MATRIZ DE AUDITORÍA DE CIBER RIESGOS

ENCRYPT 4.0

Cofinanciado por el programa Erasmus+ de la Unión Europea

El proyecto ENCRYPT4.0 (2020-1-RO01-KA202-079983) ha sido financiado con el apoyo de la Comisión Europea. Esta publicación refleja únicamente la opinión del autor, y la Comisión no se hace responsable del uso que pueda hacerse de la información contenida en ella.

Contenido

1. INTRODUCCIÓN 3

2. PROPUESTA DE VALOR DE CRAM 3

3. LA METODOLOGÍA DE LA MATRIZ DE AUDITORÍA DE CIBER RIESGOS 7

4. MATRIZ DE AUDITORÍA DE CIBER RIESGOS (CRAM) 8

4.1 CATEGORÍAS DE LA MATRIZ DE CIBER RIESGOS 8

5. AUDITORÍA DE CIBERSEGURIDAD 10

5.1 ¿QUÉ ES UNA AUDITORÍA DE CIBERSEGURIDAD? 10

AUDITORÍA DE CIBERSEGURIDAD vs. EVALUACIÓN DE CIBERSEGURIDAD 10

AUDITORÍA DE CIBERSEGURIDAD EXTERNA vs. AUDITORÍA DE CIBERSEGURIDAD INTERNA 10

5.2 ¿CÓMO REALIZAR UNA AUDITORÍA INTERNA DE CIBERSEGURIDAD? 11

VISIÓN GRÁFICA DEL PROCESO CON EL CRAM 20

6. PROYECTO Y CONSORCIO 21

BIBLIOGRAFÍA 22

ANNEX A - RECOPILACIÓN DE LAS NORMAS EXISTENTES PARA LOS RIESGOS DE CIBERSEGURIDAD 24

1. INTRODUCCIÓN

La productividad, la calidad y los costes de fabricación pueden beneficiarse potencialmente de importantes mejoras de la creciente conectividad de la Industria 4.0, el uso de las tecnologías de la información y el almacenamiento de datos fuera de las instalaciones. Sin embargo, existen riesgos asociados para las pymes manufactureras, por ejemplo, la posibilidad de que las entidades competidoras accedan a sus datos. Los ciberataques son cada vez más comunes y suelen emplearse para extraer o robar datos confidenciales y/o propios, manipular los datos capturados para causar efectos indeseados y destruir activos de capital (Margot Hutchins y Stefanie Robinson 2015). Los ciberataques pueden definirse como "un ataque cuyo objetivo es el uso del ciberespacio por parte de una empresa para interrumpir, desactivar, destruir o controlar maliciosamente un entorno/infraestructura informática; o destruir la integridad de los datos o robar información controlada" (National Institute for Standards and Technology 2012). El Foro Económico Mundial, FEM prioriza dos soluciones para hacer frente a los riesgos cibernéticos impulsados por la innovación: i) medir el riesgo cibernético y ii) evaluar la ciberseguridad (World Economic Forum 2017). En 2019, el fraude o robo de datos y los ciberataques, fueron identificados por el FEM como el cuarto y el quinto riesgo más probable de ocurrir (World Economic Forum 2020). En 2020 se identificaron los problemas de ciberseguridad, los ciberataques y el fraude o robo de datos, dentro de la lista de los 10 principales riesgos a largo plazo.

La industria manufacturera necesita herramientas para incorporar los riesgos cibernéticos a sus actuales procesos de gestión de riesgos. En este contexto, ENCRYPT 4.0 aborda esta necesidad identificada, centrándose en la evaluación de la ciberseguridad, mediante el desarrollo de una **Matriz de Auditoría de Ciber Riesgos**, por sus siglas en inglés, **CRAM** (**Cyber Risk Audit Matrix**). CRAM es una herramienta integral destinada a ayudar a los/as gerentes de las PYMEs manufactureras a realizar un análisis exhaustivo de sus procesos, teniendo en cuenta el uso de soluciones tecnológicas innovadoras basadas en la Industria 4.0, identificando los riesgos cibernéticos y apoyándolos en el diseño y establecimiento de controles eficaces. CRAM se ha desarrollado teniendo en cuenta la experiencia en las normativas nacionales, europeas y mundiales (Anexo A), así como los comentarios de expertos/as en ciberseguridad de seis países europeos: Austria, Portugal, Rumanía, Bulgaria, Chipre y España.

- Este documento contiene: a) la propuesta de valor del CRAM, b) la metodología del CRAM, c) la descripción de las categorías de la matriz de auditoría de los ciber riesgos, c) los pasos para realizar las auditorías de Ciberseguridad y, d) las referencias bibliográficas.

ENCRYPT 4.0 se centra en la evaluación de la ciberseguridad, mediante el desarrollo de la matriz de auditoría de ciber riesgos

2. PROPUESTA DE VALOR DE CRAM

La **Matriz de Auditoría de Ciber Riesgos (CRAM)** permitirá a las fábricas inteligentes realizar una visión sistemática de su panorama de riesgos cibernéticos y crear un perfil preciso del riesgo de amenazas cibernéticas. CRAM de Encrypt 4.0 permitirá a las fábricas inteligentes realizar un análisis de datos consistente en tiempo real y evaluar sus riesgos cibernéticos,

basándose en una matriz específica y extensa. CRAM es una herramienta analítica que ayudará a las empresas manufactureras a identificar, analizar, priorizar los riesgos y establecer medidas de protección con celeridad. En los últimos años, uno de los problemas más acuciantes del mundo digital es la ciberseguridad y la protección de la privacidad de los datos. En 2019, el Foro Económico Mundial (FEM) situó los ciberataques entre los cinco principales riesgos mundiales.

En el 2020, año marcado por la pandemia de la COVID-19, la mayor dependencia a la conectividad y a la infraestructura digital debido al bloqueo mundial, aumentó las oportunidades de intrusión y ataques cibernéticos. Al mismo tiempo, para maximizar los daños y los beneficios económicos, los ciberdelincuentes están desplazando su objetivo inicial (los individuos y las pequeñas empresas), a las grandes corporaciones, los gobiernos y las infraestructuras críticas, que desempeñan un papel crucial en la respuesta al virus (Interpol 2020). Así lo expresó Juncker (Former President of the European Commission): "Los ciberataques suponen más peligro para las democracias y las economías que las armas y los tanques" (Juncker 2017).

Cybersecurity Ventures, líder mundial en la investigación de la ciber economía global, predijo que "los daños globales relacionados con la ciberdelincuencia en 2021 alcanzarán los seis billones de dólares, lo que supondrá más que todos los desastres naturales en un año" (Morgan 2020). El informe "*Official Annual Cybercrime Report*" de 2019 afirmó que "a finales de 2016, una empresa fue víctima de un ataque *ransomware* cada 40 segundos" (Ventures 2019) y las predicciones apuntan a que esta cifra aumentará a cada 10 segundos en 2021. Los ciberataques a infraestructuras críticas, calificados como el quinto mayor riesgo en 2020 por la red de expertos del FEM, se han convertido en la nueva normalidad en sectores como la energía, la sanidad y el transporte. Sin embargo, la industria manufacturera está sufriendo un aumento de los ciberataques, tal y como figura en el informe "*2020 Data Breach Investigations Report*", que detalla 922 incidentes, 381 con revelación de datos confirmada solo en EEUU (Forum 2020; 15th Edition). Las organizaciones de ciberdelincuentes están uniendo fuerzas y se estima que su probabilidad de detección y persecución sea muy baja, sobre el 0,05% en Estados Unidos, *"el Cybercrime-As-A-Service* es un modelo de negocio creciente, ya que la creciente sofisticación de las herramientas en la *darknet* hace que los servicios maliciosos sean más asequibles y fácilmente accesibles por cualquier persona". (Forum_ 2020) La capacidad de defensa de las PYMES suele ser más débil en comparación con las empresas más grandes, y las cifras sugieren que sólo el 14% de las PYMES afectadas pueden recuperarse por sí solas. Además, la "*National Cyber Security Alliance"* afirma que el 60% de las pymes que sufren un ciberataque pierden su negocio en 6 meses, y las fábricas son más propensas a las amenazas a su seguridad, debido a su conectividad en los sistemas de TI y OT (*Operational Technologies*), a través de la digitalización de la Industria 4.0" (Yew 2017)

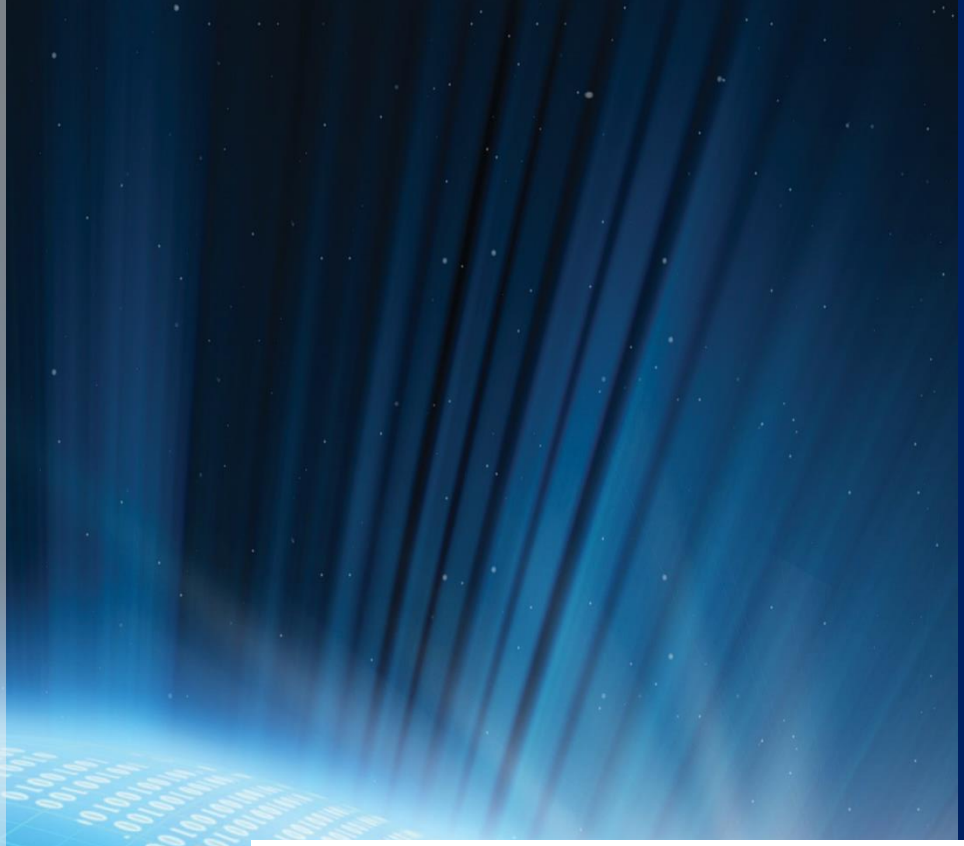
La mayoría de las empresas de fabricación, en su intento de mantener una ventaja competitiva adaptándose a las prácticas de la Industria 4.0, realizan esfuerzos esporádicos invirtiendo en sistemas de control y asesores externos, pero carecen de un enfoque integrado para la gestión de los ciber

riesgos. Sus esfuerzos no logran hacer frente a la rápida evolución de las ciberamenazas, porque la mayoría de los sistemas de fabricación se desarrollaron tradicionalmente para centrarse en la protección (de riesgos de naturaleza accidental) y el alto rendimiento, en lugar de la seguridad. Además, en lo que respecta a la seguridad, los fabricantes se preocupaban históricamente por asegurar su entorno OT, descuidando a menudo la seguridad TI, "la aparición de la Industria 4.0 introduce nuevas tecnologías en los entornos OT tradicionales, por lo que las personas familiarizadas con las OT que trabajan en estos entornos deben adaptarse" (EU Agency for Cybersecurity 2019). Pero los/as empleados/as suelen utilizar información potencialmente contradictoria para describir o evaluar algunos aspectos del ciber riesgo.

Por ello, CRAM esbozará indicadores de riesgos clave que se aplicarán fácilmente a los datos en tiempo real. CRAM también permitirá a los/as empleados/as no sólo elaborar una estrategia de ciberseguridad a largo plazo, sino también realizar rápidamente informes diarios. Esto mostrará los niveles de riesgo reales para los procesos en cualquier momento, de crucial importancia en el entorno de la fabricación, ya que mantener la producción en marcha es un aspecto crítico y la más mínima suspensión de cualquier proceso, puede tener un impacto irreparable y causar enormes pérdidas económicas. Los riesgos de seguridad industrial son cada vez más complejos y evolucionan, por lo que es muy importante dotar a las PYMES manufactureras de una herramienta analítica adecuada, para perfilar las precauciones que deben tenerse en cuenta en el día a día en el entorno de la fabricación. A diferencia de los fallos en procesos mecánicos, que pueden clasificarse como estáticos, los fallos de ciberseguridad son dinámicos, ya que están estrechamente relacionados con las interacciones humanas.

Por tanto, el **objetivo principal de CRAM** es proporcionar a los/as **responsables y/o gerentes de fabricación** una visión de los **posibles riesgos de ciberseguridad en sus sistemas** y ayudarles/as a **adoptar una estrategia eficaz para mitigar los riesgos**. Dado que la investigación en el campo de la evaluación de los riesgos de ciberseguridad en los sistemas de fabricación es limitada, **el CRAM de Encrypt 4.0** constituye una herramienta innovadora destinada a ser incorporada en la política de gestión de riesgos de las empresas de fabricación.

La matriz de auditoría de ciber riesgos esbozará indicadores de riesgos clave que se aplicarán fácilmente a los datos en tiempo real

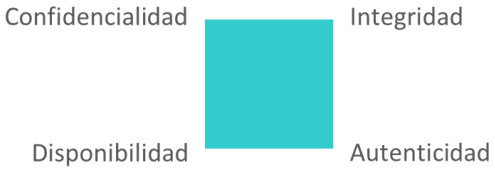


El objetivo principal del CRAM es proporcionar a los/as directivos/as de la industria manufacturera, una visión de los posibles riesgos de ciberseguridad en sus sistemas y ayudarles/as a adoptar una estrategia eficaz para mitigar los riesgos.

3. LA METODOLOGÍA DE LA MATRIZ DE AUDITORÍA DE CIBER RIESGOS

El CRAM se diseñó teniendo en cuenta el cuarteto "**CIAA**", siglas que provienen de las palabras en inglés ***"Confidentiality"*** (confidencialidad), ***"Integrity"*** (integridad), ***"Availability"*** (disponibilidad), y "***Authenticity***" (autenticidad). Para ello, CRAM medirá dos aspectos principales: la **Probabilidad de Riesgo** y el **Impacto del Riesgo**, adaptados para **responder** a las necesidades específicas de las PYME de la industria de la fabricación, con el potencial de ser fácilmente configurados y adaptados en la cultura organizativa individual de una empresa determinada.

El CRAM se diseñó teniendo en cuenta el cuarteto de la "CIAA"



El CRAM también contiene: i) los tipos de riesgos numerados, ii) las categorías de riesgo, iii) el origen de los riesgos, iv) la descripción de los riesgos, v) los costes potenciales asociados a las consecuencias de los riesgos, vi) departamento de la organización que podría verse afectado, vii) las acciones correctoras/aplicadas anteriormente, viii) impacto del riesgo, ix) probabilidad del riesgo, x) nivel de riesgo global, xi) factores desencadenantes, xii) mitigación/acciones a aplicar, xiii) costes potenciales de la mitigación, xiv) plazo, xv) persona responsable de la gestión del riesgo, xvi) supervisor responsable del seguimiento y xvii) evaluación de la eficacia.

A continuación, se describen los principales conceptos que componen la Matriz de Auditoría de Ciberriesgos:

Disponibilidad: Garantizando un acceso a la información a tiempo y de forma fiable.

Autenticidad: Garantizando las características de los datos de: ser auténticos y originales, capaces de ser verificados y la confianza en la validez de una transmisión, un mensaje o el emisor del mensaje. (Encrypt 4.0 project, 2020).

Evaluación de la ciberseguridad: Mecanismos de orientación y evaluación de la ciberseguridad mejorados, incluidos los principios comunes para las evaluaciones de la ciberseguridad, un mecanismo de puntuación basado en puntos de mejora y pasos prácticos, que permiten a las empresas evaluar y mejorar su preparación en materia de ciberseguridad (World Economic Forum 2017).

Confidencialidad: Preservar las restricciones (controladas) de acceso y divulgación de la información, incluidos los medios para proteger la intimidad personal y la propiedad intelectual.

Impacto: El impacto potencial evaluado resultante de un compromiso de la confidencialidad, integridad o disponibilidad de un tipo de información, expresado como un valor *bajo*, *moderado* o *alto*.

Integridad: Protección contra la modificación o destrucción indebida de la información e inclusión de la garantía al no rechazo y a la autenticidad de la información.

Probabilidad: Factor ponderado basado en un análisis subjetivo de la probabilidad de que una determinada amenaza sea capaz de explotar una determinada vulnerabilidad o un conjunto de vulnerabilidades.

Descripciones inspiradas en la Guía para la realización de evaluaciones de riesgos (National Institute of Standards and Technology, 2012).

4. MATRIZ DE AUDITORÍA DE CIBER RIESGOS (CRAM)

El CRAM de ENCRYPT4.0 representa una herramienta integral destinada a ayudar a los gerentes de las PYMES manufactureras a realizar un análisis exhaustivo de sus procesos teniendo en cuenta el uso de soluciones tecnológicas innovadoras basadas en la Industria 4.0 e identificar los riesgos cibernéticos y ayudarles a diseñar y establecer controles eficaces en el lugar.

4.1 CATEGORÍAS DE LA MATRIZ DE CIBER RIESGOS

Estas categorías provienen de una investigación y análisis de más de 20 normativas (Anexo A) en el campo de la seguridad de la información y la protección de datos, así como de 12 entrevistas en profundidad realizadas a expertos y expertas en materia de ciberseguridad de Austria, Portugal, Rumanía, Bulgaria, Chipre y España.

Tabla 1. Categorías de la Matriz de Auditoría de Ciber Riesgos

Categoría de Riesgo	Descripción de la Categoría de Riesgo
Recursos Humanos	Identificación de los riesgos relacionados con los recursos humanos de la empresa. Los riesgos relacionados con las funciones y responsabilidades del personal de la empresa, la toma de decisiones, la gestión de las identificaciones, el control de los accesos, la sensibilización...
Propiedad Intelectual	Identificación de los riesgos que se relacionan con la Propiedad Intelectual de la empresa. La Propiedad Intelectual incluye la Propiedad Industrial, los Derechos de Autor y los derechos afines, y confiere el derecho de uso exclusivo de la respectiva información técnica, comercial e industrial. La Propiedad Industrial tiene como objetivo proteger las invenciones, patentes, marcas y proyectos amparados por derechos de uso exclusivo, producción y comercialización.
Seguridad de los Sistemas de Control Industrial (SCI)	La seguridad SCI implica la custodia y la seguridad de los sistemas de control industrial, del software y hardware necesarios que utiliza el sistema.
Productos	Identificación de los riesgos relacionados con los productos. La aparición de este tipo de riesgos puede poner en peligro los productos fabricados por la organización.
Riesgos legales de ciberseguridad	Identificación de los riesgos relacionados con las responsabilidades legales y reglamentarias. La aparición de este tipo de riesgos puede poner en peligro las responsabilidades legales y/o reglamentarias de la organización.
Ataques a la cadena de suministro	Identificación de las vulnerabilidades en la cadena de suministro o de distribución. La organización debe definir, evaluar y gestionar los procesos de gestión de riesgos de la cadena de suministro y logística. Así como la identificación de los vínculos con proveedores con posturas de seguridad deficientes.
Tecnología, TIC y seguridad operativa	Identificación de los riesgos que están relacionados con la Tecnología, las TICs y las operaciones de la empresa. Hacer frente a los riesgos derivados de las insuficiencias de la funcionalidad prevista, de las perturbaciones operativas o del mal uso/errores razonablemente previsibles de los colaboradores relacionados con la tecnología, las TICs y las operaciones.
Clientes	La aparición de un determinado riesgo puede poner en peligro el servicio prestado a los/as clientes de la organización, o comprometer los datos de éstos/as.
Ciberseguridad física	La ciberseguridad física es la protección de los sistemas físicos cibernéticos, los dispositivos del IoT (*Internet of Things*), la protección de las personas, la propiedad y los activos físicos de las acciones y eventos que podrían causar daños o pérdidas.

5. AUDITORÍA DE CIBERSEGURIDAD

5.1 ¿QUÉ ES UNA AUDITORÍA DE CIBERSEGURIDAD?

La cuarta revolución industrial o Industria 4.0 ha traído consigo una serie de nuevas tecnologías que conectan los mundos físico y digital de los procesos empresariales en sistemas inteligentes integrados. Esto trae consigo muchas oportunidades para mejorar los procesos y el rendimiento general, pero también muchas nuevas responsabilidades y amenazas. El mayor nivel de conectividad entre todos los sistemas a través del IoT, la computación en la nube y muchas otras tecnologías, además de muchos beneficios, posee nuevos retos para las empresas relacionados con la seguridad de la información, Big Data, etc. que es procesada por estos sistemas integrados. Por ello, las empresas, y especialmente las PYMES, necesitan herramientas que les apoyen en el proceso de comprobación y análisis de sus puntos débiles en cuanto a la seguridad de las tecnologías de la Industria 4.0 que tienen implementadas. Es decir, esta herramienta eficaz para llevar a cabo esta comprobación, es la realización de una **auditoría de ciberseguridad**.

Una auditoría de ciberseguridad representa una evaluación del rendimiento con respecto a las especificaciones, normas, controles o directrices.

Una auditoría de ciberseguridad suele definirse como una evaluación del rendimiento con respecto a las especificaciones, normas, controles o directrices (CyLumena s.f.). Las auditorías de ciberseguridad suelen realizarse en función de una lista de control (o biblioteca de controles) que se define en función de unas normas de ciberseguridad (nacionales, internacionales e internas de la empresa) y/o de los procedimientos y/o políticas de la empresa. El objetivo de una auditoría de ciberseguridad es ayudar a las organizaciones a evaluar si cuentan con los mecanismos de seguridad adecuados, identificando las brechas de seguridad o validando los procedimientos y políticas aplicados. Las auditorías de ciberseguridad también ayudan a las empresas a verificar lo que existe en su red, lo que hay que proteger y las lagunas que existen en sus protecciones actuales para que puedan hacer mejoras (Dosal, 2020).

AUDITORÍA DE CIBERSEGURIDAD vs. EVALUACIÓN DE CIBERSEGURIDAD

En ciberseguridad, los términos “auditoría” y “evaluación” difieren. Mientras que la auditoría de ciberseguridad se refiere a si existen determinados controles establecidos, la evaluación de ciberseguridad tiene como objetivo evaluar la eficacia de estos controles (Aldorisio 2020). Aunque las evaluaciones pueden incluir algún grado de auditoría, no siempre es así. Las auditorías de ciberseguridad, dependiendo del objetivo, también podrían aplicarse cuando una organización quiere evaluar su cumplimiento de cierta ley o normas, en este caso normalmente la auditoría la realiza a través de un tercer actor externo competente en la materia. Las evaluaciones de ciberseguridad, por otro lado, podrían ser realizadas internamente, es decir, por personas de la organización que tengan un buen conocimiento de la infraestructura de ciberseguridad.

AUDITORÍA DE CIBERSEGURIDAD EXTERNA vs. AUDITORÍA DE CIBERSEGURIDAD INTERNA

Las auditorías externas son llevadas a cabo por profesionales, especialmente cuando el objetivo de la auditoría es proporcionar una base para la certificación bajo ciertas normas de ciberseguridad y la evaluación del cumplimiento de las normas oficiales, leyes, etc. Las auditorías internas de ciberseguridad (auditorías de primera parte) podrían ser realizadas por un experto interno que conozca bien los procesos de la empresa y la arquitectura de ciberseguridad. De acuerdo con la Ley General de Protección de Datos (Commission s.f.) – art. 37, 38 y 39 -, cada empresa está obligada a tener designada a un Delegado/a de Protección de Datos (un “*Data Protection Officer*”), encargada de la gestión de los datos: qué información entra y sale de la empresa, en qué procesos se utiliza y cómo se gestiona. Por lo tanto, una opción para llevar a cabo una auditoría interna de ciberseguridad podría ser realizada por la persona responsable de la protección de datos designada, o por un equipo de la empresa, dependiendo del alcance de la auditoría.

En las próximas secciones, presentaremos un enfoque combinado para llevar a cabo una auditoría y evaluación de ciberseguridad interna, basada en varias categorías antes mencionadas, que deben tenerse en cuenta en el proceso de auditoría.

5.2 ¿CÓMO REALIZAR UNA AUDITORÍA INTERNA DE CIBERSEGURIDAD?

El objetivo de esta sección es proporcionar una guía fácil de seguir, para la auto-realización de una auditoría de ciberseguridad (auditoría interna de ciberseguridad) que podría servir como herramienta eficaz para evaluar la ciberseguridad y la seguridad de los datos dentro de su organización y / o a modo de preparación para las auditorías externas de ciberseguridad (llevadas a cabo por terceras partes).

PASO 1: Definir las prioridades de seguridad de su organización y el alcance de la auditoría

En esta fase, la persona o el equipo designado para llevar a cabo la auditoría tiene que identificar cuál será el alcance del proceso de auditoría. Un buen punto de partida es hacer una lista de todos los ciber activos de la empresa, que podrían ser ciber activos asociados a activos críticos como: sistemas de control; sistemas de adquisición de datos; equipos de red; plataformas de hardware para máquinas virtuales o almacenamiento; sistemas secundarios o de apoyo como escáneres de virus, sistemas HVAC y sistemas de alimentación ininterrumpida UPS (*Uninterruptible Power Supplies*) (n.d., Versify Solutions);

A continuación, hay que evaluar cuáles son los ciber activos críticos o CCA (por sus siglas en inglés *Critical Cyber Assets*). Según la norma *"Critical Infrastructure Protection (CIP)",* versión 4 de la "*North American Electric Reliability Corporation (NERC)",* un CCA es "cualquier dispositivo que utilice un protocolo enrutable para comunicarse fuera del perímetro de seguridad ESP (*Electronic Security Perimeter*), que utilice un protocolo enrutable dentro de un centro de control, o que sea accesible por vía telefónica" (ThomasLangill 2015). En palabras más sencillas, los activos pueden variar desde equipos informáticos hasta diversos sistemas, e información sensible de clientes y empresas, documentación interna y sistemas de comunicación.

Una vez identificados los ciber activos críticos, habrá que identificar dónde se encuentran los **parámetros de seguridad críticos** y, por tanto, segmentar lo que se incluirá en el ámbito de la auditoría (LeCount 2019). Los parámetros de seguridad y los activos varían mucho de una empresa a otra, por lo que este paso inicial y la correcta definición del alcance de la auditoría son de crucial importancia para la eficacia del proceso de auditoría. Una vez definido el alcance de la auditoría, se puede pasar al siguiente paso: la identificación de las amenazas potenciales.

PASO 2: Identificar los riesgos y amenazas potenciales

Basándose en entrevistas en profundidad con 12 expertos/as en el campo de la ciberseguridad, el consorcio ENCRYPT 4.0 ha identificado nueve posibles categorías de riesgo y ha elaborado una lista de las amenazas potenciales que cada una de estas categorías puede suponer para los ciber activos críticos. El modelo ENCRYPT incluye las siguientes nueve categorías de riesgo a tener en cuenta: (1) Recursos humanos; (2) Propiedad intelectual; (3) Seguridad de los Sistemas de Control Industrial (SCI); (4) Productos; (5) Riesgos legales de ciberseguridad; (6) Ataques a la cadena de suministro; (7) Tecnología, TICs y seguridad operativa; (8) Clientes; y (9) Ciberseguridad física. Tenga en cuenta que, dependiendo de las actividades de su organización, su modelo de negocio y su sector de operaciones, es posible que no se apliquen todas las categorías o que decida que no tiene activos cibernéticos críticos relacionados con estas categorías. Para evaluar esto, revise el Anexo 1 y elija las categorías aplicables a su organización y las amenazas que considere relevantes en función de los ciber activos cruciales identificados en su empresa.

PASO 3: Priorizar los riesgos

En este paso crucial, debe comprobar la lista de amenazas potenciales que considera aplicables a su empresa y, de acuerdo con una serie de criterios, decidir qué riesgos son altamente probables y con un impacto adverso potencialmente más grave. Por ello, el consorcio de ENCRYPT 4.0 ha elaborado una metodología de evaluación de riesgos que tiene en cuenta los siguientes componentes:

- Costes potenciales asociados a las consecuencias del riesgo;
- Departamento(s) de la organización que podría(n) verse afectado(s);
- Impacto potencial;
- Probabilidad - a la hora de evaluar la probabilidad, hay que tener en cuenta las tendencias del sector y los fallos de seguridad anteriores;
- Y el nivel de riesgo.

Puede utilizar directamente el CRAM de Encrypt 4.0, la herramienta desarrollada específicamente para priorizar fácilmente los riesgos potenciales.

PASO 4: Auditoría de las medidas de seguridad vigentes

Una vez identificadas las categorías de riesgo y las amenazas aplicables a su organización, el siguiente paso es evaluar si sus activos e infraestructuras cibernéticas críticas son vulnerables a alguna de estas amenazas. Para ello, debe evaluar los protocolos/procedimientos/medidas de seguridad establecidos con respecto a la identificación de las posibles brechas de seguridad que deben abordarse. En la tabla 2, encontrará algunas preguntas orientativas y consejos sobre cómo evaluar si las medidas de seguridad establecidas son adecuadas, aunque también depende de las amenazas que considere aplicables en cada categoría.

Tabla 2. Consejos para identificar las medidas de seguridad existentes

No.	Categoría	Consejos para identificar las medidas de seguridad existentes
1	**Recursos Humanos**	Compruebe la distribución de las funciones y responsabilidades relacionadas con la gestión y la seguridad de los datos, la ciberseguridad, el control del sistema, etc. Hable con los/as empleados/as responsables designados/as dentro de estos ámbitos: pregúnteles cómo reaccionarían en determinadas situaciones, qué protocolos de seguridad aplicarían, y así podrá evaluar si el personal es consciente y está preparado en caso de que se produzcan determinados riesgos de ciberseguridad; si necesitan formación o no. Analiza los accidentes y las brechas de seguridad debidas a errores de empleados y cómo se han gestionado. Piensa si se puede hacer algo más para minimizar la aparición de esta amenaza en el futuro.
2	**Propiedad Intelectual**	Comprobar la distribución de funciones y responsabilidades relacionadas con la gestión de la propiedad intelectual y los secretos comerciales, etc. Entrevistar a los empleados responsables, revisar la documentación pertinente relativa a la protección de activos como patentes, marcas comerciales y derechos de autor. ¿Cómo se guarda y gestiona esta documentación, quién tiene acceso a ella? ¿Hubo incidentes en el pasado relacionados con violaciones de la información, falta de información en este ámbito? ¿Cómo se han gestionado? ¿Se ha actualizado el protocolo de seguridad?
3	**Seguridad de los Sistemas de Control Industrial (SCI)**	¿Quién tiene acceso remoto y/o físico al SCI? ¿Cómo se administra el acceso remoto a los SCI? ¿Existen controles de seguridad como autenticación fuerte, control de acceso y encriptación para proteger contra el acceso no autorizado y la explotación de estos sistemas? ¿Cuáles son las medidas de control de acceso físico? ¿Utiliza cortafuegos que tengan en cuenta el protocolo SCI para aplicar controles de acceso al tráfico de la red SCI? ¿Dispone de un sistema de prevención de intrusiones?
4	**Productos**	Dependiendo del proceso de producción de los productos, hay que identificar en qué procesos se maneja la información sensible y de qué manera está siendo gestionada y administrada. ¿Existen algún secreto comercial relacionado con la producción de los productos, etc.? ¿Cómo garantiza la empresa la gestión segura de esta información? ¿Cuál es el protocolo - funciones y responsabilidades, procedimientos, etc.?

		¿Existe algún tipo de control de acceso físico y remoto a los ordenadores y redes, sistemas de producción, etc.? ¿Cómo se aseguran y controlan éstos?
5	**Riesgos legales de ciberseguridad**	¿Hay algún control en el acceso físico y remoto a los ordenadores y redes de la empresa? ¿Cómo se aseguran y controlan? ¿Cómo se gestionan y administran los datos legales? ¿Está asegurado el servidor? ¿Quién tiene acceso a esta información? ¿Hubo algún fallo o brecha de seguridad en el pasado? ¿Cómo se gestionaron? ¿Hay alguna forma de mejorar los protocolos de seguridad en función de las tendencias/eventos/desarrollos tecnológicos recientes?
6	**Ataques a la cadena de suministro**	¿Quién tiene acceso a los sistemas de gestión de suministros? ¿Existe una gestión de accesos privilegiados? ¿Quién tiene acceso a los datos sensibles? ¿Cómo se asegura este acceso? ¿Tiene implementados "*HoneyTokens*" ("*honeypots*" que no son sistemas informáticos)? ¿Cuál es el nivel de control del acceso de los proveedores de servicios? ¿Cuántos proveedores tienen acceso al software? ¿Se supervisa la red de los proveedores para detectar vulnerabilidades?
7	**Tecnología, TIC y seguridad operativa**	¿Tiene políticas estrictas de seguridad móvil y protección de datos? ¿Están actualizadas todas las aplicaciones de software y los sistemas operativos? ¿Existen controles de acceso para los activos críticos de ciberseguridad? ¿Supervisa la actividad de las cuentas de usuario, el registro y el acceso a su red? Compruebe si los *firewalls* están bien configurados y asegúrese de que dispone de cifrado de extremo a extremo para los datos sensibles. ¿Tiene mecanismos configurados para reconocer y evitar ataques como el *"phishing"* y el "*pharming"*?
8	**Clientes**	¿Quién tiene acceso a los datos importantes de los clientes? ¿Tiene una copia de seguridad o back-up de los datos e información importante de la empresa?
9	**Ciberseguridad física**	¿Cómo se gestiona el mantenimiento de los equipos y activos críticos de ciberseguridad? ¿Quién tiene acceso físico a los equipos y activos críticos de ciberseguridad? ¿Cómo se protege el acceso?

PASO 5: Establecer/actualizar los protocolos de seguridad en función de la auditoría

Una vez completado el PASO 4, necesita tener identificadas en un listado, las amenazas aplicables a su organización, para ser consciente de lo que ya está haciendo y de lo que tal vez, le falta por hacer. También necesita identificar los controles de seguridad de la información adecuados para neutralizar o erradicar el riesgo de amenaza (LeCount 2019).

Los **controles de seguridad de la información** son medidas adoptadas para reducir los riesgos de seguridad de la información, como las violaciones de los sistemas de información, el robo de datos y los cambios no autorizados en la información o los sistemas digitales (Garcia 2019). El objetivo principal de los controles de seguridad es proteger la disponibilidad, confidencialidad e integridad de los datos y las redes de una empresa. Como ya se ha mencionado, los controles de seguridad suelen aplicarse después de una evaluación de los riesgos de la información o de la ciberseguridad, y representan un resultado esperado de las evaluaciones y auditorías de ciberseguridad en lo que respecta a abordar las brechas de seguridad identificadas, reales o potenciales.

En la tabla 3, según el modelo de evaluación de riesgos de ciberseguridad de ENCRYPT 4.0 basado en entrevistas con expertos/as en ciberseguridad de 6 países de la UE, hemos identificado dos tipos de controles: preventivos y correctivos, en cada una de las nueve categorías de riesgo. Sobre la base de la auditoría realizada en el "PASO 4", usted ya conoce los procedimientos de ciberseguridad existentes en su organización. En la tabla 3, puede encontrar algunas sugerencias de controles preventivos y correctivos para cada una de las categorías, que podría echar en falta en su organización.

Tabla 3. Controles preventivos y correctivos de ciberseguridad

Categoría de Riesgo	Medidas preventivas	Medidas correctivas
Recursos Humanos	Establecer un programa de formación y sensibilización Identificar claramente la gestión de las identidades, la autenticación y el control de los accesos La empresa deberá tener una política que incluya: ● Una lista de software autorizado. ● Un repositorio de software autorizado y registro de licencias. ● Sanciones disciplinarias asociadas al incumplimiento de esta normativa. Renovar las contraseñas trimestralmente ("*política de contraseña segura*") Desarrollar soluciones de recuperación de desastres y planes de continuidad de la actividad	Control de los permisos de los usuarios Implementar el **Sistema de Detección de Intrusos (SDI)** para detectar el acceso no autorizado a un PC o a una red Cambiar todas las contraseñas después de una posible violación de datos Bloquear las cuentas sospechosas de acceso no autorizado Establecer la verificación en dos factores cuando sea posible, lo que proporcionará una doble autentificación.

Categoría de Riesgo	Medidas preventivas	Medidas correctivas
Propiedad Intelectual	Políticas y competencias adecuadas para la gestión de la propiedad intelectual Todos los activos aplicables deben estar protegidos por patentes, derechos de autor y marcas registradas. Los activos pertinentes deben ser supervisados y protegidos por seguros. Desarrollar medidas, políticas y responsabilidades en la gestión de la reputación	Evaluación periódica y actualización de las políticas y responsabilidades Si se carece de una patente registrada, se debe obtener una patente provisional, una marca comercial y derechos de autor Evaluación periódica y actualización de las políticas y responsabilidades
Seguridad de los Sistemas de Control Industrial (SCI)	Desarrollo de medidas, políticas, responsabilidades y respuesta rápida en caso de incidencia	Evaluación periódica y actualización de las políticas y responsabilidades
Productos	Evaluación de los procesos del flujo de trabajo Estandarización y evolución Control del acceso físico a los ordenadores y a los componentes de la red	Implementar un enfoque por capas para cada riesgo o, al menos, para aquellos que tienen un alto potencial en el caso específico, con el fin de tener al menos algunas capas de protección, sin importar si se trata de tecnologías, empleados, procesos, clientes, etc.
Riesgos legales de ciberseguridad	Conserve sólo lo que necesita. Haga un inventario del tipo y la cantidad de información en sus archivos y ordenadores Proteja los datos Destruya antes de eliminarlos Actualice los procedimientos Educar/formar a los empleados Controle el uso de los ordenadores Asegurar todos los ordenadores	Identificar y notificar a las partes afectadas Buscar asesoramiento jurídico
Ataques a la cadena de suministro	Implementar Honeytokens Gestión segura de los accesos privilegiados Identificar todos los hilos potenciales de la información privilegiada Identificar y proteger los recursos vulnerables	Comprobar las licencias en toda la cadena de suministro de las PYMEs Busque los datos de contacto de su mantenimiento preventivo y correctivo de la maquinaria de las PYME en toda la cadena de suministro a nivel regional/local

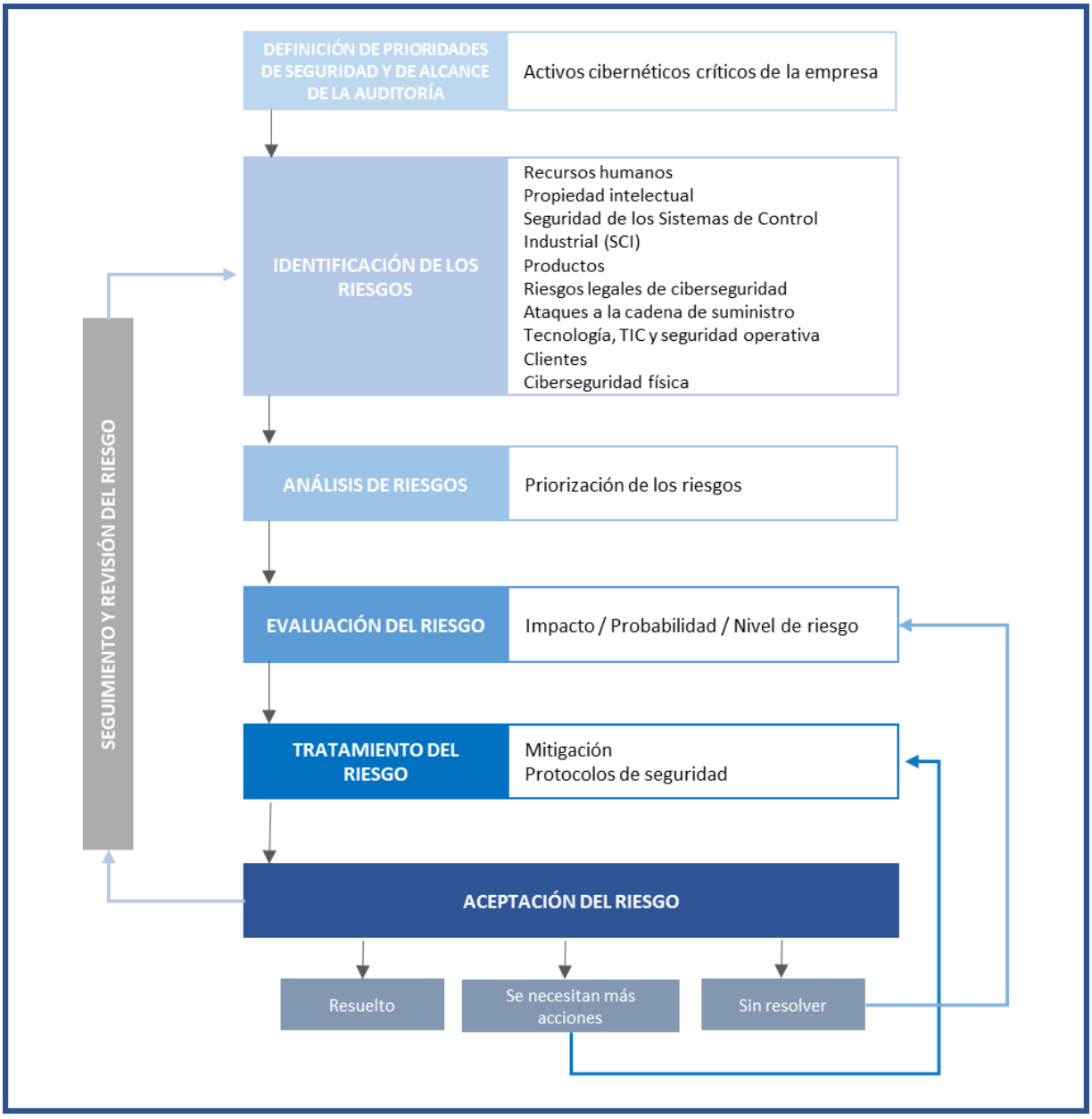
Categoría de Riesgo	Medidas preventivas	Medidas correctivas
	Minimizar el acceso a los datos sensibles Envíe regularmente evaluaciones de riesgo de terceros Supervisar la red de proveedores en busca de vulnerabilidades Identificar todas las fugas de datos de los proveedores	
Tecnología, TIC y seguridad operativa	Descargue e instale actualizaciones de software para sus sistemas operativos y aplicaciones a medida que estén disponibles Actualice los sistemas operativos y el *firmware* Instale un cortafuegos entre Internet y la LAN Identifique los activos críticos Ser conscientes de la seguridad, Haga copias de seguridad y de recuperación, Gestione las vulnerabilidades y parches, Aplicar controles de acceso, Utilizar el filtrado de contenidos y listas blancas, Configurar correctamente los puntos finales, Establecer procesos de respuesta a incidentes, Utilizar soluciones y sistemas de inteligencia de amenazas. Los cortafuegos correctamente configurados, las políticas estrictas de seguridad móvil, el cifrado de extremo a extremo, el registro de auditoría y la autorización de los dispositivos para acceder a la red son algunas de las prácticas que reducen las amenazas derivadas del uso de dispositivos móviles en una red corporativa.	Comprobar todos los plazos límite del *OS* y del *firmware*, que tiene en sus PYMES, y supervisar que todo esté actualizado Instalar *firewall* entre Internet y la LAN. Eliminar el software ilegal o no permitido en el repositorio de software Instalar el estándar a todos los equipos informáticos Configurar VPN si es necesario conectarse desde el exterior. Identificación y corrección del problema. Auditar y actualizar las políticas y reglas de seguridad.

Categoría de Riesgo	Medidas preventivas	Medidas correctivas
	Evaluar el software con respecto a los principios de ciberseguridad. Asegúrese de que los sistemas operativos y todas las aplicaciones de software estén actualizados, Asegurarse de que los datos sensibles están encriptados, Utilizar software de protección de datos, Supervisar regularmente la actividad de las cuentas de usuario, Gestionar la configuración de privacidad de las aplicaciones móviles, Aplicar controles estrictos de los dispositivos para los medios extraíbles, Establecer mecanismos para reconocer y evitar ataques como el *phishing* y el *pharming*. Funcionamiento basado en políticas y reglas de seguridad	
Clientes	Hacer copias de seguridad de los datos e información importantes de la empresa	Establecer la verificación en dos factores cuando sea posible, lo que proporcionará una doble autentificación. Bloquear las cuentas sospechosas de tener acceso no autorizado Bloquear las direcciones IP de los presuntos actores de la amenaza en función de las actividades detectadas

Categoría de Riesgo	Medidas preventivas	Medidas correctivas
Ciberseguridad física	Poner en marcha un plan de seguridad en caso de incendios, inundaciones, robos, pérdidas, etc. Apagar las herramientas y/o equipos que no se estén utilizando Disponer de un sistema de alimentación ininterrumpida de reserva o conseguir una segunda fuente de energía de emergencia Comprobar regularmente todos los dispositivos Hacer copias de seguridad Tener preferentemente todos los datos alojados en la nube	En las instalaciones, estar al día en materia de seguridad del edificio y disponer de medidas contra incendios. Tener una batería de reserva para el ordenador o conseguir una segunda fuente de energía de emergencia. Hacer una copia de seguridad Hacer un *safety switch* o interruptor de seguridad Sustituir o arreglar los dispositivos dañados o averiados

VISIÓN GRÁFICA DEL PROCESO CON EL CRAM

Aquí se representa la visión gráfica del proceso de auditoría usando CRAM de Encrypt 4.0, como una herramienta que esboza las medidas correspondientes que debe tomar la persona responsable en las PYMES manufactureras para realizar un análisis exhaustivo de sus procesos mediante la identificación de los riesgos cibernéticos y el apoyo en el diseño y el establecimiento de controles eficaces en el lugar de acuerdo con la naturaleza progresiva del ciberataque.



El CRAM de Encrypt 4.0 sigue un proceso sistemático y continuo. Es un proceso cíclico que una vez ha identificado, analizado, valorado, evaluado, tratado y aceptado los riesgos, se debe llevar a cabo un seguimiento y una revisión de los mismos. En caso de que el problema persista, se tendrá que aplicar más acciones complementarias hasta resolverlo, y para ello, se tendrá que volver al paso anterior del tratamiento de riesgos. Y si el problema sigue sin resolverse, tendrá que volver a evaluar el riesgo.

6. PROYECTO Y CONSORCIO

ENCRYPT 4.0

Iniciativa conjunta de desarrollo de la mano de obra cibernética para permitir que la industria europea supere la escasez de profesionales de la ciberseguridad

El proyecto ENCRYPT4.0 (2020-1-RO01-KA202-079983) tiene como objetivo permitir a la dirección de las PYME manufactureras adoptar un enfoque proactivo hacia la ciberseguridad, apoyándolas en el proceso de análisis, identificación y tratamiento de los riesgos y amenazas cibernéticas aplicables a su organización. Promoviendo el aprendizaje interactivo basado en proyectos en lo que respecta a potenciar las habilidades y competencias en materia de ciberseguridad de los empleados de las PYME o de los profesionales de la ciberseguridad.

"George Emil Palade" University of Medicine, Pharmacy, Sciences and Technology of Târgu Mureș - Romania

Project coordinator

European Center for Quality Ltd., Consulting company - Bulgary

Instituto de Soldadura e Qualidade, Technological institution - Portugal

Avantalia, technology-based SME - Spain

FH Joanneum, University of Applied Sciencies - Austria

PCX Management, Computers & Information Systems Ltd. - Cyprus

BIBLIOGRAFÍA

Aldorisio, J. *Best Practices for Cybersecurity Auditing [a Step-by-Step Checklist]. Security Scorecard. .* Retrieved from https://securityscorecard.com/blog/best-practices-for-a-cybersecurity-audit, 2020.

Commission, European. "Data protection in the EU (EUR-LEX)." n.d. https://ec.europa.eu/info/law/law-topic/data-protection/data-protection-eu_en (accessed August 2020).

Cybersecurity Ventures. "Cybersecurity Ventures Official Annual Cybercrime Report." 2019.

CyLumena, a CitiusTech Company. *Overcoming Cybersecurity Assessment & Audit Confusion.* n.d. https://www.cylumena.com/insights/security-assessment-audit-types/ (accessed August 2020).

EU Agency for Cybersecurity. "Industry 4.0 Cybersecurity: Challenges & recommendations." 2019.

European Union Agency for Cybersecurity. *Information security and privacy standards for SMEs - Recommendations to improve the adoption of information security and privacy standards in small and medium enterprises.* ENISA, 2015.

Forum, World Economic. "The Global Risks Report." Insight Report, 2020; 15th Edition.

Forum_, World Economic. *Cyber-Risk Assessments: the vaccine for companies in the Fourth Industrial Revolution.* January 2020. https://www.weforum.org/agenda/2020/01/cyber-risk-assessments/ (accessed 2021).

Garcia, Thea. *Reciprocity.* 18 November 2019. https://reciprocity.com/resources/what-are-information-security-controls/.

Interpol, General Secretariat. *Global Landscape on COVID-19 Cyberthreat.* 2020.

Juncker, Commission Ex President Jean-Claude, interview by European Commission. *"President Jean-Claude Juncker's State of the Union Address 2017*" (13 September 2017).

LeCount, Richard. *Hackernoon.* 22 November 2019. https://hackernoon.com/how-to-conduct-an-in-depth-cyber-security-audit-for-your-business-wgn33zym.

Margot Hutchins, Raunak Bhinge, Maxwell Micali, and John Sutherland, David Dornfeld Stefanie Robinson. "Framework for Identifying Cybersecurity Risks in." *U.S. Department of Energy*, 2015: 17.

Morehouse, Tony Flick and Justin. "Public and Private Companies." In *Securing the Smart Grid; Next Generation Power Grid Security*, by Tony Flick and Justin Morehouse, 85-108. 2011.

Morgan, Steve. *Cybersecurity Ventures Official Annual Cybercrime Report.* 26 October 2020. https://cybersecurityventures.com/annual-cybercrime-report-2020/.

National Institute for Standards and Technology. *Guide for Conducting Risk Assessments.* Gaithersburg: Special Publication 800-30, 2012, 95.

ThomasLangill, Eric D. Knapp and Joel. "Chapter 2 - About Industrial Networks." In *Industrial Network Security; Securing Critical Infrastructure Networks for Smart Grid, SCADA, and Other Industrial Control Systems*, 9-40. Syngress, ISBN 9780124201149, https://doi.org/10.1016/B978-0-12-420114-9.00002-2., 2015.

Ventures, Cybersecurity. "Global ransomware damage costs predicted to reach $20 billion (USD) by 2021." *Cybercrime Magazine*, 2019.

Verizon. *Manufacturing.* 2020. https://enterprise.verizon.com/resources/reports/dbir/2020/data-breach-statistics-by-industry/manufacturing-data-breaches/.

Verizon. “Verizon Data Breach Investigations Report.” 2017.

World Economic Forum . “Innovation-Driven Ciber-risk to Costumer Data in Financial Services.” Cologny/Geneva, 2017.

World Economic Forum. “The Global Risks Report.” 2020.

—. *World Economic Forum. Global Risks Report 2020.* 2020. https://reports.weforum.org/global-risks-report-2020/wild-wide-web/.

Yew, Tin Zaw and Richard. *Verizon media.* 26 July 2017. https://www.verizondigitalmedia.com/blog/2017-verizon-data-breach-investigations-report/.

ANNEX A - RECOPILACIÓN DE LAS NORMAS EXISTENTES PARA LOS RIESGOS DE CIBERSEGURIDAD

	NORMAS DE PROTECCIÓN DE DATOS Y CIBERSEGURIDAD
Seguridad de la información (Intersectorial)	ISO/IEC 27001:2018 Information security management systems – Requirements
	ISO/IEC 27002:2018 Code of practice for information security controls
	ISO/IEC 27003:2017 Information security management systems guidance
	ISO/IEC 27004:2016 Information technology — Security techniques — Information security management — Monitoring, measurement, analysis and evaluation
	International Organisation for Standardisation and International Electrotechnical Commission
	ISO/IEC 27014:2013 Governance of information security
	ISO/IEC TR 27016:2014 Information security management - Organisational economics
	ISO/IEC 27032:2012 Guidelines for information security
	ISO/IEC 27033-1:2015 Network security - Part 1: Overview and concepts
	ISO/IEC 27033-2:2012 Network security - Part 2: Guidelines for the design and implementation of network security
	ISO/IEC 27033-3:2010 Network security - Part 3: Reference networking scenarios - Threats, design techniques and control issues
	ISO/IEC 27033-4:2014 Network security - Part 4: Securing communications between networks using security gateways
	ISO/IEC 27033-5:2013 Network security - Part 5: Securing communications across networks using Virtual Private Networks (VPNs)
	ISO/IEC 27033-6:2016 Network security - Part 6: Securing wireless IP network access
	ISO/IEC 27034-1:2011 Application security - Part 1: Overview and concepts
	ISO/IEC 27039:2015 Selection, deployment and operations of intrusion detection systems (IDPS)
	ISO/IEC 27040:2015 Storage security
	CSA Cloud Controls Matrix
	BSI PAS 555:2013 Cybersecurity risk. Governance and management. Specification
	PCI Data Security Standard
	ISF The Standard of Good Practice for Information Security
	UK Gov. Security policy framework
	UK Gov. Cyber essentials scheme

	ETSI GS ISI 001 Part 1: A full set of operational indicators for organisations to use to benchmark their security posture
	ETSI TR 103 305 Critical Security Controls for Effective Cyber Defence
	BSI 100-1 Information Security Management Systems (ISMS)
	BSI 100-2: IT- Grundschutz Methodology
	BSI 200-1 Information Security Management Systems (ISMS)
	BSI 200-2: IT- Grundschutz Methodology
	ISO/IEC 15408-1:2009 Evaluation criteria for IT security - Part 1: Introduction and general model
	ISO/IEC 15408-2:2008 Evaluation criteria for IT security - Part 2: Security functional components
	ISO/IEC 15408-3:2008 Evaluation criteria for IT security - Part 3: Security assurance components
	ISO/IEC 19790:2012 Security requirements for cryptographic modules
	ISO/IEC 27006:2015 Requirements for bodies providing audit and certification of information security management systems
	ISO/IEC 27007:2017 Guidelines for information security management systems auditing
	ISO/IEC 27014:2020 Governance of information security
	ISO/IEC 27017:2015: Code of practice for information security controls based on ISO/IEC 27002 for cloud services
	ISO/IEC 29147:2018: Vulnerability disclosure
	ISO/IEC 30111:2019: Vulnerability handling processes
	OENORM A 7700-3:201910 Web Applications - Part 3: Security requirements
	ISO/IEC 27701:2019 Security techniques- Extension to ISO/IEC 27001 and ISO/IEC 27002 for privacy information management - Requirements and guidelines
	ISO/IEC TS 27100:2020 Information technology -Cybersecurity- Overview and concepts

	NORMAS DE PROTECCIÓN DE DATOS Y CIBERSEGURIDAD
Gestión de riesgos	ISO/TR 31004:2013 Risk management - Guidance for the implementation of ISO 31000
	ISO/IEC 27005:2016 Information security risk management
	ISO/IEC 31000 Risk management - Risk assessment techniques
	IEC 31010:2009 Risk management - Risk assessment techniques
	BSI BIP 0076 Information security risk management. Handbook for ISO/IEC 27001
	BSI 100-3: Risk Analysis based on IT-Grundschutz

	BSI 200-3: Risk Analysis based on IT-Grundschutz
	ISO/IEC 27005:2018 Information security risk management
	ISO/IEC 27102:2019 Information security management — Guidelines for cyber-insurance

	NORMAS DE PROTECCIÓN DE DATOS Y CIBERSEGURIDAD
Gestión de la continuidad del negocio	ISO 22301:2012 Business continuity management systems – Requirements
	ISO 22313:2012 Business continuity management systems – Guidance
	ISO/IEC 27031:2011 Guidelines for information and communication technology readiness for business continuity
	100-4: Business Continuity Management
	OENORM A 7700-4:201910 Web Applications - Part 4: Requirements for secure operations

	NORMAS DE PROTECCIÓN DE DATOS Y CIBERSEGURIDAD
Protección de datos y Privacidad	ISO/IEC 27018:2014 Code of practice for protection of personally identifiable information (PII) in public clouds acting as PII processors
	ISO/IEC 29100:2011 Privacy framework
	ISO/IEC 29101:2013 Privacy architecture framework
	BSI BS 10012:2009 Data protection. Specification for a personal information management system
	CEN CWA 16113:2010 Personal Data Protection Good Practices
	OEVE/OENORM 17529:2020: Data protection and privacy by design and by default
	OENORM A 7700-2:201912 Web Applications - Part 2: Data protection requirements
	ISO/IEC 27018:2019: Code of practice for protection of personally identifiable information (PII) in public clouds acting as PII processors
	ISO/IEC 29134:2017: Guidelines for privacy impact assessment
	ÖNORM EN 419231:2019 11 01: Protection profile for trustworthy systems supporting time stamping
	ÖNORM EN 419241-1:2019 03 15: Trustworthy Systems Supporting Server Signing - Part 1: General System Security Requirements
	ÖNORM EN 419241-2:2019 06 01: Trustworthy Systems Supporting Server Signing - Part 2: Protection profile for QSCD for Server Signing

	NORMAS DE PROTECCIÓN DE DATOS Y CIBERSEGURIDAD
	ISO/PAS 22399:2007 Societal security - Guideline for incident preparedness and operational continuity management

Gestión de incidencias	ISO/IEC 27036-2:2014 Information security for supplier relationships - Part 2: Requirements
	ISO/IEC 27036-3:2013 Information security for supplier relationships - Part 3: Guidelines for information and communication technology supply chain security
	ISO/IEC 27035-1:2016 Information security incident management — Part 1: Principles of incident management
	ISO/IEC 27035-1:2016 Information security incident management — Part 2: Guidelines to plan and prepare for incident response

	NORMAS DE PROTECCIÓN DE DATOS Y CIBERSEGURIDAD
Gestión de Terceros	ISO/IEC 27036-1:2014 Information security for supplier relationships - Part 1: Overview and concepts
	ISO/IEC 27035:2011 Information security incident management
	ISO/IEC 27037:2012 Guidelines for identification, collection, acquisition and preservation of digital evidence

	NORMAS DE PROTECCIÓN DE DATOS Y CIBERSEGURIDAD
Seguridad Industrial	OVE EN IEC 62443-4-1:2018 11 01: Security for industrial automation and control systems - Part 4-1: Secure product development lifecycle requirements
	OVE EN IEC 62443-4-2:2020 01 01: Security for industrial automation and control systems - Part 4-2: Technical security requirements for IACS components
	OVE IEC TS 62351-100-1:2020 06 01