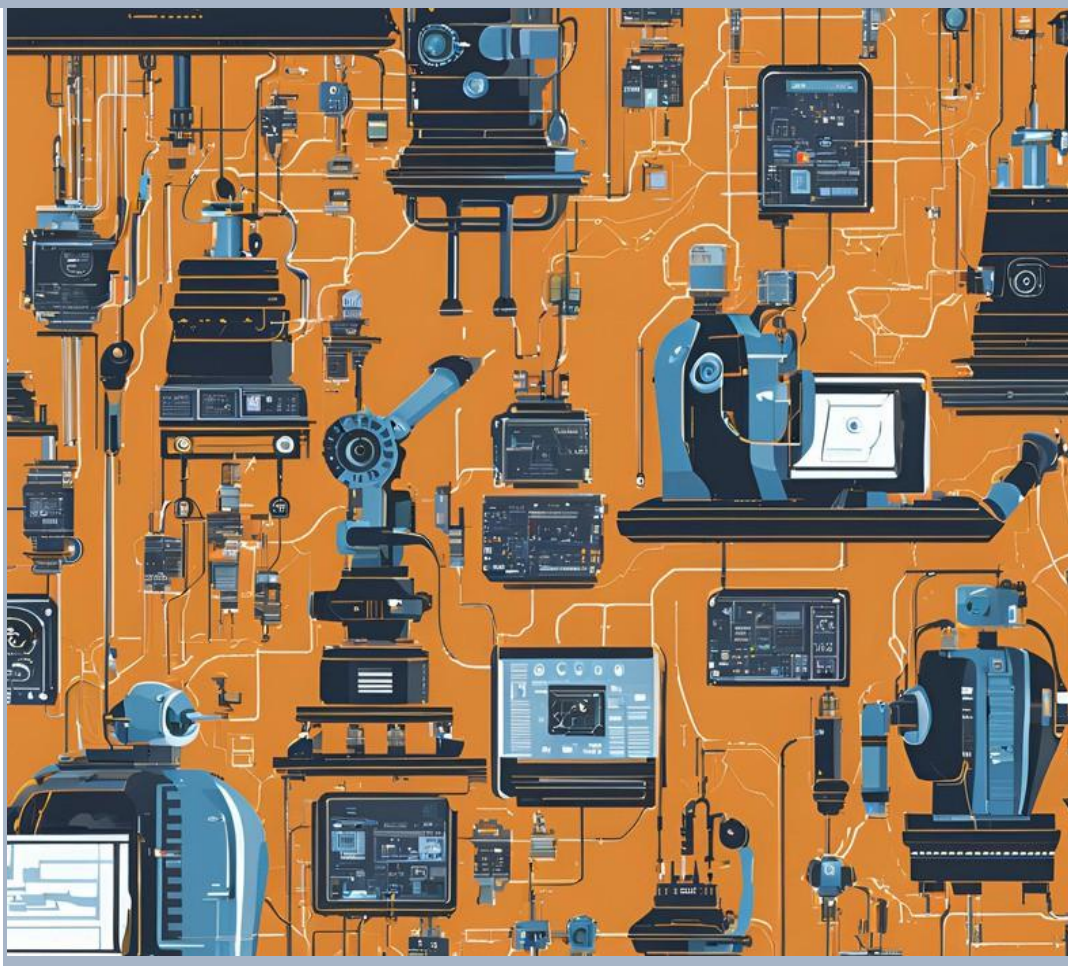
Co-funded by the European Union

CIBERSEGURIDAD EN ENTORNOS OT

DEFICIENCIAS EN LAS COMPETENCIAS Y NECESIDADES DE FORMACIÓN

Referencia del proyecto: 2023-1-NL01-KA220-VET-000153812

Elaborado por:



www.cyber-in.eu

ESTE PROYECTO HA SIDO FINANCIADO CON EL APOYO DE LA COMISIÓN EUROPEA. ESTA PUBLICACIÓN [COMUNICACIÓN] REFLEJA ÚNICAMENTE LAS OPINIONES DEL AUTOR, Y LA COMISIÓN NO SE HACE RESPONSABLE DEL USO QUE PUEDA HACERSE DE LA INFORMACIÓN CONTENIDA EN ELLA.

Índice

Introducción

La ciberseguridad es uno de los principales retos a los que se enfrentan las empresas en el contexto del Internet de las cosas industrial (IoT), en el que una serie de dispositivos inteligentes asociados a máquinas, ordenadores y personas están conectados en red y se comunican entre sí.

En este escenario industrial conectado, el personal debe ser consciente de las cuestiones relacionadas con la ciberseguridad para prevenir o minimizar la ocurrencia de incidentes de ciberseguridad y violaciones de datos corporativos, y así hacer que las empresas sean resilientes ante los ciberataques.

Aunque existe un interés creciente en la literatura por los diferentes elementos clave que caracterizan la gestión de la ciberseguridad en contextos industriales del IoT, se ha prestado poca atención a los diversos aspectos de la concienciación sobre la ciberseguridad en esos mismos contextos industriales.

Además, la ciberseguridad no es un tema nuevo en nuestras escuelas, ni en la batería de proyectos Erasmus+ implementados hasta la fecha. En la plataforma de difusión de Erasmus+ hay 100 proyectos KA2 relacionados con el tema. Sin embargo, si tenemos en cuenta las aplicaciones de la ciberseguridad a la industria (y en particular al paradigma de la Industria 4.0), los resultados se reducen significativamente.

Mientras que las empresas industriales avanzan hacia la fabricación inteligente y la digitalización de la maquinaria, los datos, los procesos y los puestos de trabajo mediante la aplicación de tecnologías facilitadoras como el IoT, la computación en la nube o el big data, con el objetivo de ganar en eficiencia en su respuesta a unos mercados en constante cambio, las vulnerabilidades en materia de ciberseguridad aumentan exponencialmente.

El objetivo final de este documento era determinar cuáles son las carencias de los profesionales de IT y OT que trabajan en industrias con un alto nivel de automatización en materia de ciberseguridad, de modo que las escuelas de formación profesional puedan subsanarlas a la hora de impartir formación a los alumnos de los programas de IT y OT.

Para ello, llevamos a cabo entrevistas y grupos de discusión en los países socios (Países Bajos, España, Dinamarca, Estonia e Italia) con el fin de comprender en profundidad los retos reales de las plantas industriales interconectadas en materia de ciberseguridad y protección de datos.

El primer paso fue comprender los retos, puntos débiles y necesidades a los que se enfrenta la industria interconectada en materia de ciberseguridad, con el fin de definir y detallar mejor la descripción de un perfil de OT con las competencias de ciberseguridad que demandan las industrias interconectadas, así como la de un técnico de TI industrial con las competencias necesarias para tender un puente con el mundo de la OT.

A continuación, combinamos los comentarios recibidos de las empresas con un análisis de los planes de estudios actuales que ya impartimos en nuestras escuelas de formación profesional, identificando las carencias relacionadas con la ciberseguridad. El resultado fue una definición de las competencias en ciberseguridad para profesionales de IT y OT que puede servir de base para desarrollar materiales de formación destinados a subsanar esas carencias; materiales que pueden ser utilizados por profesores y formadores para el autoaprendizaje, así como integrarse en los planes de estudios actuales de nuestros programas de EFP o ser utilizados por las empresas para la formación interna de su propio personal de IT y OT.

En las siguientes secciones presentamos nuestras conclusiones y los resultados de nuestra investigación y análisis.

Necesidades de las empresas

Cada socio llevó a cabo focus groups y/o entrevistas con empresas en cada contexto local (Italia, Dinamarca, España, Países Bajos y Estonia).

La combinación de actores de IT y OT y formadores/profesores nos permitió recopilar información mediante preguntas específicas con el fin de comprender cuáles son los retos de ciberseguridad a los que se enfrentan las industrias interconectadas.

Número de empresas que proporcionaron comentarios

34 empresas

Número de sectores implicados

11 sectores

El objetivo de los grupos focales y las entrevistas era identificar las principales carencias detectadas desde el punto de vista técnico y de las competencias transversales, y extraer conclusiones sobre la necesidad de un nuevo perfil OT/IT con la mejora de las competencias y el reciclaje profesional de los trabajadores y estudiantes actuales:

- Comprender qué saben ya las empresas de OT de los sectores definidos sobre ciberseguridad (conceptos principales, contexto empresarial…)
- Definir el grado de concienciación sobre los riesgos (puntos débiles específicos del sector, factor humano, existencia de protocolos y normativas…)
- Explorar las normas conocidas sobre ciberseguridad (estándares y normativas aplicadas al sector específico)
- Explorar los incidentes a los que se enfrentan otras empresas (estudios de casos, simulaciones…).
- Comprender qué conocimientos tienen las empresas de ciberseguridad de IT y/o los profesionales de IT sobre los riesgos a los que se enfrentan las empresas de OT
- Detectar las carencias o necesidades en materia de conocimientos, habilidades y concienciación entre los estudiantes y los trabajadores de ambos campos.

Por motivos de privacidad, no revelamos los nombres de las empresas entrevistadas, pero sí indicamos los sectores a los que pertenecen, así como la función del entrevistado o participante en el grupo de discusión.

COUNTRY	PARTNER	COMPANY AREA	ROLE OF THE INTERVIEWED
DK	Roskilde Tekniske Skole	Production for aviation	Infrastructure Supervisor
DK	Roskilde Tekniske Skole	water supply	Team Leader
DK	Roskilde Tekniske Skole	production of medicin	SVP Education Proffessional
DK	Roskilde Tekniske Skole	water supply	
DK	Roskilde Tekniske Skole	water supply	Operations Manager
ITA	ECOLE SCARL	Cybersecurity and consultancy	Lead Reliability & Planning
ITA	ECOLE SCARL	Electrical engineering	Strategic Planner & Automation Specialist
ITA	ECOLE SCARL	Chemicals and energy company	APC & Cybersecurity Specialist
ITA	ECOLE SCARL	Pharmaceutical chemical	CYBER SECURITY MANAGER
ITA	ECOLE SCARL	ENGINEERING, PROCUREMENT & CONSTRUCTIO	ICT Budget & Reporting Analyst
ITA	ECOLE SCARL		Account Specialist, Senior Security Engineer
EST	BCS Koolitus	Telecommunication equipment production	Cybersecurity engeneer
EST	BCS Koolitus	IT security solutions	Head of Department, IT specialist (2 people)
EST	BCS Koolitus	IT security solutions	IT specialist
EST	BCS Koolitus	Telecommunication, production	Sysadmin
EST	BCS Koolitus	Governmental Institution	Helpdesk Operations Manager
EST	BCS Koolitus	Gambling software development	IT specialist
EST	BCS Koolitus	VET College	IT specialist, teacher of IT
EST	BCS Koolitus	Wood production	IT specialists (2 people)
EST	BCS Koolitus	Food production	IT specialist
EST	BCS Koolitus	VET	IT specialist, teacher of IT
EST	BCS Koolitus	VET	Teacher of Cybersecurity, cybersecurity expert
EST	BCS Koolitus	VET	Teacher of Cybersecurity, cybersecurity expert
ES	Maristak / HETEL	IT security solutions	CEO
ES	Maristak / HETEL	Cybersecurity association	Managing Director
ES	Maristak / HETEL	Transport - Automotive	IT Manager
ES	Maristak / HETEL	Energy - Solar	Cybersecurity manager
ES	Maristak / HETEL	Energy - Wind	Cybersecurity manager
ES	Maristak / HETEL	Energy - Chemical	IT manager
ES	Maristak / HETEL	Energy - Electric equipment	Cybersecurity manager
ES	Maristak / HETEL	Transport - Aviation	Cybersecurity manager
ES	Maristak / HETEL	Transport - Machine tool	HR manager
NL	Da Vinci College	Robotics (welding)	Device manager
NL	Da Vinci College	Industrial Analytics en Machine Learing	Junior consultant smart technologies
NL	Da Vinci College	IT solutions	CEO
NL	Da Vinci College	Fiber optics/network solution	Manager
NL	Da Vinci College	Security	Support specialist

Planteamos 10 preguntas a las empresas, clasificadas en 3 áreas temáticas:

- Área 1. Comprender qué saben ya las empresas de OT sobre ciberseguridad.
- Área 2. Comprender qué saben las empresas de ciberseguridad de IT sobre los riesgos a los que se enfrentan las empresas de OT
- Área 3. Detectar las carencias y necesidades en materia de conocimientos, habilidades y concienciación entre los estudiantes y los trabajadores de ambos ámbitos.

Los resultados obtenidos en los países del proyecto (Italia, Estonia, España, Dinamarca y Países Bajos) proporcionaron una visión general detallada de los retos y oportunidades en el panorama de la ciberseguridad. A continuación se presentan los resultados obtenidos, agrupados por áreas temáticas y preguntas formuladas durante los grupos focales y las entrevistas.

Área temática 1: Concienciación sobre la ciberseguridad y riesgos en las empresas de OT

Preguntas clave planteadas durante los grupos focales/entrevistas en esta temática:

1 ¿Cuáles son los beneficios o las ventajas competitivas de la ciberseguridad en su sector?

2 ¿Qué tipo de incidentes o amenazas de ciberseguridad ha experimentado y cómo los ha gestionado? ¿Qué lecciones ha aprendido de los incidentes de ciberseguridad que usted u otras empresas han experimentado?

3 ¿Qué nivel de formación y concienciación en materia de ciberseguridad tienen sus empleados y colaboradores? ¿Qué acciones de formación o información llevan a cabo al respecto?

Beneficios

Las empresas de los países participantes reconocen que la ciberseguridad ofrece numerosas ventajas, entre ellas el aumento de la confianza de los clientes, la protección de la información sensible y la garantía de la continuidad operativa. Sin embargo, existen diferencias significativas en las motivaciones específicas y los beneficios percibidos entre los distintos sectores y países.

Análisis específico por países

Italia: Las empresas italianas, especialmente en el sector farmacéutico, han experimentado un aumento significativo de la concienciación sobre la ciberseguridad en los últimos años. Muchas grandes empresas han implementado funciones de ciberseguridad centralizadas y programas de formación obligatorios para todos los empleados, incluidos los proveedores. Este enfoque ha mejorado la protección de la información sensible y ha creado un entorno de trabajo más seguro y regulado, lo que ha potenciado la competitividad de estas empresas.

España: En España, la ciberseguridad se ha convertido en un componente esencial de las estrategias empresariales, especialmente en sectores regulados como el energético y la fabricación operativa (OT). El cumplimiento de normativas, como la Directiva NIS2, se considera una ventaja competitiva que refuerza la posición de las empresas en el mercado. La ciberseguridad también refuerza la confianza de los clientes y reduce los riesgos financieros asociados a las filtraciones de datos y los ciberataques.

Estonia: Las empresas estonias reconocen que un sistema de ciberseguridad bien configurado aumenta la confianza de los clientes y protege la información sensible. La reducción del riesgo de ataques y la mejora de la eficiencia operativa son ventajas significativas. Además, la confianza de los empleados en sus empleadores ha aumentado gracias a unas sólidas medidas de ciberseguridad.

Países Bajos: En los Países Bajos, la ciberseguridad se considera un elemento clave para mantener la competitividad, especialmente en los sectores marítimo y offshore. Las empresas que adoptan normas de seguridad avanzadas, como la NIS2, pueden garantizar un entorno seguro para sus clientes, mejorando su posición en el mercado y evitando interrupciones operativas.

Área temática 1: Concienciación sobre ciberseguridad y riesgos en las empresas de tecnología operativa

Gestión de incidentes y lecciones aprendidas

Las empresas han informado de experiencias comunes con ataques de phishing, ransomware y problemas relacionados con sistemas obsoletos. Las respuestas a los incidentes incluyen mejoras técnicas, políticas más estrictas y formación avanzada. La respuesta rápida a los incidentes, la formación de los empleados y la mejora continua de las políticas de seguridad son esenciales para mitigar los daños y prevenir futuros ataques.

Análisis específico por países

Italia: Las empresas italianas se han enfrentado a diversos incidentes, entre ellos ataques de phishing y problemas con cortafuegos obsoletos. En un caso, una gran empresa farmacéutica descubrió vulnerabilidades a través de sistemas de monitorización de la dark web. Las respuestas a los incidentes pusieron de relieve la importancia de un enfoque de confianza cero y la confirmación de cada transacción mediante autenticación. La gestión rápida de los incidentes y la documentación exhaustiva de las operaciones de los proveedores se identificaron como claves para mejorar la seguridad.

España: Los incidentes de ciberseguridad son una realidad en todos los sectores, incluidos el gobierno, las empresas privadas, la energía, la industria manufacturera, la banca y los seguros. En ciberseguridad de IT, los incidentes comunes incluyen vishing, spam, ransomware y phishing, mientras que en OT, los incidentes pueden afectar a los sistemas de control industrial y a los dispositivos conectados, con amenazas como ataques de denegación de servicio, manipulación de datos, malware específico de OT, acceso no autorizado a sistemas SCADA y fugas de información sensible. Las empresas han aprendido la importancia de la autenticación multifactorial, la formación continua y la preparación para responder a los ataques. La adopción de medidas preventivas y la mejora de las políticas de seguridad fueron cruciales para una gestión eficaz de los incidentes.

Estonia: Las empresas estonias destacaron la creciente sofisticación de los ataques de phishing y la importancia de la formación de los usuarios para prevenir incidentes. Los ataques a la cadena de suministro y el ransomware han sido especialmente problemáticos. Las respuestas eficaces a los incidentes incluyeron mejoras técnicas, políticas más estrictas y un enfoque particular en la formación de los empleados.

Países Bajos: Las empresas de los Países Bajos se han enfrentado a ataques DDoS y a problemas relacionados con software obsoleto. La formación continua y las actualizaciones de los sistemas se identificaron como factores cruciales para prevenir incidentes. La preparación y la formación continua se consideraron esenciales para mantener un alto nivel de seguridad y responder de manera eficaz a los ataques.

Dinamarca: En Dinamarca, los ataques simulados y los apagones parciales son prácticas habituales para preparar a las empresas ante situaciones reales. La gestión de riesgos y la preparación para los peores escenarios se consideran fundamentales para mitigar los daños y garantizar la continuidad operativa.

Área temática 1: Concienciación sobre ciberseguridad y riesgos en las empresas de OT

Formación y concienciación

Se implementan ampliamente la formación periódica, las simulaciones de phishing y los programas de concienciación. Sin embargo, existen diferencias significativas en el nivel de estructuración y el carácter obligatorio de los programas de formación entre los distintos países.

Análisis específico por país

Italia: La concienciación ha aumentado en los últimos 5-6 años. Las industrias no gestionan a diario la ciberseguridad y las redes, ya que estas son las dos últimas competencias que han desarrollado. La concienciación sobre la ciberseguridad ha aumentado debido a los ciclos de formación en línea obligatorios para todos los empleados y proveedores de sectores como el farmacéutico y el químico. Las empresas llevan a cabo simulaciones continuas y exigen a los empleados completar al menos seis horas de formación antes de acceder a los sistemas corporativos. Este enfoque garantiza que todos los empleados mantengan un alto nivel de concienciación y competencia en materia de ciberseguridad. Hoy en día, la ciberseguridad es algo que concierne a todos los empleados que forman parte del entorno corporativo.

España: Existe un déficit significativo en materia de formación integral, centrada en la sensibilización y la integración de las medidas de seguridad en la cultura diaria de la empresa. La formación suele limitarse a cursos en línea y cambios de contraseña, pero se están realizando esfuerzos para mejorar la concienciación y la preparación de los empleados a través de programas más estructurados.

Estonia: La concienciación sobre la ciberseguridad varía entre las empresas estonias. Algunas empresas implementan programas de formación obligatorios y pruebas periódicas de phishing, mientras que otras necesitan mejorar la comunicación de las políticas de seguridad. La formación continua y la colaboración entre los departamentos de TI y otros departamentos son cruciales para abordar eficazmente los retos de ciberseguridad.

Países Bajos: La formación anual específica y los programas de aprendizaje continuo son la norma. Las empresas hacen hincapié en la importancia de mantenerse al día sobre nuevas amenazas y tecnologías, dotando a los empleados de las habilidades necesarias para proteger eficazmente las infraestructuras corporativas.

Dinamarca: Es habitual la formación práctica basada en escenarios, con medidas de seguridad prácticas y actualizaciones periódicas proporcionadas por los CERT específicos de cada sector. Esta formación prepara eficazmente a los empleados para gestionar incidentes reales y mantener una postura de seguridad sólida.

Área temática 2: Prácticas de ciberseguridad en IT y OT

Características específicas de IT y OT e implicaciones para la ciberseguridad

Los sistemas OT suelen ser más antiguos, están menos conectados a Internet y tienen requisitos operativos únicos en comparación con los sistemas de TI, que se centran más en la seguridad de los datos. Ambos entornos requieren medidas de ciberseguridad a medida, prestando especial atención a las operaciones en tiempo real y a la compatibilidad con los sistemas heredados.

Análisis específico por país

Italia: Los sistemas OT requieren inversiones significativas en actualizaciones de seguridad y una estrecha colaboración con los departamentos de TI. La segregación de redes y la gestión segura de los proveedores son cruciales para proteger los sistemas contra el acceso no autorizado y las vulnerabilidades.

España: La falta de estandarización en los sistemas OT plantea un reto importante. La ciberseguridad debe adaptarse para satisfacer las necesidades específicas de cada sistema, prestando especial atención al cumplimiento normativo y a la gestión de riesgos.

Estonia: Las empresas estonias suelen utilizar sistemas heredados y redes aisladas, lo que requiere segmentación de la red y dispositivos redundantes para mantener la seguridad. La conectividad limitada a Internet reduce los vectores de ataque, pero también dificulta la actualización y la aplicación de parches a los sistemas.

Dinamarca: En Dinamarca, las redes aisladas y cifradas son habituales para proteger las infraestructuras críticas. Las medidas de seguridad prácticas, como el uso de túneles cifrados y la segmentación de la red, son esenciales para proteger los sistemas OT del acceso no autorizado.

Países Bajos: Se da prioridad a la velocidad y la fiabilidad de los sistemas. Las empresas deben actualizar continuamente las tecnologías y formar a los empleados para mantener un alto nivel de seguridad. La segmentación de la red y los controles de acceso estrictos son prácticas habituales.

Área temática 2: Prácticas de ciberseguridad en IT y OT

Limitaciones y soluciones

Las principales limitaciones incluyen restricciones financieras, equipos obsoletos y acceso limitado a Internet. Las soluciones habituales incluyen la segmentación de la red, controles de acceso estrictos y actualizaciones periódicas. La colaboración entre los departamentos de IT y OT es crucial para superar estos retos.

Análisis específico por país

Italia: Las limitaciones financieras y legales suponen retos importantes para las empresas italianas. La responsabilidad de los proveedores y el desarrollo conjunto de soluciones de seguridad son estrategias que se utilizan para mejorar la protección de los sistemas OT. La coordinación con el departamento de TI y una buena gestión interna son fundamentales para mantener un alto nivel de seguridad.

España: La obsolescencia de los sistemas OT y la falta de controles estrictos plantean retos comunes. El cumplimiento normativo y un enfoque basado en el riesgo son esenciales para proteger los entornos OT. Las empresas deben implementar soluciones a medida para gestionar eficazmente la seguridad de los sistemas heredados.

Estonia: Las empresas estonias se enfrentan a retos relacionados con equipos obsoletos y un acceso limitado a Internet. Se recomienda formación especializada y controles de acceso estrictos para mejorar la seguridad. La segmentación de la red y el aislamiento de los sistemas heredados son prácticas habituales para proteger los dispositivos de ataques externos.

Dinamarca: Los retos incluyen los sistemas antiguos y la comunicación segura entre dispositivos OT. La preparación y la seguridad multicapa se consideran fundamentales para mitigar los daños y garantizar la continuidad operativa. Las empresas deben implementar medidas de seguridad prácticas y actualizaciones periódicas para proteger las infraestructuras críticas.

Países Bajos: Las restricciones financieras y la falta de conocimientos específicos en OT representan retos importantes. La formación continua y el cumplimiento normativo son esenciales para mejorar la seguridad. Las empresas deben encontrar el equilibrio adecuado entre seguridad y operatividad para mantener un alto nivel de protección.

Área temática 2: Prácticas de ciberseguridad en IT y OT

Criterios, prioridades e impacto en la gestión de la ciberseguridad

Es crucial garantizar la continuidad, la calidad y la eficiencia mediante procedimientos estandarizados, copias de seguridad periódicas y supervisión en tiempo real. Equilibrar las necesidades operativas y los requisitos de seguridad es fundamental para una gestión eficaz de la ciberseguridad.

Análisis específico por países

Italia: La adopción de sistemas sin contraseña y la conectividad segura de los empleados son prioridades. Las políticas de «no estigmatización» mejoran la cultura de ciberseguridad y animan a los empleados a notificar incidentes sin temor a represalias.

España: La clasificación por criticidad y el análisis de impacto son esenciales para identificar los componentes críticos e implementar las medidas de seguridad adecuadas. La segmentación de la red y la implementación de sistemas de monitorización avanzados son prácticas habituales para proteger las infraestructuras de OT.

Estonia: Las empresas estonias adoptan copias de seguridad periódicas, formación de los usuarios y el cumplimiento de las normas internacionales para mantener una sólida postura de seguridad. La segmentación de la red y el aislamiento de los sistemas heredados son esenciales para proteger los dispositivos de ataques externos.

Dinamarca: La seguridad multicapa y los planes de emergencia se consideran fundamentales para garantizar la continuidad operativa y la seguridad de las infraestructuras críticas. Las empresas implementan medidas de seguridad prácticas y actualizaciones periódicas para proteger los sistemas OT del acceso no autorizado.

Países Bajos: Una estructura organizativa clara y una respuesta en tiempo real son esenciales para garantizar la seguridad y la continuidad operativa. La flexibilidad en la gestión de la seguridad es crucial para hacer frente a nuevas amenazas y mantener un alto nivel de protección.

Área temática 3: Gaps de conocimiento y necesidades de competencias

Perfiles profesionales y competencias buscadas

Las empresas valoran una combinación de habilidades técnicas, capacidad para resolver problemas y una comprensión sistémica de la ciberseguridad. Las habilidades de trabajo en equipo y comunicación también son cruciales. Esto pone de relieve la necesidad de contar con profesionales completos, capaces de adaptarse a los retos cambiantes de la ciberseguridad.

Análisis específico por país

Italia: Es importante comprender los riesgos empresariales y tener una visión sistémica. Las habilidades técnicas en automatización y TI son fundamentales. Se valora la colaboración interfuncional y el pensamiento crítico. Las empresas buscan profesionales que puedan comprender los riesgos de manera holística y comunicarse eficazmente con las distintas partes interesadas.

España: Las empresas españolas exigen una combinación de competencias transversales, como la comunicación, el trabajo en equipo, la resolución de problemas y la flexibilidad, y competencias técnicas, como SCADA, cortafuegos industriales y segmentación de redes, siempre con una comprensión holística de la organización y el negocio principal.

Estonia: La capacidad de trabajar entre departamentos y las habilidades técnicas para garantizar la protección de los sistemas heredados y la segmentación de redes constituyen el núcleo de las habilidades que demandan las empresas estonias. Los especialistas en gestión de redes industriales y los administradores son perfiles muy buscados.

Dinamarca: Son habituales las habilidades prácticas en la gestión de infraestructuras críticas, la formación interna y los enfoques basados en escenarios. La seguridad multicapa y la preparación son fundamentales. Las empresas buscan perfiles con experiencia práctica en la gestión de la seguridad de sistemas OT.

Países Bajos: Son fundamentales los conocimientos técnicos en TIC y ciberseguridad, el dominio de las normas internacionales y unas sólidas habilidades de comunicación. El aprendizaje continuo y la capacidad de adaptación son esenciales. Las empresas buscan profesionales con competencias en seguridad en la nube e inteligencia artificial.

Área temática 3: Gaps de conocimiento y necesidades de competencias

Competencias técnicas específicas en ciberseguridad

El conocimiento de SIEM, EDR, seguridad de redes y cumplimiento de las normas internacionales goza de un amplio reconocimiento. Se valoran mucho el pensamiento crítico y la capacidad de resolución de problemas. El aprendizaje continuo y el estar al día de las últimas tendencias y tecnologías de seguridad son esenciales para los profesionales de la ciberseguridad.

Análisis específico por país

Italia: Las habilidades técnicas requeridas incluyen la gestión de eventos de seguridad (SIEM), la detección y respuesta en endpoints (EDR) y la seguridad de redes. El pensamiento crítico y la evaluación de riesgos son fundamentales. Las empresas también buscan habilidades en gestión de identidades y accesos (IAM) y análisis de registros de seguridad.

España: Las habilidades requeridas incluyen el análisis de vulnerabilidades, la gestión de incidentes y el conocimiento de los sistemas OT. Se hace hincapié en la formación continua y las medidas proactivas. Las empresas también buscan habilidades en cifrado, seguridad en la nube y monitorización de redes.

Estonia: Las habilidades técnicas incluyen el dominio de SIEM, EDR y seguridad de redes. El aprendizaje continuo y la adaptabilidad son esenciales para hacer frente a nuevas amenazas. Las empresas también buscan habilidades en gestión de identidades, configuración de cortafuegos y análisis de vulnerabilidades.

Dinamarca: Se valoran las habilidades prácticas en la gestión de infraestructuras críticas, la segmentación de redes y las medidas de seguridad prácticas. La preparación y la seguridad multicapa son fundamentales. Las empresas también buscan habilidades en gestión de registros de seguridad y respuesta a incidentes.

Países Bajos: Las habilidades requeridas incluyen seguridad de redes, computación en la nube e IA. El cumplimiento de la normativa y el aprendizaje continuo son esenciales para mantener un alto nivel de seguridad. Las empresas también buscan habilidades en análisis de datos de seguridad, gestión de identidades y protección de información sensible.

Área temática 3: Gaps de conocimiento y necesidades de competencias

Normas y certificaciones

Certificaciones como CISSP, ISO 27001 y otras normas del sector gozan de un amplio reconocimiento y son muy recomendadas. La experiencia práctica y el aprendizaje continuo son igualmente importantes. Las certificaciones proporcionan un punto de referencia para las habilidades y los conocimientos, pero la experiencia práctica y el aprendizaje continuo son esenciales para mantener un alto nivel de competencia en ciberseguridad.

Análisis específico por país

Italia: Las certificaciones recomendadas incluyen CISSP, ISO 27001 y programas de formación interna. Se hace hincapié en el aprendizaje continuo y la adaptabilidad. Las empresas también buscan certificaciones en seguridad de sistemas industriales y gestión de identidades.

España: Las certificaciones incluyen CISSP, CISM, CEH e ISO 27001. Se destaca la importancia del cumplimiento de nuevas normativas como la NIS2. Las empresas también buscan certificaciones en gestión de incidentes y seguridad en la nube.

Estonia: Las certificaciones requeridas incluyen CISSP, GSEC, ISO 27001 y normas locales como E-ITS. La formación continua y las pruebas de phishing son prácticas habituales. Las empresas también buscan certificaciones en gestión de identidades y respuesta a incidentes.

Dinamarca: Se valoran las certificaciones prácticas como CompTIA Security+, junto con la formación interna. La formación basada en escenarios es fundamental. Las empresas también buscan certificaciones en gestión de identidades y seguridad de infraestructuras críticas.

Países Bajos: Las certificaciones requeridas incluyen ISO 27001, NIS2 y otras normas del sector. Se hace hincapié en la experiencia práctica y la adaptabilidad. Las empresas también buscan certificaciones en seguridad en la nube y gestión de incidentes.

Área temática 3: Gaps de conocimiento y necesidades de competencias

Áreas emergentes dentro de la ciberseguridad

La seguridad en la nube, la seguridad impulsada por la IA y la seguridad del IoT se identifican como áreas de creciente demanda. La rápida evolución de la tecnología exige que los profesionales de la ciberseguridad actualicen continuamente sus habilidades y se adapten a los nuevos retos.

Análisis específico por país

Italia: La atención se centra en el pensamiento sistémico, la seguridad en la nube y la seguridad basada en la inteligencia artificial. La colaboración en equipo y la formación continua son esenciales para hacer frente a las nuevas amenazas. Las empresas buscan competencias en análisis de datos de seguridad y gestión de identidades.

España: La regulación de la IA y la seguridad del IoT son áreas de especialización emergentes. La integración de la IA y la gestión de datos en la nube se consideran cruciales para la seguridad. Las empresas buscan competencias en cifrado y protección de información confidencial.

Estonia: El doble papel de la IA en la ciberseguridad, la seguridad en la nube y el cumplimiento normativo son áreas de creciente demanda. La formación continua y la adaptabilidad son esenciales para hacer frente a las nuevas amenazas. Las empresas buscan competencias en análisis de datos de seguridad y gestión de identidades.

Dinamarca: La seguridad impulsada por la IA y la seguridad del IoT son áreas de creciente demanda. La seguridad multicapa y la preparación son fundamentales para mitigar los riesgos. Las empresas buscan competencias en gestión de identidades y protección de información confidencial.

Países Bajos: La seguridad en la nube, la seguridad impulsada por la IA y la seguridad del IoT se identifican como áreas emergentes. El cumplimiento normativo y el aprendizaje continuo son esenciales para mantener un alto nivel de seguridad. Las empresas buscan competencias en análisis de datos de seguridad y gestión de identidades.

Resumen de conclusiones

Área temática 1: Concienciación sobre ciberseguridad y riesgos en las empresas de tecnología operativa

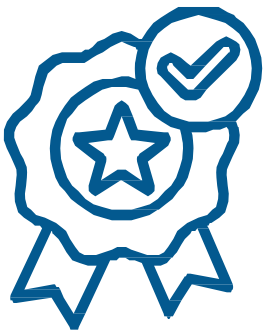
Conclusiones clave. Para mejorar la ciberseguridad: aumentar la concienciación, actualizar la formación, dar una respuesta rápida a los incidentes y revisar y mejorar continuamente las políticas de seguridad.

LA CONCIENCIACIÓN, LA FORMACIÓN Y LAS POLÍTICAS DE SEGURIDAD SON ESENCIALES

Beneficios de una mayor ciberseguridad: mayor confianza de los clientes, protección de la información confidencial, continuidad operativa, aumento de competitividad, cumplimiento normativo y eficiencia operativa.

Retos: carencias de competencias, escasa concienciación, gestión de sistemas heredados manteniendo la seguridad operativa en tiempo real.

Buenas prácticas: segmentación de la red, controles de acceso estrictos y actualizaciones periódicas del sistema, colaboración entre los departamentos de OT y IT.



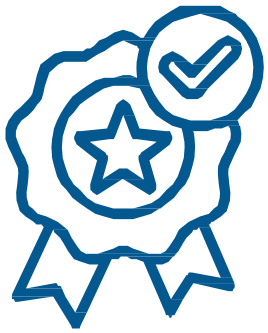
Resumen de conclusiones

Área temática 2: Prácticas de ciberseguridad en IT y OT

Conclusiones clave : Ciberseguridad a medida para garantizar la continuidad, la calidad y la eficiencia, así como la supervisión en tiempo real, son fundamentales.

LA CIBERSEGURIDAD A MEDIDA Y LA SEGMENTACIÓN DE RED SON CLAVE EN LOS ENTORNOS DE OT

Retos: limitaciones financieras, equipos, acceso limitado a Internet y falta de estandarización.



Buenas prácticas: segmentación de la red, gestión segura de proveedores, medidas de seguridad multicapa, formación práctica basada en escenarios y actualizaciones continuas del sistema.

Recomendaciones: Invertir en formación especializada y capacitar a los especialistas en IT para que puedan abordar los retos específicos de la tecnología operativa (OT). Fomentar la colaboración entre los departamentos de IT y OT y garantizar un enfoque de seguridad integral

Resumen de conclusiones

Área temática 3: Gaps de conocimiento y necesidades de competencias

Conclusiones clave: Es fundamental una combinación de competencias técnicas, capacidad de resolución de problemas y una comprensión sistémica de la ciberseguridad.

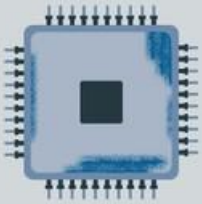
EL APRENDIZAJE CONTINUO Y UN ENFOQUE HOLÍSTICO SON ESENCIALES

Demanda de competencias: Gestión de información y eventos de seguridad (SIEM), detección y respuesta en endpoints (EDR) y seguridad de redes. Las empresas también valoraron las competencias en análisis de vulnerabilidades, gestión de incidentes y cumplimiento de normas internacionales. Se valoró especialmente la experiencia práctica en la gestión de infraestructuras críticas y el conocimiento tanto de los sistemas de TI como de los de TO.

Certificaciones: Certificaciones como la de Profesional Certificado en Seguridad de Sistemas de Información (CISSP), la ISO 27001 y otras normas del sector fueron ampliamente reconocidas y recomendadas. Estas certificaciones proporcionan un punto de referencia para las habilidades y los conocimientos requeridos en los puestos de ciberseguridad.

Áreas emergentes y Áreas de especialización: Seguridad, seguridad basada en IA y seguridad del IoT.

Cybersecurity weak points in companies



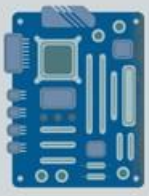
- Outdated firewalls
- Vulnerable identification systems
- Integration issues
- Lack or weak security policies
- Deficit in a comprehensive approach to cybersecurity risks
- Lack of standardization in OT systems
- Financial constraints
- Lack of specific OT expertise

Recommendations to improve cybersercurity in OT environments

- Continuous training of workers
- System updates
- Regular phishing tests / penetration tests
- Effective communication of security policy in the company
- Network segmentation and encryption
- Secure supplier management
- Regular backups
- Just in time monitoring
- Identification of critical components
- Comply with international standards
- Count with emergency plans
- Scenario based training

Skills demand for IT profiles

- Cybersecurity elements in an industrial plant
- Application of cybersecurity activities in operations and maintenance, according to the company´s security policy.
- Detection of anomalies in industrial control systems using monitoring tools and analysis procedures.



Skills demand for OT profiles

- Cloud security and AI
- Security Event Management (SIEM) and Endpoint Detection and Response (EDR)
- Network monitoring
- Security log management

Skills demand for both IT and OT profiles

- Understanding business risks and have a systematic vision
- Effective communication across profiles and departments regarding cybersecurity issues (policy, vulnerability detection, incidents...)
- International standards and regulations applied to the sector (with different proficiency levels of knowledge for IT and OT professionals). For example, CISSP, ISO 27001, NIS2.
- Understanding of the most frequent critical cybersecurity risks and their consequences/impact on the company (in terms of safety at work, money loses, environmental impact...)
- Critical thinking, problem solving, team collaboration, and continuous learning

Revisión de ciclos de FP IT y OT

Los focus group y las entrevistas realizadas por los socios nos permitieron comprender cuáles son los puntos débiles en materia de ciberseguridad en entornos industriales automatizados. Los comentarios recibidos también incluyeron algunos elementos clave para mejorar la ciberseguridad y cuáles son las competencias necesarias en los perfiles de IT y OT para implementarlos. Al analizar los programas de formación profesional que se imparten actualmente en los diferentes países socios (Países Bajos, España, Dinamarca, Italia y Estonia), pudimos identificar carencias concretas en relación con las competencias de ciberseguridad que demandan las empresas.

Dado que existen diferentes programas de formación profesional relacionados con las IT y la TO, aunque con denominaciones diferentes en los países socios, centramos nuestro análisis en dos perfiles:

- En el caso de las IT, el perfil es el de Técnico en Gestión y Administración de Redes, es decir, el profesional que planifica e implementa la infraestructura de red en una organización, elige los componentes de hardware y software adecuados, configura los dispositivos y protocolos de red y coordina la instalación de los equipos y cables de red, resuelve cualquier problema que surja y documenta la configuración y la topología de la red.

- En el caso de la OT, el perfil es el de un técnico en automatización y robótica industrial, es decir, el profesional que trabaja en empresas relacionadas con los sistemas industriales automáticos, en las áreas de diseño, montaje y mantenimiento de sistemas de automatización industrial.

En lo sucesivo, cuando mencionemos perfiles de IT/OT, nos referiremos en particular a este tipo de técnicos.

Para el perfil de IT, hemos analizado los certificados descritos en la tabla siguiente. Tras examinar los contenidos y los resultados de aprendizaje ya cubiertos por los planes de estudios actuales en los países del proyecto, hemos identificado aquellas carencias relacionadas con la ciberseguridad en entornos industriales interconectados, basándonos en las conclusiones de las empresas.

País	Título traducido del programa de formación	Duración del programa y número de horas	EQF nivel	Breve explicación de los ámbitos profesionales de actividad
Países Bajos	Ingeniero de sistemas de TIC	3 cursos académicos (2.500 horas)	4	Un ingeniero de sistemas TIC de nivel MBO 4 (itinerario BOL) se especializa en el diseño, la implementación, la gestión y el mantenimiento de infraestructuras de TI dentro de las organizaciones. Se encarga de garantizar el buen funcionamiento de las redes, los servidores y los sistemas operativos, dando respuesta a diversos aspectos de las necesidades tecnológicas de una organización.
España	Técnico superior en redes informáticas Gestión de sistemas	2 años académicos (2.000 horas)	5	El titular de este título habrá adquirido las competencias generales necesarias para: configurar, administrar y mantener sistemas informáticos, garantizando la funcionalidad del sistema, la integridad de los recursos y los servicios, con la calidad requerida y cumpliendo con la legislación vigente.
Estonia	Tecnologías de la Información y la Comunicación, nivel 4	2 años (si se accede desde la educación secundaria)	5	Un especialista en sistemas informáticos desarrolla y gestiona la infraestructura informática de una organización, proporcionando soluciones técnicas modernas soluciones para sistemas integrales.
Italia	Técnico Superior en Infraestructuras Informáticas, Redes, Nube y Virtualización - Especialista en Redes y Nube ITS	2 años (2.000 horas)	5	Este profesional es capaz de gestionar, comprender y diseñar sistemas de seguridad de seguridad para

El certificado de ingeniero de sistemas TIC en los Países Bajos se estructura en 5 áreas de competencia. Al comparar los resultados de aprendizaje ya cubiertos por el plan de estudios actual con las exigencias de las empresas industriales en materia de ciberseguridad, a continuación se muestran las carencias de competencias detectadas en cada una de esas áreas.

Áreas de competencia	Gaps relacionadas con la ciberseguridad en entornos industriales interconectados
Presta apoyo a usuarios/solicitantes/clientes	Tiene conocimientos básicos sobre la estructura de los entornos OT Comprende la importancia de la integración de IT y OT, incluidas las diferencias clave y los posibles retos de seguridad entre los entornos de IT y OT. Es capaz de comunicarse con profesionales de OT y actuar como puente entre las necesidades de OT y TI.
Instala y gestiona la infraestructura	Tiene conocimientos sobre protocolos y redes específicos de OT, como Modbus (por ejemplo). Conoce y comprende la estructura y los componentes de los sistemas OT, como los sistemas SCADA, los PLC (controladores lógicos programables) y los DCS (sistemas de control distribuido) Comprende la segmentación de redes para entornos OT y conoce los principios de diseño de redes que aíslan los sistemas OT de las redes de TI para minimizar los riesgos.
Gestiona aplicaciones	Tiene conocimientos sobre la gestión de parches para sistemas OT y comprende los retos específicos de la actualización de dispositivos OT, teniendo en cuenta factores como el tiempo de inactividad del sistema y la compatibilidad. Tiene conocimientos sobre las aplicaciones utilizadas en sistemas OT.
Desarrolla sistemas de información digital (gestión de bases de datos)	Tiene conocimientos de scripts básicos utilizados en entornos OT y de sus vulnerabilidades. Conoce las diferentes plataformas de datos para proteger los datos (big data).
Controles de seguridad	Conoce las posibles vulnerabilidades asociadas a los sistemas OT, como SCADA Es capaz de realizar evaluaciones de riesgos específicas para entornos OT con el fin de detectar las vulnerabilidades básicas en los sistemas OT Tiene conocimientos sobre las vulnerabilidades potenciales asociadas al hardware OT, como los PLC Tiene conocimientos sobre diversas normativas y legislaciones relacionadas con la ciberseguridad OT, como NIS2 e ISO 27001 Tiene conocimientos específicos sobre hardware y software centrados en la ciberseguridad OT para proteger sistemas y redes

En **España, el plan de estudios del Técnico Superior en Administración de Sistemas Informáticos en Red (ASIR)** está estructurado en módulos. Para cada uno de los módulos técnicos, hemos identificado las carencias relacionadas con la ciberseguridad industrial.

Áreas de competencia	Gaps relacionadas con la ciberseguridad en entornos industriales interconectados
Implementación de sistemas operativos	Sabe en qué consiste un sistema SCADA para una planta de producción.
Planificación y gestión de redes	Diseña y configura la segmentación de redes en una planta de producción, garantizando la implementación de medidas de ciberseguridad para proteger la infraestructura crítica y limitar el acceso a los sistemas sensibles. Conoce protocolos industriales como Modbus y OPC-UA
Fundamentos de hardware	Implementa políticas de seguridad físicas (autenticación, cámaras) y lógicas (antivirus, antimalware) para proteger los dispositivos OT críticos, garantizando la integridad y la disponibilidad de los sistemas industriales. Sabe qué es un PLC, sus características y funciones generales.
Gestión de bases de datos	Diseña y ejecuta consultas SQL seguras, implementando técnicas de saneamiento de entradas para prevenir ataques de inyección SQL.
Lenguajes de marcado y sistemas de gestión de la información	Implementa medidas de validación de datos para prevenir inyecciones de código en documentos XML, el cifrado de datos en el intercambio de información sensible y configura permisos de control de acceso para prevenir ataques de Cross-Site Scripting (XSS) en interfaces HTML
Gestión de sistemas operativos	Implementa Active Directory para controlar el acceso a los sistemas industriales, aplica políticas de seguridad y realiza auditorías y supervisión para proteger contra amenazas de seguridad. Configura servicios en la nube, como Infraestructura como Servicio (IaaS) y Plataforma como Servicio (PaaS), para mejorar la eficiencia, la seguridad y la escalabilidad de los sistemas industriales.
Servicios de red e Internet	Implementa redes inalámbricas industriales aplicando los estándares del sector. Gestiona servicios de red críticos en entornos industriales, como servidores SCADA, sistemas de control distribuido (DCS) y redes de sensores industriales. Implementa sistemas de detección de intrusiones (IDS) y segmentación de red para proteger los sistemas críticos contra el acceso no autorizado.
Implementación de aplicaciones web	Configura aplicaciones web utilizadas en entornos industriales, garantizando que se implementen las medidas de seguridad adecuadas, como la autenticación, el cifrado de datos y la protección contra vulnerabilidades comunes, como las inyecciones SQL y los ataques de Cross-Site Scripting (XSS).

Áreas de competencia	Gaps relacionadas con la ciberseguridad en entornos industriales interconectados
Administración de sistemas de gestión de bases de datos	Implementa medidas de ciberseguridad con sistemas MES, controlando el acceso a los datos, supervisando continuamente y garantizando la disponibilidad de las bases de datos distribuidas.
Seguridad y alta disponibilidad	Configura cortafuegos específicos para proteger las redes industriales contra el acceso no autorizado y los ciberataques. Conoce y aplica las normativas (NIS2) y estándares (IEC 62443, NIST SP 800-82, ISO 27001) de ciberseguridad específicos para entornos industriales. Desarrolla, implementa y gestiona políticas de seguridad en entornos OT. Conoce técnicas para identificar, preservar, analizar y presentar pruebas en caso de incidentes de seguridad, utilizando herramientas de análisis forense (Autopsy) para realizar investigaciones forenses en sistemas industriales. Implementa soluciones de virtualización para mejorar la seguridad y la gestión de los sistemas industriales, lo que permite una respuesta rápida ante incidentes. Configura sistemas de alta disponibilidad para garantizar la continuidad operativa de los sistemas industriales críticos, minimizando el tiempo de inactividad en caso de ataques.
Competencias transversales relacionadas con la ciberseguridad en entornos industriales interconectados	Comprende las operaciones empresariales y los riesgos críticos, con una visión sistémica/holística de las diferentes áreas/departamentos y las interacciones entre ellos. Comprende los riesgos críticos de ciberseguridad más frecuentes y sus consecuencias/impacto en la empresa (en términos de seguridad en el trabajo, pérdidas económicas, impacto medioambiental…). Se comunica de forma eficaz con los distintos perfiles y departamentos de la organización en lo relativo a cuestiones de ciberseguridad (políticas, detección de vulnerabilidades, incidentes, etc.). Colabora con los perfiles de OT de la organización para implementar actividades de ciberseguridad en la operación y el mantenimiento de la planta industrial. Toma decisiones en situaciones críticas. Planifica tareas. Escala las incidencias.

Los estudios estonios en Tecnologías de la Información y la Comunicación ofrecen diferentes alternativas de especialización basadas en asignaturas optativas. El plan de estudios está estructurado en créditos ECVET y ofrece una gran modularización. Sin embargo, incluso los itinerarios especializados en ciberseguridad presentan Gaps en materia de ciberseguridad industrial. Estas son las que hemos detectado en relación con 7 áreas de competencia:

Áreas de competencia	Gaps relacionadas con la ciberseguridad en entornos industriales interconectados
Gestión de la seguridad de la información	Comprensión de marcos como el Marco de Ciberseguridad del NIST, la norma ISO 27001 y los controles CIS. Creación y mantenimiento de documentación de acuerdo con normas como E-ITS e ISO 27002.
Gestión de la continuidad del negocio	Es esencial comprender y abordar los riesgos de seguridad específicos de la nube. Comprender las normativas de privacidad de datos (por ejemplo, el RGPD o la CCPA) e implementar medidas para proteger los datos sensibles.
Prestación de servicios	Identificar, evaluar y mitigar las vulnerabilidades en sistemas y aplicaciones. Desarrollar e implementar planes de respuesta a incidentes para gestionar eficazmente las brechas de seguridad. Desarrollar e impartir formación en materia de concienciación sobre seguridad a los empleados para mejorar su comprensión de las amenazas de seguridad y las mejores prácticas. Comprender la seguridad de los modelos de nube (IaaS, PaaS, SaaS) e implementación de medidas para proteger los datos y las aplicaciones en la nube. Configuración de cortafuegos, sistemas de detección de intrusiones y otros controles de seguridad de red para proteger contra el acceso no autorizado.
Protección de soluciones de TI	Comprensión de los derechos y permisos de los usuarios dentro de los sistemas de seguridad. Familiaridad con tecnologías específicas, como MS Security. Conocimiento de las leyes y normas pertinentes (p. ej., E-ITS, ISO). Capacidad para configurar y comprender políticas de seguridad. Conocimiento de las reglas de los cortafuegos, el análisis de registros y la gestión. Experiencia en diversas herramientas de ciberseguridad, incluidos IDS, cortafuegos y sistemas SIEM. Comprensión y aplicación de las mejores prácticas de seguridad de aplicaciones para protegerlas frente a vulnerabilidades.
	Habilidades analíticas y de resolución de problemas: capacidad para analizar incidentes de seguridad complejos y desarrollar soluciones eficaces. Habilidades de comunicación: Sólidas habilidades de comunicación para colaborar con equipos, partes interesadas y terceros. Conocimientos de hacking ético: Profundo conocimiento de las técnicas de hacking ético para identificar vulnerabilidades y mejorar la postura de seguridad. Aprendizaje continuo: compromiso de mantenerse al día con las últimas tendencias, amenazas y mejores prácticas en materia de ciberseguridad.

Los planes de estudios de la FP en Italia son diseñados por las regiones y pueden ser diferentes, incluso bastante diferentes, entre sí. Además, los planes de estudios pueden variar incluso de un centro a otro, especialmente en profesiones relacionadas con la tecnología y la digitalización. En el caso de **Italia**, decidimos analizar el plan de estudios del **Técnico Superior en Infraestructuras de IT, Redes, Nube y Virtualización — Especialista en Redes y Nube del ITS—,** por ser el más cercano a los demás analizados por los socios.

Áreas de competencia	Gaps relacionadas con la ciberseguridad en entornos industriales interconectados
Instalación de hardware y software	Formación sobre métodos específicos para mantener la seguridad durante la instalación de hardware y software, especialmente en entornos mixtos de IT/OT Garantizar la compatibilidad al tiempo que se mantiene la seguridad de la información. Identificar y mitigar las vulnerabilidades que puedan surgir durante la integración de sistemas. Abordar los riesgos que conlleva la integración de nuevas tecnologías con sistemas heredados, en particular aquellos vulnerables a amenazas comunes como el phishing o los componentes obsoletos. Mejorar la concienciación y la respuesta ante vectores de ataque comunes durante la instalación y configuración de componentes.
Arquitectura informática	Identificar y abordar las posibles vulnerabilidades en el diseño de hardware y software. Implementar medidas de seguridad que se adapten tanto a los cambios empresariales como a los tecnológicos. Asegurar los nuevos cambios arquitectónicos para mitigar el riesgo de amenazas cibernéticas. Hacer hincapié en los principios de diseño seguro para arquitecturas escalables e interoperables. Fortalecer la comprensión sistémica de las necesidades de ciberseguridad, garantizando que la escalabilidad y la interoperabilidad estén alineadas con marcos de seguridad robustos. Incorporar formación práctica en la identificación y evaluación de vulnerabilidades durante el diseño de la arquitectura. Mejorar la formación sobre el cumplimiento normativo y la aplicación de las normas de ciberseguridad durante la fase de arquitectura.
Administración de sistemas informáticos	Comprender las prácticas seguras para la instalación y actualización de software. Implementar procedimientos seguros para la configuración de las actualizaciones del sistema. Fomentar la concienciación sobre los riesgos relacionados con el software obsoleto y las actualizaciones. Hacer hincapié en las prácticas seguras de actualización de software, incluida la gestión de parches que aborde las vulnerabilidades tanto en los sistemas de TI como en los de TO. Formación práctica sobre cómo gestionar los sistemas OT obsoletos y sus retos de ciberseguridad, como mantener la seguridad al actualizar tecnologías antiguas. Abordar las carencias de habilidades en herramientas de seguridad específicas, como los sistemas de detección y respuesta en endpoints (EDR) y de gestión de información y eventos de seguridad (SIEM)

Áreas de competencia	Gaps relacionadas con la ciberseguridad en entornos industriales interconectados
Mantenimiento de sistemas	Aplicación de métodos seguros durante las reparaciones del sistema para prevenir vulnerabilidades. Detección de amenazas de ciberseguridad durante la ejecución de tareas de mantenimiento. Respuesta a incidentes relacionados con vulnerabilidades en el rendimiento del sistema; gestión integral de los incidentes manteniendo un alto nivel de satisfacción del cliente. Gestión segura de las actividades de reparación, especialmente en lo que respecta a los sistemas heredados. Ciberseguridad durante las actividades de reparación física y alineación de estas con los procedimientos definidos para evitar el acceso no autorizado.
Operaciones de TI	Técnicas avanzadas de detección y mitigación de amenazas de ciberseguridad. Planes de recuperación ante desastres con medidas de ciberseguridad. Respuestas en tiempo real a las amenazas, garantizando la continuidad operativa. Copias de seguridad seguras, incluida la gestión de los riesgos de seguridad durante el almacenamiento y la recuperación de datos. Abordar los retos para garantizar la continuidad, la calidad y la eficiencia en los sistemas OT, manteniendo al mismo tiempo los estándares de ciberseguridad.
Automatización	Prácticas seguras de scripting para garantizar que la automatización de la gestión no introduzca vulnerabilidades. Comprensión de las posibles vulnerabilidades en las herramientas y procedimientos de automatización. Ciberseguridad relacionada con las herramientas de automatización, incluidas las vulnerabilidades inherentes a los sistemas OT antiguos o heredados Automatización de las comprobaciones de ciberseguridad para garantizar el cumplimiento normativo y la integridad del sistema. Colaboración con los departamentos de TO para abordar la ciberseguridad en la automatización de forma integral.
Computación en la nube	Aplicación medidas de ciberseguridad específicas para la nube a medidas para proteger entornos virtuales. Garantizar la privacidad de los datos en entornos en la nube. Seguridad de redes descentralizadas, especialmente para entornos de tecnología operativa (OT) con requisitos operativos específicos. Seguridad basada en IA y seguridad del IoT. Conocimiento de las medidas de seguridad multicapa, especialmente aquellas destinadas a gestionar de forma segura los servicios en la nube de terceros
Definición y gestión de los indicadores clave de rendimiento (KPI)	Indicadores clave de rendimiento (KPI) centrados en la seguridad para evaluar y mejorar la postura de ciberseguridad de los entornos de IT y OT Análisis de datos para identificar brechas de ciberseguridad en el rendimiento del sistema. Incorporación de KPI basados en el riesgo que tengan en cuenta los sistemas heredados y sus posibles vulnerabilidades. Garantizar que los KPI reflejen las amenazas de ciberseguridad en constante evolución, como el ransomware y los ataques de phishing, y que se utilicen para impulsar mejoras proactivas en materia de seguridad. Interpretar los datos de los KPI para mejorar la toma de decisiones en materia de y las prioridades.

Hemos realizado el mismo ejercicio analítico con los planes de estudios de FP relacionados con los profesionales aptos para trabajar en entornos industriales con un alto nivel de digitalización. En este caso, hemos identificado dos perfiles principales: mecatrónica y automatización industrial. Cada socio ha analizado el plan de estudios relacionado con uno de ellos para identificar las deficiencias en materia de ciberseguridad.

País	Título traducido del programa de formación	Duración del programa y número de horas	EQF nivel	Breve explicación de los ámbitos profesionales de actividad
Países Bajos	Técnico en mecatrónica	3 años académicos (2.500 horas)	4	Un «Technicus Mechatronica» de nivel 4 de MBO (itinerario BOL) se especializa en el diseño, la construcción, la prueba y el mantenimiento de sistemas mecatrónicos que combinan tecnologías mecánicas, eléctricas e informáticas. Su trabajo abarca diversos sectores, entre los que se incluyen la fabricación, la automatización, la robótica y la maquinaria de alta tecnología
España	Técnico Superior en Automatización Industrial y Robótica	2 años académicos (2.000 horas)	5	El titular de este título habrá adquirido la competencia general en lo que respecta a: desarrollar y gestionar proyectos de montaje y mantenimiento de instalaciones automáticas de medición, regulación y control de procesos en sistemas industriales, así como supervisar, montar, mantener e implementar estos sistemas, respetando los criterios de calidad, seguridad y respeto por el medio ambiente, así como el diseño.
Estonia	Técnico en automatización	2 años (si se accede desde la educación secundaria)	5	El objetivo de los estudios es adquirir competencias que les permitan trabajar como trabajadores cualificados en empresas especializadas en automatización de la producción o en automatización de edificios.
Italia	Solución digital ITS 4.0 Especialista en la transición digital - ITS Transformación digital industrial Transformación Especialista	2 años (2.000 horas)	5	Los especialistas en IDT son profesionales de las tecnologías de la información que desarrollan soluciones integradas a medida para guiar a las empresas hacia la digitalización, creando entornos ciberfísicos que optimizan la gestión de datos.

En el plan de estudios impartido en los **Países Bajos para «Technicus Mechatronica MBO 4**», hay tres áreas de competencia principales. Aunque el plan de estudios ofrece una buena combinación de conocimientos y habilidades en IT y OT, seguimos detectando grandes Gaps en materia de ciberseguridad.

Áreas de competencia	Gaps relacionadas con la ciberseguridad en entornos industriales interconectados
Fabricación de productos mecatrónicos	Posee conocimientos fundamentales sobre el IoT (Internet de las cosas) y comprende cómo se integra el IoT en los sistemas mecatrónicos para la monitorización, el control y la recopilación de datos a distancia Posee conocimientos básicos de TI en un entorno industrial y comprende los aspectos de TI relevantes que intervienen. Posee conocimientos sobre concienciación para garantizar la seguridad de los desarrollos Posee conocimientos para proteger la infraestructura de las máquinas y el aprendizaje automático
Instalación y modificación de productos y/o sistemas mecatrónicos	Posee conocimientos básicos de ciberseguridad para entornos industriales Conoce los riesgos básicos comunes de ciberseguridad en entornos industriales Conocimientos básicos de redes y conectividad, y comprensión de los fundamentos de la resolución de problemas de conexiones de red Capacidad para supervisar los riesgos relacionados con el uso o la instalación de herramientas Conciencia de las posibles amenazas dentro de los programas o herramientas que se van a utilizar
Orientación y gestión del proceso de trabajo	Sabe utilizar herramientas de monitorización y diagnóstico remotas que permiten el diagnóstico, la monitorización y el mantenimiento a distancia de equipos mecatrónicos. Es capaz de comunicarse con especialistas en TI para trabajar de forma orientada a la resolución de problemas. Posee conocimientos sobre protección de datos. Tiene conocimientos o comprende las amenazas a la ciberseguridad, como el phishing, el malware o las tácticas de ingeniería social.

En **España, hemos analizado el perfil de un Técnico Superior en Automatización y Robótica Industrial (ARI)**, que es el más demandado por las empresas en nuestro contexto para fusionarse con las competencias informáticas relacionadas con la ciberseguridad. El Gobierno español ha creado incluso un curso de especialización en ciberseguridad en entornos OT, accesible para quienes ya posean el título de Técnico Superior en Automatización Industrial y Robótica (más información en el suplemento Europass:

Áreas de competencia	Gaps relacionadas con la ciberseguridad en entornos industriales interconectados
Sistemas eléctricos, neumáticos e hidráulicos	Es consciente de la necesidad de cambiar las contraseñas predeterminadas de dispositivos como relés o controladores neumáticos para proteger el acceso a los equipos.
Sistemas secuenciales programables	Implementa controles de acceso mediante contraseña en los sistemas de control secuencial para garantizar que solo el personal autorizado pueda modificar la lógica de control.
Sistemas de medición y control	Supervisa y registra las lecturas de los sensores para poder identificar comportamientos anómalos o la manipulación de datos con el fin de detectar posibles problemas de seguridad.
Sistemas de energía	Conoce la importancia de cambiar las credenciales predeterminadas de los dispositivos conectados a la red, como los inversores o los sistemas SAI, una práctica sencilla pero crucial para evitar el acceso no autorizado
Documentación técnica	Incluye el historial de cambios en la documentación técnica, registrando quién modificó cada sección y cuándo, lo que ayuda a prevenir y detectar alteraciones no autorizadas.
Informática industrial	Instala y configura antivirus y cortafuegos en los sistemas informáticos que controlan la producción, como una forma sencilla de proteger los sistemas contra el malware.
Sistemas programables avanzados	Bloquea el acceso remoto a los PLC cuando no es necesario, como medida básica de protección contra el acceso no autorizado.

Áreas de competencia	Gaps relacionadas con la ciberseguridad en entornos industriales interconectados
Robótica industrial	Configura listas de acceso en robots industriales para definir qué usuarios pueden modificar programas o controlar el robot, reduciendo el riesgo de manipulaciones no deseadas.
Comunicación industrial	Comprende las principales vulnerabilidades relacionadas con la computación en la nube (configuración incorrecta, amenazas internas, pérdida y fuga de datos, e interfaces y API inseguras) y cuáles son los métodos utilizados por los hackers para aprovecharlas (phishing, errores de software, ataques DoS, ingeniería social, ransomware y malware). Conoce métodos y herramientas para proteger las vulnerabilidades relacionadas con la computación en la nube, en consonancia con la política de seguridad de la organización. Conoce el plan de respuesta a incidentes, que forma parte de la solución SIEM implementada por la organización. Interpreta y detecta anomalías basándose en los datos proporcionados por los sistemas MES (Manufacturing Execution Systems) y los sistemas HMI. Configura el cifrado básico en la transmisión de datos, por ejemplo, utilizando VPN o protocolos seguros para proteger las comunicaciones entre dispositivos industriales.
Integración de la automatización industrial	Tiene en cuenta los riesgos existentes a la hora de planificar e instalar un sistema automático, identificando cuándo se necesita un sistema EDR y cuál elegir. Conoce las normas y regulaciones internacionales aplicables al sector (por ejemplo, CISSP, ISO 27001, NIS2) y, en particular, la norma ISA/IEC 62443, especialmente relevante para la automatización industrial. Aplica la gestión de registros de seguridad al planificar e instalar un sistema automático. Conoce los ICS (sistemas de control industrial, como SCADA) y conoce los diferentes componentes de una red OT y cómo se interconectan. Segmentación de redes: crear diagramas que aíslen las redes de automatización críticas del resto de las redes de la empresa.
Competencias transversales relacionadas con la ciberseguridad en entornos industriales interconectados	Comprende los riesgos empresariales y tiene una visión sistémica/holística de las diferentes áreas/departamentos y de las interacciones entre ellos. Alto nivel de concienciación sobre los riesgos cibernéticos que afectan a los sistemas OT, conociendo sitios como shodan.io y su sección dedicada a ICS o MITREATT&CKforICS1 para evaluar el número de amenazas a las que están expuestos estos sistemas. Se comunica de forma eficaz entre perfiles y departamentos en lo relativo a cuestiones de ciberseguridad (políticas, detección de vulnerabilidades, incidentes…). Concienciación: identificación de amenazas comunes en entornos industriales. Resolución de problemas: detección y corrección de fallos de seguridad. Gestión de riesgos: evaluación de riesgos: identificación de posibles vulnerabilidades. Comunicación eficaz: explicar las mejores prácticas básicas de seguridad a un público sin conocimientos técnicos (como los operadores). Responsabilidad y ética profesional: analizar las brechas de seguridad que pueden afectar a personas y empresas. Autonomía y aprendizaje continuo: mantenerse al día de las últimas tendencias en ciberseguridad industrial.

Tras examinar diferentes perfiles en **Estonia**, hemos seleccionado el plan de estudios de «Automatización», cuyo contenido es muy similar al del plan de estudios español, aunque está estructurado de forma diferente, con una combinación de estudios generales y estudios técnicos. Para el análisis, nos hemos centrado únicamente en la parte técnica. Las carencias relacionadas con la ciberseguridad industrial son muy similares a las detectadas en el plan de estudios español.

Áreas de competencia	Gaps relacionadas con la ciberseguridad en entornos industriales interconectados
Puesta en marcha de equipos y sistemas de automatización	Arquitecturas ICS: Familiarizarse con las arquitecturas ICS más comunes, incluidos los sistemas de control de supervisión y adquisición de datos (SCADA), los sistemas de control distribuido (DCS) y los controladores lógicos programables (PLC). Protocolos de comunicación industrial: Comprender protocolos como Modbus, Profibus, Ethernet/IP y OPC UA, así como sus implicaciones en materia de seguridad. Dispositivos OT: Conocer las vulnerabilidades específicas de los dispositivos OT, como sensores, actuadores y controladores.
Instalación de equipos y sistemas de automatización	Segmentación de redes: Implemente la segmentación de redes para aislar las redes OT de las redes de TI corporativas y reducir la superficie de ataque. Configuración de cortafuegos: Configurar cortafuegos para restringir el acceso a las redes y dispositivos OT. Gestión de parches: Actualizar periódicamente los dispositivos y el software OT con parches de seguridad. Control de acceso: Implemente controles de acceso rigurosos para limitar quién puede acceder a los sistemas y dispositivos OT. Supervisión de la seguridad: Utilice herramientas de supervisión de la seguridad para detectar y responder a actividades anómalas en las redes OT.
Conocimientos básicos de automatización	Espionaje industrial: Comprender los riesgos del acceso no autorizado a los sistemas OT con el fin de robar propiedad intelectual o interrumpir las operaciones. Sabotaje: Estar al tanto de las amenazas de actores maliciosos que pretenden dañar o interrumpir infraestructuras críticas. Ataques a la cadena de suministro: Comprender los riesgos que entraña el compromiso de componentes de hardware o software.
Fundamentos de ingeniería eléctrica y electrónica	Conoce la importancia de cambiar las credenciales predeterminadas de los dispositivos conectados a la red, como los inversores o los sistemas SAI, una práctica sencilla pero crucial para evitar el acceso no autorizado. Control y actualización de contraseñas.
Competencias transversales	Actualización profesional sobre el hackeo de sistemas de control industrial: Manténgase informado sobre las últimas técnicas utilizadas por los atacantes para atacar los ICS. Inteligencia artificial y aprendizaje automático para mejorar la seguridad de la tecnología operativa (OT), por ejemplo, para la detección de anomalías y el mantenimiento predictivo.

El plan de estudios analizado en el caso de **Italia** es, sin duda, el que ofrece el programa más «híbrido» entre conocimientos y habilidades de IT y OT de entre los explorados por la asociación en los niveles 4-5 del MEC en nuestros respectivos países. Aunque ofrece una buena combinación, hemos detectado varias carencias en materia de ciberseguridad.

Áreas de competencia	Deficiencias relacionadas con la ciberseguridad en entornos industriales interconectados
Implementación de la empresa digital	Integridad de los datos, confidencialidad y detección de amenazas. Normas y protocolos de seguridad en los sistemas informáticos. Formación práctica basada en escenarios y simulaciones para mejorar la respuesta ante incidentes.
Programación y pruebas **Diseño y desarrollo de aplicaciones**	Prácticas de codificación segura para prevenir vulnerabilidades. Modelización de amenazas como parte del desarrollo de software. Análisis de vulnerabilidades, sistemas SIEM y EDR para mejorar la seguridad de la codificación. Metodologías de depuración seguras para identificar y mitigar los riesgos de seguridad.
Diseño e implementación de soluciones de IoT	Comunicación segura entre dispositivos de automatización industrial. Vulnerabilidades específicas de los sistemas de control en tiempo real. Mitigación de riesgos en redes de automatización.
Tecnología de monitorización	Arquitecturas de red seguras para la integración IT-OT. Técnicas de segmentación para reducir los riesgos de seguridad. Sistemas heredados y seguridad operativa en tiempo real. Mitigación de amenazas específicas de OT y respuesta a incidentes
Toma de decisiones estratégicas	Impacto de la integración de nuevas tecnologías en la ciberseguridad. Identificación de vulnerabilidades introducidas por tecnologías emergentes. Validación de la seguridad antes de implementar nuevas tendencias. Seguridad en la nube, seguridad impulsada por IA y seguridad del IoT como áreas emergentes de demanda. Incorporar consideraciones de ciberseguridad en la planificación estratégica de las TIC. Centrarse en medidas de protección de datos para procesos orientados al cliente. Alinear las estrategias de TIC con los estándares de ciberseguridad del sector y el cumplimiento normativo. Desarrollo de marcos de ciberseguridad que refuercen la confianza de los clientes y la ventaja competitiva.

Áreas de competencia	Gaps relacionadas con la ciberseguridad en entornos industriales interconectados
Gestión de clientes	Evaluación de riesgos de ciberseguridad como parte del asesoramiento al cliente. Gestión segura de proveedores y estándares de ciberseguridad. Soluciones tecnológicas resilientes y seguras. Análisis de las necesidades de seguridad del cliente para ofrecer asesoramiento personalizado sobre alternativas tecnológicas. Gestión de incidentes.
Transformación digital	Gestión de riesgos de ciberseguridad durante iniciativas de transformación digital. Procedimientos estandarizados, copias de seguridad y supervisión en tiempo real para la continuidad del proyecto. Comunicación segura e integridad del sistema durante los cambios. Protección de los activos digitales a lo largo del ciclo de vida de la transformación.
Gestión de proyectos	Gestión de riesgos de ciberseguridad en la planificación de proyectos. Gestión segura de hitos críticos del proyecto que impliquen la convergencia de IT y OT. Comunicación y coordinación seguras dentro de equipos multifuncionales. Cumplimiento normativo y enfoque basado en el riesgo para gestionar la ciberseguridad. Indicadores clave de rendimiento (KPI) de ciberseguridad, como la frecuencia de incidentes y las vulnerabilidades del sistema. Informes sobre medidas de ciberseguridad. Evaluación del rendimiento según las normas de ciberseguridad.

Conclusiones clave

Los programas de FP en IT y OT analizados son similares en todos los países del proyecto, lo que confirma los comentarios recibidos de las empresas durante los grupos focales, independientemente del sector en el que operen.

En los niveles del MEC analizados, hemos observado que los programas de formación profesional en Estonia e Italia ofrecen una gama más amplia de especializaciones y una combinación de contenidos de IT y OT, pero siguen pasando por alto las competencias específicas de ciberseguridad en entornos industriales.

Próximos pasos

Tras analizar los diferentes programas de FP relacionados con las IT (gestión de redes) y la OT (automatización industrial y digitalización), hemos clasificado las carencias en tres grupos de competencias necesarias para que los trabajadores de IT y OT puedan trabajar en entornos industriales ciberseguros:

COMPETENCIAS TÉCNICAS

Las necesarias para desempeñar su trabajo habitual, incluidas las competencias técnicas en ciberseguridad acordes con su perfil y su función en la organización.

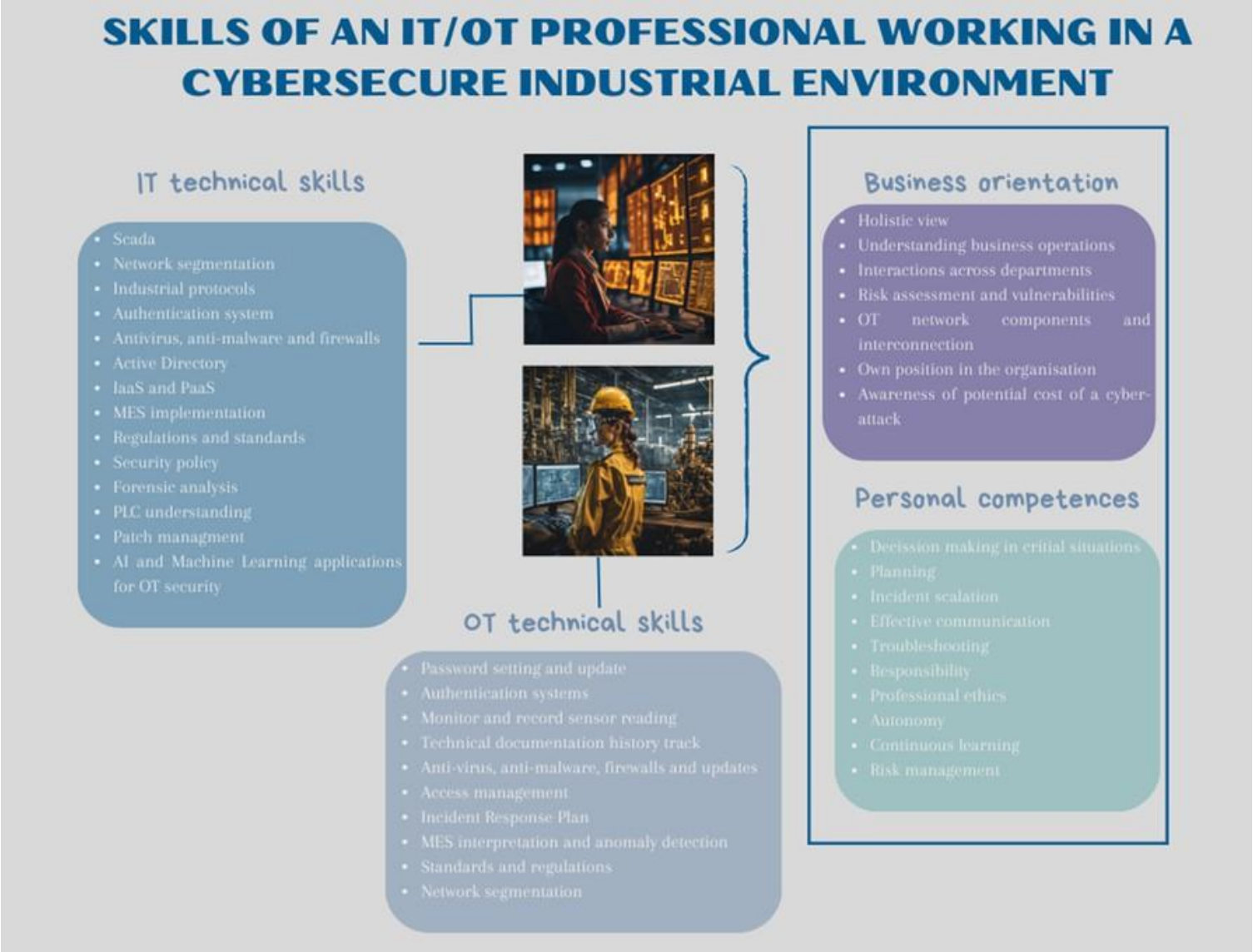
ORIENTACIÓN EMPRESARIAL

La capacidad de comprender la empresa en su conjunto, así como de posicionarse dentro del esquema de la empresa. También incluye la capacidad de evaluar los riesgos potenciales de un ciberataque para la empresa, así como el impacto que podría tener en la seguridad de las personas, la capacidad de producción o los datos sensibles.

COMPETENCIAS PERSONALES

Competencias necesarias para interactuar con compañeros y entre departamentos de la empresa, reflexionar y pensar de forma crítica, resolver problemas, analizar situaciones desde diferentes perspectivas, trabajar de forma autónoma pero también como parte de un equipo y actuar con espíritu de equipo.

Hemos agrupado las habilidades identificadas como carencias en cada plan de estudios según la clasificación mencionada. Las habilidades técnicas son específicas de cada perfil (TI/TO), pero las que se engloban en las categorías «orientación empresarial» y «competencias personales», en lo que respecta a la ciberseguridad, son las mismas para ambos.



Mientras que en los distintos países existen opciones para continuar estudiando y especializándose en ciberseguridad industrial dirigidas tanto a perfiles de FP de OT como de IT, el enfoque de Cyber-In consiste en entender las competencias de ciberseguridad como transversales a cualquier profesional y, en particular, la ciberseguridad industrial como transversal a los profesionales de IT y OT, especialmente a aquellos más involucrados en procesos industriales automatizados, tal y como demandan las empresas.

Con el fin de proporcionar entornos industriales seguros con un alto nivel de automatización (entendiendo la seguridad desde todos los puntos de vista posibles), la ciberseguridad debe integrarse en el plan de estudios de los profesionales de IT y OT.

Además, las demandas de la industria se orientan hacia un perfil híbrido/interdisciplinario de TI/OT, especialista en ciberseguridad industrial. Si bien la integración de los resultados de aprendizaje relacionados con la ciberseguridad en los perfiles actuales de IT y OT que se imparten en los distintos países mejorará la preparación de estos profesionales, nuestra recomendación, como resultado de nuestras conclusiones, es ofrecer un plan de estudios de FP interdisciplinario en ciberseguridad industrial como especialización para ambos tipos de profesionales.

Hemos definido dicho plan de estudios alineado con los marcos EQF y ECTS, utilizando una estructura modular que puede dividirse en microcredenciales para facilitar la adquisición y acreditación de las competencias necesarias.

Curriculum interdisciplinar en ciberseguridad industrial

Estructura del plan de estudios e integración en los programas de FP existentes

Este plan de estudios interdisciplinario integra competencias en ciberseguridad de las tecnologías de la información (IT) y las tecnologías operativas (OT) en un programa de especialización dirigido a titulados y trabajadores de estos campos. Aborda las carencias de competencias identificadas en el informe Cyber-In sobre las necesidades de las empresas y promueve prácticas de seguridad colaborativas en entornos de OT, garantizando que los titulados y trabajadores de este campo sean capaces de diseñar, implementar y mantener sistemas industriales seguros.

El plan de estudios se ajusta a perfiles del ESCO como «técnico en ciberseguridad» y «técnico en automatización industrial», abarcando las competencias comunes a estos dos perfiles. Se ha estructurado siguiendo los principios del ECTS, donde 1 crédito equivale a aproximadamente 25 horas de aprendizaje.

El número total de horas del plan de estudios es de aproximadamente 250 horas, lo que equivale a 10 créditos ECTS. De acuerdo con el Marco Europeo de Cualificaciones y teniendo en cuenta que este programa de especialización se dirige principalmente a personas ya tituladas en programas de FP en IT/OT con un nivel 4-5 del MEC, el programa de especialización se ha concebido como un nivel 5 del MEC en sí mismo.

Si bien se fomenta el desarrollo del plan de estudios interdisciplinario completo propuesto por el proyecto Cyber-In, el objetivo de Cyber-In no es desarrollar un programa de especialización que se complete como complemento a los actuales títulos de formación profesional en IT y OT, sino INCORPORAR algunos de los resultados del aprendizaje (conocimientos, habilidades y competencias) definidos en el plan de estudios e identificados por las empresas entrevistadas por los socios del proyecto como transversales y esenciales para un profesional de la administración y gestión de redes de IT y para operadores en entornos industriales automatizados e interconectados.

Curriculum interdisciplinar en ciberseguridad industrial

Estructura curricular e integración en los programas de FP existentes

Por lo tanto, hemos diseñado un curso más breve que aborda los resultados de aprendizaje mencionados y que puede integrarse más fácilmente en los programas actuales porque:

- Tiene una duración más breve y está fragmentado en módulos y capítulos cortos, lo que facilita su integración en los contenidos actuales que ya se imparten en los programas de TI y de formación profesional.

- Incide especialmente en los aspectos actitudinales e influye en el factor humano y en la concepción de la ciberseguridad como parte de la cultura empresarial.

- Se centra en conceptos clave, definiciones y herramientas relacionadas con la ciberseguridad industrial. No profundiza en los aspectos técnicos, pero cubre lo esencial y deja margen para centrarse en aspectos concretos de la ciberseguridad industrial en función de la finalidad del curso o de los objetivos de aprendizaje fijados por el profesor/formador o el trabajador, en el caso de empleados o recién titulados.

El MOOC «Cyber-In» permite a los alumnos comprender los principales conceptos y elementos relacionados con la ciberseguridad industrial. Les permite utilizar e interpretar herramientas de monitorización, analizar posibles riesgos y vulnerabilidades, y adoptar un enfoque proactivo para minimizar los riesgos de violación de la seguridad. Además, proporciona a los alumnos conocimientos sobre la normativa más reciente en materia de ciberseguridad en entornos industriales y sobre cómo esta afecta a las empresas y a su papel como profesionales.

El MOOC es de acceso libre, sin necesidad de registrarse, para cualquier usuario interesado en mejorar esas competencias. Se puede acceder a él a través de la página web del proyecto: www.cyber-in.eu, en la sección «recursos de aprendizaje».

Curriculum interdisciplinar en ciberseguridad industrial

Plan de estudios. Estructura e integración en los programas de FP existentes

Título del módulo	ECTS	Duración
Módulo 1. Introducción a la ciberseguridad en entornos OT	0,4	10 horas
Módulo 2. Segmentación y protocolos industriales	1,6	40 horas
Módulo 3. Sistemas de detección de intrusiones (IDS) para la gestión de la continuidad del negocio	1,2	30 horas
Módulo 4. Normas y regulaciones de ciberseguridad OT	0,8	20 horas
Módulo 5. Sistemas centralizados de gestión de la seguridad y aplicaciones de IA	1,2	30 horas
Módulo 6. Gestión de la continuidad del negocio y prestación de servicios	0,8	20 horas
Módulo 7. Proyecto: Protección de una fábrica inteligente	4	100 horas

Curriculum interdisciplinar en ciberseguridad industrial

Descripciones de los módulos

Módulo 1 — Introducción a la ciberseguridad en entornos OT

Duración: 10 horas | 0,4 créditos ECTS

Objetivo: Comprender los fundamentos de la ciberseguridad, la convergencia entre IT y OT, y el panorama de amenazas industriales.

Contenidos:

- Principios y definiciones de ciberseguridad: la tríada CIA, la defensa en profundidad, riesgo frente a resiliencia.
- Diferencias entre las prioridades de TI y de TO.
- Casos prácticos: Stuxnet, BlackEnergy, Industroyer…

Resultados del aprendizaje:

- Conocimientos: Explicar los principios de la OT, el control de procesos y la relación entre la CIA y la seguridad.
- Habilidades: Identificar los componentes de los sistemas OT y situarlos dentro de la arquitectura de una planta.
- Competencias: Reconocer las consecuencias ciberfísicas de las brechas de seguridad.

Métodos de evaluación: Debate en grupo, evaluación práctica, examen.

Microcredencial 1: **Módulo 1 de Cyber-In. Introducción a la ciberseguridad en entornos OT**

Curriculum interdisciplinar en ciberseguridad industrial

Descripciones de los módulos

Módulo 2 — Segmentación y protocolos industriales

Duración: 40 horas | 1,6 créditos ECTS

Objetivo: Identificar y clasificar componentes y arquitecturas industriales utilizando el modelo de Purdue.

Contenidos:

- Componentes OT: PLC, RTU, SCADA, sensores, HMI.
- Mapeo del sistema, inventario de activos e interdependencias.
- Jerarquía de control industrial y mapeo del flujo de datos.

Resultados del aprendizaje:

- Conocimientos: Describir el modelo Purdue, las zonas de red, los conductos y los flujos de datos.
- Habilidades: Aplicar la segmentación e identificar protocolos inseguros.
- Competencias: Diseñar y documentar un plan de segmentación de la red OT.

Métodos de evaluación: Debate en grupo, evaluación práctica, examen.

Microcredencial 2: **Módulo 2 de Cyber-In. Segmentación y protocolos industriales**

Curriculum interdisciplinar en ciberseguridad industrial

Descripciones de los módulos

Módulo 3 — Redes industriales y seguridad de protocolos

Duración: 30 horas | 1,2 créditos ECTS

Objetivo: Proteger los protocolos industriales y los canales de comunicación.

Contenidos:

- Seguridad de Modbus, OPC-UA, PROFINET, DNP3 y MQTT.
- Herramientas de análisis de redes e inspección de paquetes.
- Diseño e implementación de canales seguros (TLS, VPN).

Resultados del aprendizaje:

- Conocimientos: Cortafuegos de última generación
- Habilidades: Configurar sensores IDS/IPS, interpretar alertas, evaluar anomalías.
- Competencias: Correlacionar los datos de monitorización con las necesidades de seguridad operativa y proponer medidas correctivas.

Métodos de evaluación: Debate en grupo, evaluación práctica, examen.

Microcredencial 3: Módulo 3 de Cyber-In. Sistemas de detección de intrusiones y seguridad en

Curriculum interdisciplinar en ciberseguridad industrial

Descripción de los módulos

Módulo 4 — Normas y reglamentos de ciberseguridad de sistemas operativos de tecnología operativa

Duración: 20 horas | 0,2 créditos ECTS

Objetivo: Aprender las principales normas y regulaciones en materia de ciberseguridad de sistemas de tecnología operativa

Contenidos:

- Ley de ciberresiliencia de la UE
- IEC 62443
- Evaluación de la ciberseguridad y tipos de pruebas

Resultados del aprendizaje:

- Conocimientos: Diferencia entre directiva, norma y reglamento
- Habilidades: Pruebas de penetración y detección de vulnerabilidades
- Competencias: Cumplimiento de normas y reglamentos

Métodos de evaluación: Debate en grupo, evaluación práctica, examen.

Microcredencial 4. Módulo 4 de Cyber-In. Normas y regulaciones de ciberseguridad de OT

Curriculum interdisciplinar en ciberseguridad industrial

Descripciones de los módulos

Módulo 5 — Sistemas centralizados de gestión de la seguridad y aplicaciones de IA

Duración: 30 horas | 1,2 créditos ECVET/ECTS

Objetivo: Aplicar las normas pertinentes y realizar evaluaciones de riesgos de ciberseguridad industrial.

Contenidos:

- Gestión centralizada de la seguridad
- Aplicaciones de IA
- Gobernanza y políticas

Resultados del aprendizaje:

- Conocimientos: Comprensión del CMS
- Habilidades: identificar funciones, políticas y procedimientos esenciales para la gobernanza de la seguridad
- Competencias: aplicar el CMS y utilizar aplicaciones de IA para la detección y respuesta ante amenazas

Métodos de evaluación: Debate en grupo, evaluación práctica, examen.

Microcredencial 5. Módulo de Cyber-In: Sistemas de gestión de seguridad centralizada y detección de amenazas en tiempo real en entornos de TI empresariales

Curriculum interdisciplinar en ciberseguridad industrial

Descripción del módulo

Módulo 6 — Gestión de la continuidad del negocio y prestación de servicios

Duración: 20 horas | 0,8 créditos ECTS

Objetivo: Integrar la ingeniería de seguridad y la ciberseguridad en infraestructuras críticas.

Contenidos:

- Concepto y retos de la gestión de la continuidad del negocio
- Buenas prácticas
- Prestación de servicios
- ITIL

Resultados del aprendizaje:

- Conocimientos: Comprender los conceptos de gestión de la continuidad del negocio (BCM), prestación de servicios y «Zero Trust»
- Habilidades: Cómo garantizar la gestión de la continuidad y la prestación de servicios
- Competencias: Aplicar estrategias de recuperación y diseñar planes de respuesta a incidentes

Métodos de evaluación: Debate en grupo, evaluación práctica, examen.

Microcredencial 6 — Módulo Cyber-In: Gestión de la continuidad del negocio y prestación de servicios

Curriculum interdisciplinar en ciberseguridad industrial

Descripciones de los módulos

Módulo 7 — Proyecto. Protección de una fábrica inteligente

Duración: 100 horas | 4 créditos ECTS

Objetivo: Aplicar todas las competencias adquiridas en los módulos anteriores en un escenario simulado de fábrica inteligente.

Contenidos:

- Diseño e implementación en equipo de una red industrial segura.
- Pruebas de seguridad, mitigación de riesgos y gestión de incidentes.
- Presentación del proyecto.

Resultados del aprendizaje:

- Conocimientos: Integrar el diseño de la tecnología operativa (OT), la gestión de riesgos y los conceptos de normas y regulaciones.
- Habilidades: Desarrollar y presentar un plan de ciberseguridad industrial.
- Competencias: Justificar las decisiones tomadas en materia de diseño y seguridad.

Métodos de evaluación: Debate en grupo, evaluación práctica, examen.

Microcredencial 7. Actividad de aprendizaje basada en

Conclusiones

La ciberseguridad de la tecnología operativa (OT) aumenta la confianza de los clientes y garantiza la continuidad operativa

Las empresas de los países participantes reconocen que la ciberseguridad ofrece numerosas ventajas, entre ellas una mayor confianza de los clientes, la protección de la información sensible y la garantía de la continuidad operativa. Los beneficios de proteger el entorno OT chocan con el reto de encontrar profesionales de TI con conocimientos específicos sobre redes OT, así como profesionales de OT con el nivel adecuado de concienciación sobre los riesgos de ciberseguridad y la autonomía y las habilidades técnicas suficientes para desempeñar un papel en la arquitectura global de ciberseguridad de la empresa.

Por lo tanto, aumentar la concienciación y la formación es crucial para mejorar la ciberseguridad en entornos industriales con un alto nivel de automatización. Las empresas que dan prioridad a la formación continua, a la colaboración entre los departamentos de IT y OT, y a la implementación de las mejores prácticas están mejor equipadas para proteger sus infraestructuras críticas y mantener la continuidad operativa.

La sensibilización y la formación en competencias técnicas y personales son fundamentales

Existe una gran demanda de una combinación de competencias personales, habilidades técnicas y un enfoque holístico de la empresa, incluida la capacidad de colaboración entre los departamentos de IT y OT para garantizar un enfoque de seguridad eficaz.

Sin embargo, la realidad actual en los centros de formación profesional es que los planes de estudios de IT y OT no responden a estas exigencias. Existe una falta generalizada de atención a la ciberseguridad en los programas de FP de TI cuando se hace referencia a entornos industriales, y esta falta de atención a la ciberseguridad es absoluta en los programas de TO. Podríamos afirmar que el principal problema de los profesionales de TI es la falta de conocimientos y habilidades sobre una red de TO, mientras que la deficiencia de los profesionales de TO comienza por la falta de concienciación. Esta realidad es común a todos los países socios, por lo que las carencias detectadas en ambos tipos de profesionales en cuanto a habilidades de ciberseguridad son prácticamente las mismas.

Partiendo de esta realidad, no hay otra opción que empezar a crear concienciación y conocimientos integrando la ciberseguridad en los planes de estudios de IT y OT como una competencia transversal, comenzando
por los profesores y formadores y extendiéndola a los estudiantes.

Agradecimientos

Queremos dar las gracias a las empresas que participan en el proyecto Cyber-In, en particular a las que participan en los grupos de discusión nacionales, por su disponibilidad, entusiasmo y compromiso con la mejora de la formación profesional continua. Su contribución ha sido esencial no solo para elaborar este informe y poner en marcha las futuras fases del proyecto, sino también para actualizar los conocimientos, habilidades y competencias de todo el personal del proyecto, los profesores y los estudiantes implicados.

Queremos expresar nuestro especial agradecimiento a las 5 entidades que han revisado, evaluado y validado el plan de estudios modular propuesto por Cyber-In. Muchísimas gracias a Secure Network SRL (IT), Cybasque (ES), Rapla County Vocational College (Estonia), NTO Automation (DK) y OIXIO (Estonia).

Contáctanos

Teléfono

+ 31 088-6572657

Correo electrónico

rbezemer@davinci.nl

Sitio web

www.cyber-in.eu

Dirección

Leerparkpromenade 100
3312 KW Dordrecht Países Bajos