y trazabilidad. Importante disponer de un inventario lo más actualizado posible y en el que se pueda identificar a qué proceso pertenece cada activo (entrada de materia prima, troceado y triturado, preparado, etc.).

- Seleccionar una metodología de análisis de riesgos en la cual:

  o Se identifiquen las amenazas a las que están expuestos los activos teniendo en cuenta las criticidades. Por ejemplo, analizar las amenazas que supone no tener filtrado a destino/servicios en el firewall, la conexión de equipos móviles personales a la red wifi, no actualización de NAS, equipos dual-home, no tener protección en el firewall industrial, etc.

  o Identificar las vulnerabilidades que podrían ser aprovechadas por las amenazas, Por ejemplo, qué vulnerabilidades presentan los equipos que no están actualizados.

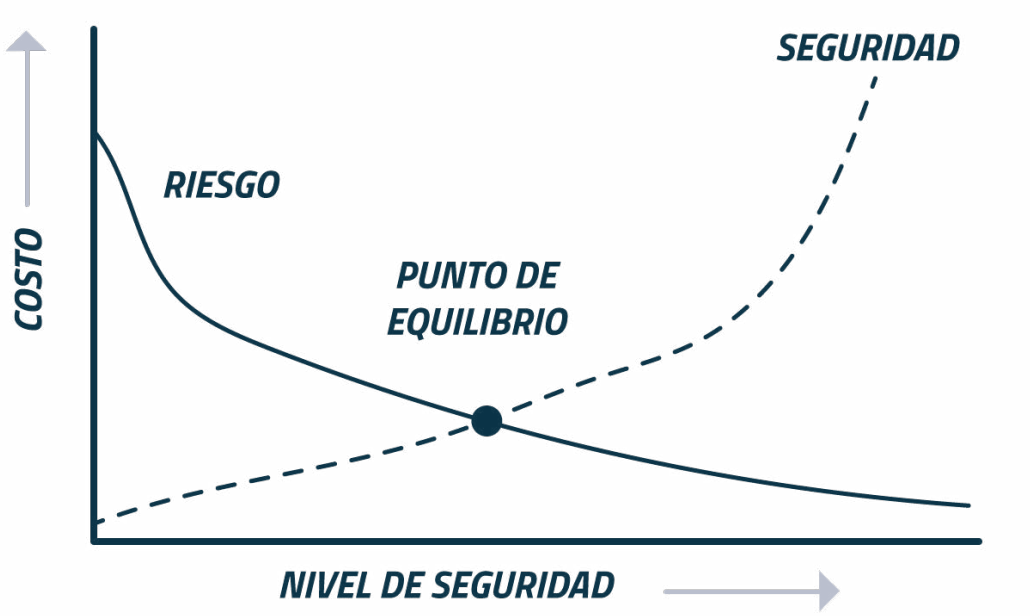
  o Evaluar el impacto derivado de la materialización de las amenazas. Se podría estimar la pérdida económica ocasionada en los 3 días en los que una línea estuvo parada por el fallo de un PLC. Principalmente evaluar las pérdidas económicas, el impacto de no entregar los productos cárnicos y el impacto reputacional.

  o Hacer una estimación del riesgo en términos de probabilidad: Riesgo = Amenaza x Vulnerabilidad x Impacto.

- Con base en los riesgos identificados, priorizar aquellos que son críticos para la Organización y aplicar medidas de seguridad para reducir la probabilidad de la materialización de una amenaza.

- Cuando se apliquen las medidas básicas de seguridad para reducir los riesgos en los procesos críticos, se podrían ir aumentando progresivamente a niveles más complejos para empezar a reducir los riesgos en otros procesos no tan críticos para el negocio.

Un aspecto clave es el nivel de seguridad que necesita la PYME acorde al negocio que genera, ya que habrá ocasiones que niveles de seguridad altos no sean rentables con el coste que supone. En la siguiente representación se puede observar el equilibrio para tener en cuenta entre coste y nivel de seguridad:



Aplicación Práctica

Por correspondencia a los puntos mencionados anteriormente y teniendo en cuenta el caso de uso, se resume de manera práctica cómo se podría aplicar la metodología de análisis de riesgos:

- En el análisis estarán incluidas las 35 personas que componen Acme, tanto las que se encuentran en oficinas como las que se encuentran en planta. Debido al nivel medio-alto de automatización, es de vital importancia garantizar la seguridad a través de las personas que tienen cualquier tipo de contacto sensible con el negocio, ya sean datos como conexiones desde/hacia a equipos de planta.

- Se define el conjunto de activos que impactan en el negocio de Acme. Para ello se puede utilizar la categorización de activos que se defina en la metodología de análisis de riesgos. Es importante que en el inventario actualizado se incluyan de cada tipología de activos la mayor cantidad de información, como los campos descripción, localización, propietario, responsable, versión SW/FW si aplicase, etc. A grandes rasgos y aterrizando los activos que se estiman que tienen impacto sobre el negocio, se podrían categorizar principalmente en:

  - Personal: las 35 personas de Acme como el personal externo, subcontratas o proveedores.

  - Datos o información (tanto a nivel de negocio como equipamiento): contenido almacenado en equipos o soportes de información, se podrían incluir claves criptográficas, copias de respaldo, registros de actividades, ficheros, etc.

  - Servicios: correo electrónico y almacenamiento en la nube, CRM en la nube.

  - Equipamiento informático (SW, HW): programas, aplicativos, Sistemas Operativos, servidores, antivirus, PCs, switches, routers, etc.

  - Equipamiento industrial (SW, HW, FW): PLC, HMI, RTU, CCTV, Telefonía IP, servidores, Sistemas Operativos, software de control, etc.

  - Redes de comunicaciones: VLAN, redes locales LAN, radio, etc.

  - Soportes de información: memorias USB, tarjetas de memoria, material impreso, etc.

  - Equipamiento auxiliar: fuentes de alimentación, generadores eléctricos, equipos destrucción, etc.

  - Instalaciones: recinto de Acme, edificio de oficinas y producción, instalaciones de recepción materias primas, líneas de producción, vehículos, etc.

- Una vez se ha elegido la metodología de análisis de riesgos, teniendo en cuenta la situación actual de la Organización, se deben identificar las amenazas que podrían impactar en el negocio. A alto nivel, se podrían elegir las derivadas de los principales riesgos (interrupción producción, accesos no autorizados, manipulación de datos y robo de propiedad intelectual). Continuando en más detalle, por ejemplo, se debería analizar las amenazas derivadas de no tener filtrados a destino/servicios en el firewall, conexiones de equipos móviles, NAS desactualizada, equipos dual-homed, etc.

- Acorde a las amenazas y riesgos identificados, se concretan las vulnerabilidades. En la Organización se contemplan vulnerabilidades asociadas a equipos de IT desactualizados (virtualización de servidores o electrónica de red), direccionamientos únicos en redes corporativas, conexiones por dispositivos móviles propios a la red WiFi, etc. En cuanto al entorno OT, trazamos vulnerabilidades conocidas respecto a equipos de campo, servidores y otros componentes (PLC con comunicaciones RDP en el SCADA, Estaciones de ingeniería, SCADA con datos, HMI con Windows 7, servidores dual-homed MS Windows 2019 desactualizados, etc.) teniendo en cuenta el inventario y amenazas.

- ¿Qué impacto supone sobre Acme la materialización de las amenazas establecidas? Principalmente evaluar las pérdidas económicas, el impacto de no entregar los productos cárnicos y el impacto reputacional.

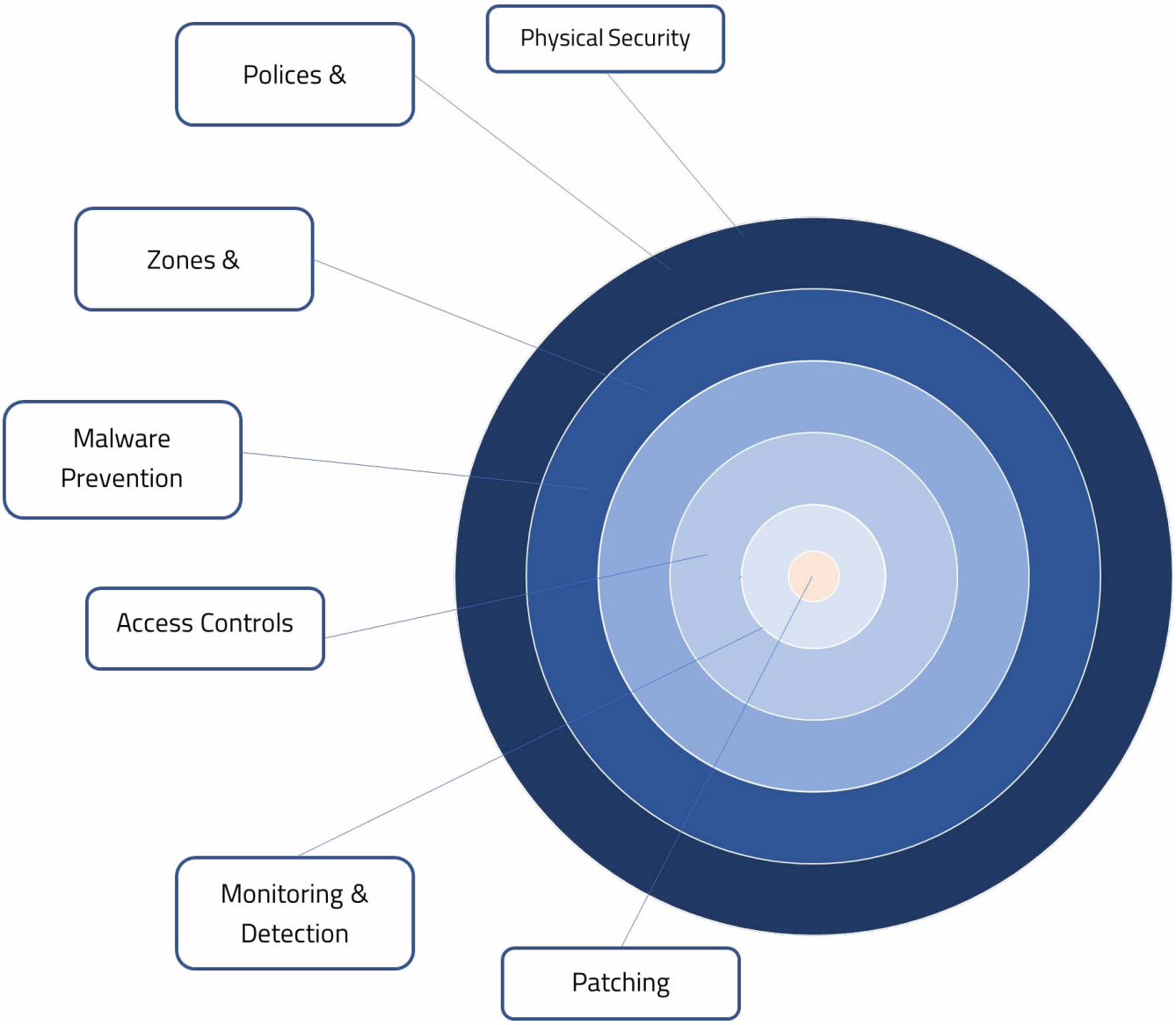
  Se puede realizar una estimación económica con base en el impacto que ocasionó la parada de tres días debido a un fallo en los PLC, considerar competidores directos para establecer el impacto que supone no entregar el producto y la pérdida de cliente, y pérdidas reputacionales asociadas a lo comentado anteriormente u otras casuísticas. También se puede tener en cuenta el fraude al CEO que se ha experimentado recientemente, que, aunque no impactó significativamente, podría haberlo hecho y haber supuesto un impacto grave en el negocio.

- Finalmente se estimará el riesgo en términos de probabilidad. Este paso se realizará en términos cuantitativos (si se ha optado por asociar valores numéricos) o cualitativos, que se tendría en cuenta la matriz adjuntada (probabilidad vs impacto).

  Por ejemplo, amenazas y los riesgos asociados a la interrupción de la cadena de producción: se establece que la probabilidad de que las amenazas identificadas se materialicen a través de las vulnerabilidades de los activos sea "posible" o con una probabilidad de nivel medio. El impacto sería "grave", por lo que obtendríamos según la matriz, que el riesgo es "alto". En base a la categorización de cada uno de los casos se actuaría en los siguientes pasos.

- El establecimiento de medidas de seguridad, desarrolladas en el siguiente apartado, se deberá hacer de manera progresiva teniendo en cuenta el balance costo-nivel de seguridad. En el caso de Acme, se podría empezar separando la red IT de la de OT y posteriormente segmentar ambas con diferentes direccionamientos. Concretamente en el entorno OT por VLAN por ejemplo para cada línea de producción o tipologías de equipo.

3.5 Establece medidas de seguridad



Al establecer las medidas de seguridad que resultan de realizar nuestro análisis de riesgos es imprescindible tomar en consideración las peculiaridades propias del entorno Operativo (OT) en comparación con los entornos de Tecnología de la Información (IT). Estas diferencias fundamentales influyen en cómo se deben abordar e implementar las estrategias de ciberseguridad.

Los entornos OT se caracterizan por la obsolescencia de sus dispositivos, el uso de protocolos propios del mundo industrial y su interacción directa con el mundo físico. Los dispositivos en estos entornos pueden estar en funcionamiento durante décadas, mucho más allá del ciclo de vida típico de los equipos de IT. Esto plantea desafíos únicos, ya que muchos de estos sistemas no fueron diseñados con la ciberseguridad en el diseño y pueden no ser compatibles con las medidas de seguridad modernas. Como resultado, las consecuencias de un incidente de seguridad en un entorno OT pueden ir más allá de las pérdidas financieras y de datos, provocando daños físicos y riesgos para la seguridad humana.

Dadas estas diferencias, es evidente que las medidas de seguridad deben ser adaptadas y específicas para los entornos OT, tomando en cuenta sus particularidades y desafíos únicos.

Como consecuencia de estas peculiaridades la recomendación que realizamos es aplicar el enfoque denominado Defensa en Profundidad. Este enfoque se basa en la idea de que no hay una única medida de seguridad que sea infalible [o incluso, que, de existir, no siempre puede aplicarse], por lo que se deben implementar múltiples capas de seguridad apiladas de forma independiente. Así, si un atacante consigue superar una capa de seguridad, las capas adicionales deben ser capaces de detectar y detener el ataque. Esta aproximación se refleja entre otros en la norma IEC62443 que articula como las capas de defensa deben implementarse en múltiples niveles, incluyendo políticas y procedimientos, controles físicos y controles técnicos que cubran todos los niveles de la organización.

A continuación, se detallan una serie de medidas de seguridad que podrían llegarse a implementar en una PYME, desglosándolas en los siguientes grupos en función del nivel de prioridad en la implantación:

Las medidas de seguridad aquí expuestas son orientativas y se recomienda se vayan aplicando de forma progresiva a medida que la organización vaya aumentando su nivel de madurez de ciberseguridad industrial.

—3.5.1 Medidas de nivel básico

Tipo de medida	Medida de seguridad	Descripción
Medidas Organizativas	Los roles y las	Definir formalmente los roles y las responsabilidades con respecto a ciberseguridad tanto de la parte IT como de OT
Medidas en la red	Separación de la red IT/OT	Separar las redes IT-OT es una medida fundamental para disponer de una base mínima de seguridad en la red. Es necesario disponer de un cortafuegos que controle las comunicaciones que pudieran producirse entre IT-OT y establecer políticas para su control. Aquellos sistemas que pudieran encontrarse entre ambos entornos se deben ubicar en zonas desmilitarizadas (DMZ) que puedan servir de punto de intercambio de información entre amas redes.
Medidas organizativas	Charlas de concienciación	Impartir charlas de concienciación a todo el personal de forma que adquieran una concienciación mínima en relación a la ciberseguridad para tratar de evitar riesgos innecesarios en la operación diaria.
Medidas físicas	Controles físicos de entrada de equipos de terceros	Definir un procedimiento de control de acceso físico de los equipos de terceros que acceden a las instalaciones para realizar intervenciones in-situ, como: comprobación de la instalación de software de protección instalado y actualizado, firewall del equipo activado, etc.

—3.5.2 Medidas de nivel inicial

Tipo de medida	Medida de seguridad	Descripción
Medidas Técnicas	Inventario de activos	Completar un inventario de activos sobre los dispositivos, componentes y sistemas existentes en la red OT, con el objeto de disponer de la información que permita: identificarlos de forma inequívoca en la red, conocer sus vulnerabilidades, así como los requerimientos de comunicaciones.
Medidas en la red	Segmentación de la red OT	Se deberían de identificar tanto las zonas de seguridad que consiste en una agrupación lógica de activos físicos, sistemas de información y aplicaciones que comparten requisitos de seguridad comunes e identificar los conductos como la agrupación lógica de flujos de comunicación, que conectan dos o más zonas.
Medidas en la red	Gestión de accesos remotos a planta	Se debe de disponer de sistemas que permitan gestionar y controlar el acceso remoto de terceros a la red OT, así como revisarlos -y gestionarlos- periódicamente. Se debe contemplar asimismo un acceso remoto alternativo en aquellos casos que debido a una emergencia no sea posible el uso o acceso a través del acceso principal. Estos accesos remotos de terceros tienen que seguir los controles y procedimientos de la planta, no los que el proveedor de servicios considere.
Medidas en la red	Revisión de políticas de seguridad en cortafuegos	Se deben de realizar revisiones periódicas de las reglas y las políticas de los cortafuegos existentes, evitando que se expongan innecesariamente en Internet servicios, así como mantenerlos actualizados. De forma general, desde las redes OT no se dispondrá de conectividad a Internet.
Medidas físicas	Controles físicos de entrada	Identificar las zonas seguras (oficinas, salas e instalaciones), que se consideren como puntos críticos, y deben protegerse mediante controles físicos en la entrada y puntos de acceso adecuados.

—3.5.3 Medidas de nivel medio

Tipo de medida	Medida de seguridad	Descripción
Medidas técnicas	Control de Usuarios	Establecer sistemas robustos de autenticación, preferiblemente de doble factor, así como favorecer la existencia de una gestión centralizada de los mismos, para permitir realizar un seguimiento del usuario y de las actividades que haya podido realizar en los sistemas.
Medidas Técnicas	Protección de puesto	Instalar protección antimalware en las estaciones de trabajo para la detección de código y actividad maliciosa. En caso de que no sea posible su instalación (incompatibilidad, retrocompatibilidad, ...), desplegar soluciones basadas en técnicas de "whitelisting". Si fuese posible el despliegue de soluciones de detección y respuesta (EDR), sería recomendable para poder actuar sobre ellas en el caso de incidente.
Medidas Organizativas	Procesos y procedimientos de protección de la información	Se recomienda la creación de políticas y procedimientos de seguridad basados en estándares de seguridad específicos y aplicables a entornos industriales como por ejemplo NIST, IEC 62443, etc.
Medidas en la red	Microsegmentación de la red	Desplegar medidas de seguridad en la red de aquellos equipos, procesos industriales de la organización que, por el uso de protocolos propietarios, antigüedad, criticidad, imposibilidad de implementar protección nativa, etc. deben disponer de un mayor grado de protección.
Medidas Técnicas	Monitorización equipos y tráfico de red	Desplegar soluciones de seguridad que permitan la monitorización de los equipos que se encuentran dentro de la red industrial, de forma que sea posible disponer de una alerta temprana frente a posibles eventos de seguridad.
Medidas Organizativas	Auditorías de seguridad	La realización de hacking éticos, auditorías de seguridad permite identificar vulnerabilidades y desplegar medidas para corregirlas.

—3.5.4 Medidas de nivel avanzado

Tipo de medida	Medida de seguridad	Descripción
Medidas	Continuidad del Negocio	Establecer medidas y planes de continuidad del negocio que contemplen la pérdida o afectación de los equipos o sistemas industriales que dispone la empresa, como por ej. copias de seguridad, realización de simulacros, existencia de equipos de reemplazo para sistemas críticos, desvío de la producción a terceros, etc.
Medidas	Procesos y procedimientos de protección de la información específicos por sector	Se recomienda ampliar/modificar las políticas y procedimientos de seguridad implantadas con aquellos basados en estándares específicos aplicables a cada uno de los sectores como, p. ej. CLC50701 (ferroviario), R155/R156 (Automoción) y otros similares.
Medidas	Concienciación y formación avanzada	Definir y ejecutar un plan de formación y concienciación sobre seguridad de la información y operación que incluya a todos los empleados de la organización para cumplir con sus deberes y responsabilidades relacionados con la ciberseguridad conforme a las políticas y procedimientos definidos.
Medidas Técnicas	Bastionado Wifi	Implementar medidas de seguridad en los puntos de acceso WIFI existentes en la red OT. Especial atención en aquellos casos en los que existan dispositivos IoT.
Medidas Técnicas	Servicios de monitorización externos	Establecer un servicio de monitorización y vigilancia de ciberseguridad 24x7 con el objetivo de monitorizar y dar servicio de seguridad.
Medidas Técnicas	Servicios de pruebas de seguridad	Es recomendable probar la efectividad de los controles de seguridad implantados, bien sea de manera activa, cuando sea posible, pasiva o creando una réplica de la planta en un entorno de simulación (cyber range)
Medidas	Parcheado de equipos	Realizar un control del software/firmware/... instalado tanto en los PLC, estaciones de control, SCADA, etc. de forma que sea posible identificar las vulnerabilidades que pudieran presentar, y realizar la actualización o parcheo de los equipos acodadas y planificadas con operaciones. Se puede plantear un parcheo virtual para no detener la producción.

Aplicación Práctica

A continuación, se detalla la aplicación práctica, considerando el caso de uso planteado, en relación a las medidas de nivel básico e inicial.

Descripción del caso Práctico

La empresa ACME está preocupada por la ciberseguridad debido al aumento de ataques que se han dado en su sector y que han afectado a la operación de algunas de ellas, incluso en algunos casos se ha llegado a parar la producción durante un periodo de tiempo, además en el pasado la empresa ACME ha tenido algún susto de carácter menor como el fraude del CEO aunque con un importe poco significativo, se recibió un correo con un fichero adjunto con un virus pero el antivirus de la parte IT lo logro detener, no han afectado a la operativa diaria de la empresa pero ha supuesto un toque de atención para la dirección.

Debido a esta situación, desde la dirección ha definido un plan que permita mejorar el nivel de seguridad de que dispone la organización, mediante la inversión en una serie de medidas de seguridad que mejoren el nivel de seguridad, para ello ha contratado a una empresa de seguridad que le ayude en este cometido y plantean la implantación de medidas de seguridad en capas conforme al concepto de seguridad en profundidad.

Para ello se han empezado la implantación de medidas en la parte físicas de un modo inicial que son empresas que no tienen ningún tipo de medida de seguridad, estas consisten en:

Controles físicos de entrada

Se han establecido medidas de seguridad en la planta para evitar que personal ajeno a la empresa ACME pueda estar dentro de ella sin control, para ello se han instalado un sistema de CCTV, tornos, así como identificaciones para personal externo.

Con respecto al personal interno se han establecido lector de huellas, para identificar los trabajadores que se encuentran dentro de la planta, así como tornos, de acceso, etc.

Control de acceso físico de personas, equipos (portátiles, USB, servidores, PDA, etc).

Se ha definido un proceso en el que los responsables de planta no permiten el acceso de equipos de terceras personas salvo casos excepcionales a la Red de la empresa ACME sin una previa identificación de los mismo y con la revisión por parte del técnico de IT de que disponen de unas medidas de seguridad mínimas como son antivirus actualizado a la última versión disponible y el firewall del equipo activado, siempre serán acompañados por personal de la empresa para comprobar las actividades que llevan a cabo.

Además, se han limitado los equipos que pueden acceder por parte del personal de planta y se ha establecido la revisión de los equipos periódicamente con el objetivo de que se disponga de antivirus corporativo actualizado y el firewall activado

Se ha procedido a la compra de USB con lector de huella y que los custodia el departamento de IT que les examina un antivirus periódicamente para evitar la distribución de malware dentro de la red de OT.

Se ha prohibido la entrada de ningún otro equipo fuera de los que están inventariados y controlados por parte del técnico de IT.

Seguridad en la red

Para conocer el estado de seguridad actual de que dispone la empresa ACME se ha procedido a contratar un empresa externa que realice revisiones periódicas de las reglas y las políticas establecidas en el Firewall de IT, el objetivo es conocer el grado de actualización si las políticas establecidas son las correctas, soporte de que dispone, además como resultado de la auditoría se detecta que no tiene ningún tipo de mantenimiento y que las reglas del firewall no se encuentran actualizadas, se contrata un servicio de soporte que incluya revisiones periódicas y defina las políticas a establecer, así como ayudar en la propuesta de mejoras en la red que permitan disponer de un mayor grado de madurez con respecto a la ciberseguridad, como son segmentación de la RED IT/OT, definir los flujos de comunicaciones, monitorizar los flujos, realizar una microsegmentación de los procesos industriales que tienen protocolos propietarios y son muy antiguos para establecer otro tipo de medidas de seguridad, etc.

Gestión de Acceso Remotos

Para que accedan a la red interna tanto por parte de terceros como personal de la planta, la empresa ACME dispone de una VPN, se contrata a una empresa externa que realice revisiones periódicas, activando los logs de la VPN para comprobar quiénes acceden, se crean grupos de usuarios con limitación de privilegios (acceso basado en roles) tanto de usuarios internos como externos, para que no puedan acceder a todos los equipos de la red, además se define una política de seguridad de contraseña con complejidad y caducidad de la contraseña (Ejemplo más de 10 caracteres con complejidad incluidos números y caracteres especiales, caducidad de la contraseña cada 90 días, etc.).

Se define un procedimiento para la petición de acceso remoto tanto para personal interno como externo, así como definiendo a que recursos se pueden acceder y cuales se limitan o necesitan autorizaciones expresa.

3.6 Despliega el plan de acción

El despliegue del plan de acción representa un hito crucial en la implementación de un Sistema de Gestión de la Ciberseguridad Industrial (SGCI), ya que es en esta etapa donde las estrategias y medidas de seguridad previamente establecidas se activan para proteger los sistemas de tecnología de la información y operacionales (IT/OT) de la organización.

Es esencial iniciar este proceso con un diseño meticuloso del plan de acción, asegurándose de que todas las medidas estén alineadas con los objetivos del SGCI y sean viables considerando los recursos disponibles. Este diseño deberá tener en cuenta los recursos humanos, técnicos y financieros, y verificar que son suficientes para garantizar un despliegue exitoso.

La criticidad y la naturaleza de los sistemas IT/OT hacen imprescindible la formación y sensibilización en ciberseguridad de todas las personas involucradas, no sólo en la implementación del plan de acción, sino también en la operación diaria de los entornos y procesos que se quieren proteger. Esta formación deberá ser transversal, implicando a todos los niveles de la organización, desde la dirección hasta el personal operativo.

Recomendamos desplegar el plan de manera progresiva, iniciando con una fase piloto en un entorno controlado. Posteriormente, se puede proceder con una implementación parcial por departamentos o áreas, y finalmente, una implementación a escala completa en toda la organización. Esta estrategia permite una gestión más eficaz de los posibles contratiempos, reduciendo su impacto en las operaciones y facilitando la detección temprana de posibles incidentes.

Es fundamental establecer un sistema robusto de seguimiento y coordinación durante el despliegue. Este sistema de monitorización debe ser capaz de evaluar el progreso y detectar rápidamente cualquier desviación o problema que pueda surgir.

La capacidad para adaptarse durante el despliegue del plan es otro elemento crítico. Es probable que surjan necesidades de ajustes debido a problemas detectados, cambios en el entorno IT/OT u otros factores. Por lo tanto, es imprescindible contar con un proceso preestablecido para la gestión de estos cambios, que permita evaluarlos y decidir sobre su implementación de manera efectiva y sin comprometer el éxito del despliegue ni los estándares de ciberseguridad deseados.

Es importante tener en cuenta que durante el diseño o despliegue del plan de acción pueden surgir riesgos que deben ser identificados y gestionados. Estos pueden estar relacionados con la implementación de las medidas de seguridad, la gestión de los cambios, entre otros aspectos. Se deben implementar medidas de mitigación para prevenir o reducir su impacto.

La comunicación efectiva es otro pilar esencial durante el despliegue. Se deben establecer canales y estrategias de comunicación claras y eficientes que permitan mantener informados a todas las partes implicadas, fomentando su compromiso y colaboración en el proceso.

Finalmente, es crucial recordar que el despliegue del plan de acción no es un fin en sí mismo, sino un paso más en el camino hacia la mejora continua de la ciberseguridad en la organización. La experiencia y los conocimientos adquiridos durante el despliegue deben ser utilizados para revisar y mejorar el SGCI, en un ciclo constante de aprendizaje y mejora de la madurez de la organización, siempre alineado a los requerimientos del negocio y a la política de riesgos de la organización.

3.7 Monitorizar para obtener una mejora continua

La mejora continua es un proceso que deberá formar parte de un sistema de gestión de la ciberseguridad industrial, por dos razones principalmente:

1. Como método para mejorar sistemáticamente el desempeño (eficacia, eficiencia) del sistema de gestión, optimizando los procesos y controles de seguridad (análisis y tratamiento de riesgos, continuidad, cumplimiento, formación, concienciación, ...) a partir del análisis de las métricas de rendimiento.

2. Como herramienta para lograr la adecuación permanente del sistema de gestión a los cambios relevantes del contexto interno y externo de una organización.

Adicionalmente, a lo anterior, si la organización pretende certificar el sistema de gestión ("para serlo y parecerlo") la mejora continua es un requisito normativo necesario.

Pero, más allá del cumplimiento normativo ¿cuál es la importancia que actualmente tiene el proceso de mejora continua por la que todo responsable de seguridad industrial debería tenerlo en consideración?

Valor de la mejora continua

Los beneficios que justifican porqué prestar atención, dedicar recursos e implantar un proceso de mejora continua en una PYME se pueden concretar en las cuatro ventajas para el negocio siguientes:

- Adecuarse a los cambios, ya sean organizativos, operativos, regulatorios, tecnológicos o de requisitos de clientes, que deberán ser tratados para mantener la posición competitiva y supervivencia de la organización.

- Aprovechar las lecciones aprendidas de la organización extraídas de la experiencia, en particular, de los incidentes de seguridad para evitar su repetición.

- Tomar decisiones de optimización de los procesos y los controles de seguridad de la organización, a partir de la medición del desempeño y el análisis de su eficacia y eficiencia,

- Poner en valor las propuestas de mejora de las personas de la organización, colaboradores o proveedores para mejorar cualquier aspecto de la seguridad y protección de los activos derivado de la práctica.

En definitiva, se trata de aprovechar un recurso de la organización, tan valioso como la información resultado de sus operaciones de ciberseguridad que además "está ahí" disponible para su uso.

Aplicación Práctica

Enfoque de la mejora continua en la ciberseguridad industrial

En el apartado 2.1 (Qué es un SGCI) de esta Guía se hace referencia al ciclo PDCA (acrónimo de las iniciales en inglés de Planificar, Hacer, Verificar y Actuar), o Ciclo de Deming como una metodología reconocida para la mejora de los procesos de seguridad.

A continuación, se propone una visión general de cómo implantar la mejora de la seguridad en el ámbito de un Sistema de Gestión de Ciberseguridad Industrial (SGCI) teniendo, muy en cuenta, la viabilidad de su aplicación por una PYME en cuanto a su limitación de recursos personales y materiales.

Premisas y algunos ejemplos ("para mejorar, primero hay que medir")

Parece evidente, pues, que para obtener todo el potencial de beneficios que ofrece la mejora continua, la organización -como premisa- deberá haber implantado un Sistema de Gestión de Ciberseguridad Industrial.

Es decir, la implantación de los procesos de planificación, ejecución y control de los controles de seguridad permitirá establecer un cuadro de métricas que sean representativas y "hablen de su desempeño" mediante la evaluación de su eficacia y eficiencia.

A continuación, se aportan dos casos de evaluación, en ámbitos diferentes de actuación y a modo de ejemplo, como son las salvaguardas técnicas y las capacidades de los usuarios y los administradores.

1. La evaluación de las pruebas de recuperación de copias de seguridad o de funcionamiento de las fuentes de alimentación ininterrumpida (SAI). Las tasas no aceptables (será necesario fijar los límites) de recuperación de copias o de duración de los SAI nos "hablan" o "avisan" de su eficacia para poder actuar a tiempo corrigiendo los defectos encontrados, antes de recuperar una copia fallida o esperar que los tiempos de suministro de alimentación sean suficientes para guardar y apagar las sesiones activas, ante un fallo de energía eléctrica.

2. La evaluación de las acciones de concienciación de usuarios o de formación de administradores, serán significativas de la transferencia real de los conocimientos al puesto de trabajo. Las tasas no aceptables (será necesario fijar los límites) de concienciación y formación nos "hablan" o "avisan" de su eficacia para poder actuar a tiempo antes fallos o errores involuntarios de usuarios y administradores.

Ciclo de vida de la mejora ("de la oportunidad a la implantación y volver a empezar")

En una fase inicial del ciclo de vida de la mejora continua la organización identifica las oportunidades de mejora.

Una oportunidad de mejora se define como:

1. La inexistencia o insuficiencia de un requisito del sistema de gestión, sea de planificación, ejecución, control e incluso de mejora, considerándose una "no conformidad" de la organización. Por ejemplo, una inexistente política y/o ejecución de la actualización de parches de seguridad.

2. El incumplimiento, basándose siempre en una evidencia objetiva, que cree una duda razonable sobre la capacidad del sistema de gestión para cumplir los objetivos de seguridad de la organización. Asimismo, el hecho de no evidenciarse objetivamente la eficacia del control de seguridad, a pesar de ejecutarse y controlarse, también constituiría una oportunidad de mejora.

Por ejemplo, una deficiente ejecución de la actualización de parches de seguridad y en particular, los de implantación urgente.

Las fuentes de información para la identificación de las oportunidades de mejora de la organización podrán ser alguna de las siguientes:

- Análisis de riesgos de los sistemas de información.
- Evaluación de impacto en la privacidad de los tratamientos de datos personales responsabilidad de la organización.
- Auditorías, internas o externas, del sistema de gestión de seguridad.
- Revisiones de seguridad de los sistemas de información.
- Análisis de logs de la monitorización de la operación de los sistemas de información.
- Análisis de métricas de los procesos y controles del del sistema de gestión de seguridad.
- Incidentes y eventos de seguridad con impacto
- Observaciones de los usuarios durante las actividades diarias.

Evaluación de oportunidades de mejora ("seleccionar las de mayor impacto y menor coste")

Una vez, se identifica la oportunidad de mejora, la organización deberá evaluarla y priorizarla adecuadamente para su aprobación y asignación de responsable.

Para la selección de las propuestas de mejora, la organización podrá seguir un criterio de Coste/Beneficio de acuerdo con los dos criterios que siguen:

- Coste de la implantación de la oportunidad de mejora que representa la valoración de los recursos personales y materiales necesarios para la implantación de una mejora. Se debe considerar el coste debido a la no implantación de la mejora (sanciones por incumplimiento normativo, reclamaciones, daños en sustitución o recuperación de activos, etc.). Por ejemplo, los costes (de ejecución y almacenamiento) de reforzar las políticas de realización de las copias de seguridad de la organización.

- Beneficio de la implantación de la oportunidad de mejora que representa la valoración de la métrica asociada a un objetivo de seguridad.

Por ejemplo, una reducción del Punto de Recuperación Objetivo de las copias de seguridad de la organización.

El análisis Coste/Beneficio, en consecuencia, permitirá a la organización la toma de decisión de la aprobación de las oportunidades de mejora mediante su clasificación, tal y como se representa a continuación.

Análisis Coste-Beneficio de las oportunidades de mejora

Seguidamente, las oportunidades aprobadas por la dirección de la organización deberán asignarse a los responsables de su implantación, que procederán a su planificación detallada, lo que permitirá su seguimiento hasta el cierre y verificación de los resultados esperados.

Actores de la mejora de la mejora continua

A continuación, se resume una propuesta de distribución de responsabilidades para la gestión de la mejora continua teniendo en cuenta el contexto de una PYME en el ámbito de la ciberseguridad industrial.

Los roles que se han tenido en cuenta, de una manera simplificada son los siguientes:

- Dirección o CEO que ejercerá la Gerencia designada por la propiedad de la PYME. Así como el Comité de Dirección como órgano colegiado para la toma de decisión.
- Responsable de sistemas o CIO que ejercerá la persona designada por la dirección para la implantación y mantenimiento de los sistemas de información de gestión y control industrial (IT/OT).

- Responsable de seguridad o CISO que ejercerá la persona designada por la dirección para la definición, supervisión y reporting de los procesos y controles de los sistemas de información de gestión y control industrial (IT/OT), así como del sistema de gestión de seguridad. En muchas PYME, debido a su tamaño reducido, podrá coincidir las responsabilidades de sistemas y seguridad en la misma persona, lo que podrá llegar a plantear incompatibilidades o conflictos de interés.
- Usuarios, con diferentes niveles de responsabilidad, que utilizan los sistemas de información de la organización para el desarrollo de las operaciones del negocio.

La matriz de responsabilidades, conocida como RACI[2], para la gestión de la mejora continua, teniendo en cuenta el contexto de una PYME en el ámbito de la ciberseguridad industrial podrá ser la siguiente:

ACTIVIDAD/ ROL	Usuarios	Responsable del sistema	Responsable de seguridad	Gerencia / Comité de Dirección
Identificación oportunidad de mejora	REALIZA	REALIZA	REALIZA	
Evaluación de la oportunidad de mejora		REALIZA	REALIZA	
Aprobación de la oportunidad de mejora	INFORMADO	INFORMADO	INFORMADO	APRUEBA
Implantación oportunidad de mejora	INFORMADO	REALIZA	REALIZA	APRUEBA

[2]https://www.forbes.com/advisor/business/raci-chart/

GLOSARIO DE TÉRMINOS

Acrónimo/ Término	Significado	Descripción
IT	Information Technologies	Entorno IT hace referencia a las redes y servicios presentes en las redes de gestión de una empresa.
OT	Operational Technologies	Entorno OT hace referencia a las redes y servicios presentes en las redes de planta de una empresa.
Componente o dispositivo	-	Elemento concreto que forma parte de un SCI, como, por ejemplo: un PLC, un HMI, un variador, etc.
SCI	Sistema de Control Industrial	Es el conjunto de componentes que se encuentran configurados para el control de procesos industriales.
ERP	Enterprise Resource Planning	El ERP es un software que ayuda a automatizar y administrar los procesos empresariales de las distintas áreas de la empresa.
MES	Manufacturing Execution System	Un MES es un software que permite organizar, monitorizar y controlar los procesos de producción industrial para conseguir la máxima eficiencia y calidad.
FW	Firewall (cortafuegos)	Elemento de seguridad de red que permite gestionar el tráfico de red entrante y saliente que lo atraviesa, en función de parámetros como puerto/IP origen puerto/IP destino.
NGFW	Next Generation FireWall	Firewall de nueva generación que además de las funcionalidades de un firewall estándar permite aplicar medidas de seguridad avanzadas sobre el tráfico que lo atraviesa.
PLC	Programmable Logic Controller	También conocido como autómata programable, es un componente que supervisa continuamente el estado de sus entradas y toma decisiones mediante un programa para gestionar el estado de sus salidas.
HMI	Human Machine Interface	Es una interfaz o panel de control que permite a una persona operar contra el proceso industrial.

Guía para la gestión de la ciberseguridad en el entorno industrial de una PYME

www.ismsforum.es
info@ismsforum.es
(+34) 915 63 50 62

@ISMSForum
ISMS Forum

Una iniciativa de

isms forum
isms EUSKADI