ANEXO III AL DECRETO XXX DE XXX DE 2021

CURSO DE ESPECIALIZACIÓN EN CIBERSEGURIDAD EN ENTORNOS DE LAS TECNOLOGÍAS DE OPERACIÓN

1. Identificación.

Denominación: Ciberseguridad en Entornos de las Tecnologías de Operación.
Nivel: Formación Profesional de Grado Superior.
Duración: 990 horas.
Familia Profesional: Electricidad y Electrónica (únicamente a efectos de clasificación de las enseñanzas de Formación Profesional).
Rama de conocimiento: Ingeniería y Arquitectura.
Créditos ECTS: 43.
Referente en la Clasificación Internacional Normalizada de la Educación: P-5.5.4.

2. Acceso al Curso de Especialización.

Estar en posesión de alguno de los títulos siguientes o su equivalente a efectos académicos:

- Título de Técnico Superior en Sistemas Electrotécnicos y Automatizados, establecido por el Decreto 222/2011, de 22 de octubre, por el que se establece el currículo correspondiente al título de Técnico Superior en Sistemas Electrotécnicos y Automatizados.
- Título de Técnico Superior en Mecatrónica Industrial, establecido por el Decreto 340/2013, de 22 de abril, por el que se establece el currículo correspondiente al título de Técnico Superior en Mecatrónica Industrial.
- Título de Técnico Superior en Automatización y Robótica Industrial, establecido por el Decreto 254/2012, de 27 de noviembre, por el que se establece el currículo correspondiente al título de Técnico Superior en Automatización y Robótica Industrial.
- Técnico Superior en Sistemas de Telecomunicaciones e Informáticos, establecido por el Decreto 118/2012, de 3 de julio, por el que se establece el currículo correspondiente al título de Técnico Superior en Sistemas de Telecomunicaciones e Informáticos.
- Título de Técnico Superior en Mantenimiento Electrónico, establecido por el Decreto 341/2013, de 22 de abril, por el que se establece el currículo correspondiente al título de Técnico Superior en Mantenimiento Electrónico.

3. Perfil profesional.

3.1. Competencia general:

La competencia general de este curso de especialización consiste en definir e implementar estrategias de seguridad en las organizaciones e infraestructuras industriales realizando diagnósticos de ciberseguridad, identificando vulnerabilidades e implementando las medidas necesarias para mitigarlas aplicando la normativa vigente y estándares del sector, siguiendo los protocolos de calidad, de prevención de riesgos laborales y respeto ambiental.

3.2. Entorno profesional:

Las personas que hayan obtenido el certificado que acredita la superación de este curso de especialización podrán ejercer su actividad en organizaciones de distintos sectores, donde sea necesario establecer y garantizar la seguridad de los procesos industriales que desarrollan.

Las ocupaciones y puestos de trabajo más relevantes son los siguientes:

- Experta o experto en ciberseguridad en entornos de la operación.
- Auditora o auditor de ciberseguridad en entornos de la operación.
- Consultora o consultor de ciberseguridad en entornos de la operación.
- Analista de ciberseguridad en entornos de la operación.

3.3. Competencias profesionales, personales y sociales:

a) Determinar perfiles de riesgo de las organizaciones identificando buenas prácticas, estándares y normativa aplicable.

b) Verificar alineación de los equipos y sistemas de las organizaciones en relación a los principios de la seguridad informática y de los riesgos de ciberseguridad.

c) Elaborar informes de ciberseguridad relativos a sistemas y entornos industriales a nivel técnico y organizativo, evaluando los elementos de seguridad desplegados.

d) Aplicar estrategias de ciberseguridad en las fases de los proyectos industriales para minimizar el impacto de cualquier posible incidente.

e) Caracterizar la evolución de los sistemas de control industrial valorando su impacto en la organización.

f) Establecer la configuración de sistemas de control industrial minimizando los riesgos de la organización.

g) Aplicar las metodologías reconocidas en el sector valorando los escenarios de riesgo tecnológico en redes industriales.

h) Identificar vulnerabilidades y establecer la configuración de dispositivos de redes minimizando los escenarios de riesgo.

i) Realizar análisis forenses en sistemas y redes industriales detectando vulnerabilidades en la organización.

j) Integrar las normas y procedimientos de seguridad física, operacional y de ciberseguridad en entornos de operación minimizando los riesgos.

k) Elaborar documentación técnica y administrativa de acuerdo con la legislación vigente y con los requerimientos del cliente.

l) Adaptarse a las nuevas situaciones laborales, manteniendo actualizados los conocimientos científicos, técnicos y tecnológicos relativos a su entorno profesional, gestionando su formación y los recursos existentes en el aprendizaje a lo largo de la vida.

m) Resolver situaciones, problemas o contingencias con iniciativa y autonomía en el ámbito de su competencia, con creatividad, innovación y espíritu de mejora en el trabajo personal y en el de las personas integrantes del equipo.

n) Generar entornos seguros en el desarrollo de su trabajo y el de su equipo, supervisando y aplicando los procedimientos de prevención de riesgos laborales y ambientales, de acuerdo con lo establecido por la normativa y los objetivos de la organización.

ñ) Supervisar y aplicar procedimientos de gestión de calidad, de accesibilidad universal y de «diseño para todas las personas», en las actividades profesionales incluidas en los procesos de producción o prestación de servicios.

4. Enseñanzas del Curso de Especialización

4.1. Objetivos generales:

a) Analizar buenas prácticas, estándares de aplicación y normativa para definir perfiles de riesgo.

b) Definir e incorporar requisitos de ciberseguridad en todas las fases de un proyecto industrial para evitar posibles incidentes.

c) Identificar y analizar las tecnologías avanzadas de aplicación en entornos OT para verificar la alineación con los principios de seguridad informática y los riesgos de ciberseguridad.

d) Analizar la convergencia de las prácticas profesionales en los entornos OT e IT y las exigencias que supone para aplicar estrategias de ciberseguridad y caracterizar la evolución de los sistemas de control industrial.

e) Definir y parametrizar sistemas de control industrial conforme a requisitos establecidos y controles de auditoría para establecer la configuración de los mismos.

f) Identificar y caracterizar equipos y configuraciones de redes industriales para realizar listados de posibles vulnerabilidades.

g) Evaluar niveles de riesgo asociados a las redes de instalaciones industriales para identificar vulnerabilidades.

h) Seleccionar y emplear diferentes herramientas para realizar análisis forenses.

i) Definir y aplicar configuraciones en redes industriales minimizando riesgos para integrar los requerimientos de seguridad.

j) Aplicar metodologías de análisis forense en sistemas SCADA, DCS, PLC, robótica industrial, dispositivos IoT y redes industriales para integrar procedimientos de seguridad.

k) Realizar informes para la presentación de resultados y conclusiones de análisis forense para elaborar documentación técnica y administrativa.

l) Determinar la normativa y los procedimientos aplicables a la seguridad física, a la seguridad operacional y a la ciberseguridad para integrar normas y procedimientos de seguridad.

m) Definir y aplicar metodologías para la gestión integral de riesgos de seguridad en entornos de la

operación.

n) Desarrollar manuales de información para los destinatarios, utilizando las herramientas ofimáticas y de diseño asistido por ordenador para elaborar la documentación técnica y administrativa.

ñ) Desarrollar la creatividad y el espíritu de innovación para responder a los retos que se presentan en los procesos y en la organización del trabajo y de la vida personal.

o) Analizar y utilizar los recursos y oportunidades de aprendizaje relacionados con la evolución científica, tecnológica y organizativa del sector y las tecnologías de la información y la comunicación, para mantener el espíritu de actualización y adaptarse a nuevas situaciones laborales y personales.

p) Evaluar situaciones de prevención de riesgos laborales y de protección ambiental, proponiendo y aplicando medidas de prevención personales y colectivas, de acuerdo con la normativa aplicable en los procesos de trabajo, para garantizar entornos seguros.

q) Identificar y proponer las acciones profesionales necesarias, para dar respuesta a la accesibilidad universal y al «diseño para todas las personas».

r) Identificar y aplicar parámetros de calidad en los trabajos y actividades realizados en el proceso de aprendizaje, para valorar la cultura de la evaluación y de la calidad y ser capaces de supervisar y mejorar procedimientos de gestión de calidad.

4.2. Módulos profesionales.

CÓDIGO	MÓDULO PROFESIONAL	ASIGNACIÓN HORARIA
5027	Ciberseguridad en proyectos industriales.	120
5028	Sistemas de control industrial seguros.	144
5029	Redes de comunicaciones industriales seguras.	168
5030	Análisis forense en ciberseguridad industrial.	192
5031	Seguridad integral.	96
E304	Formación Práctica Dual en Empresa	270
TOTAL		990

4.3. Módulos profesionales: Resultados de Aprendizaje, Criterios de Evaluación y Contenidos.

Módulo Profesional 1: Ciberseguridad en proyectos industriales.

Código: 5027.
Duración: 120 horas.
Créditos ECTS: 6.

Resultados de aprendizaje, criterios de evaluación y contenidos.

RA1. Determina los elementos de ciberseguridad a incluir en el diseño de un proyecto industrial analizando la seguridad ya implantada en la organización.

Criterios de evaluación:

a) Se ha evaluado el diseño del proyecto industrial: alcance, estudios de viabilidad financiera y requisitos técnicos, organizativos y procedimentales.
b) Se han identificado los actores y responsables involucrados en el proyecto, así como sus funciones y competencias en materia de ciberseguridad.
c) Se han caracterizado las amenazas e identificado las vulnerabilidades de los componentes de las tecnologías de automatización del proyecto.
d) Se han desarrollado los estudios que contemplen la ciberseguridad desde los diferentes actores involucrados (cliente, ingeniería y fabricantes).
e) Se han definido requisitos de ciberseguridad para los niveles de automatización del proyecto, así como sus flujos e interacciones.

Contenidos: Actividades de ciberseguridad en el diseño de un proyecto industrial.

- Diseño conceptual del proyecto. Ciclo de vida del proyecto y organización – Basado en PMBOK.
- Diseño preliminar del proyecto-estudio de viabilidad.
- Ingeniería básica o plan detallado del proyecto.
- Ingeniería de detalle o definición de las tecnologías a utilizar por cada nivel de automatización y su interacción entre ellas.
- Actividades de ciberseguridad en la fase de diseño.

RA2. Establece planes de gestión de compras determinando los requisitos de ciberseguridad a cumplir por los proveedores.

Criterios de evaluación:

a) Se ha establecido el proceso de gestión de compras a los proveedores.
b) Se han implementado los documentos básicos del proceso de gestión de compras.
c) Se han evaluado los requisitos de ciberseguridad para proveedores.
d) Se ha realizado el análisis y gestión de los riesgos asociados a la cadena de suministro.

e) Se han establecido los requisitos de ciberseguridad en el proceso de gestión de compras.

f) Se ha evaluado el cumplimiento de los requisitos de ciberseguridad establecidos en el aprovisionamiento.

Contenidos: Requisitos de ciberseguridad en el proceso de gestión de compras.

− Establecimiento del proceso de gestión de compras y elaboración de los documentos básicos del mismo.

- Evaluación de los requisitos de ciberseguridad para proveedores. “Herramienta de evaluación de requisitos de ciberseguridad para proveedores de servicios”.

− Análisis y gestión de riesgos en la cadena de suministro.

− Implementación de las medidas de ciberseguridad «extremo a extremo».

RA3. Establece las medidas de ciberseguridad en la ejecución y puesta en marcha de un proyecto industrial cumpliendo con los requisitos de calidad exigidos.

Criterios de evaluación:

a) Se ha realizado un análisis de funciones y responsabilidades de ciberseguridad en la ejecución y puesta en marcha del proyecto.

b) Se ha realizado un análisis preliminar de impacto para identificar medidas de ciberseguridad.

c) Se ha establecido el plan detallado de medidas de ciberseguridad.

d) Se ha establecido el marco metodológico de la evaluación de la seguridad.

e) Se han tenido en cuenta los principios de economía circular.

f) Se han incorporado criterios de ciberseguridad en las pruebas de aceptación en fábrica (FAT).

g) Se han incorporado criterios de seguridad en las pruebas de aceptación.

h) Se han establecido los planes de control de calidad y las auditorías.

i) Se ha contemplado la evaluación de ciberseguridad.

Contenidos: Medidas de ciberseguridad en la ejecución y puesta en marcha del proyecto industrial.

− Construcción del proyecto.

− Principios de la economía circular en la industria 4.0.

− Incorporación de las actividades de soporte a la construcción.

− Ejecución del plan detallado de seguridad física y lógica.

− Método de evaluación de la seguridad.

− Actualización de la documentación de ingeniería.

− Pruebas de aceptación en fábrica.

− Mediciones en las instalaciones.

− Ejecutar los planes de control de calidad y las auditorías.

RA4. Implementa las actividades de ciberseguridad de la fase de operación y mantenimiento de un proyecto industrial documentando las actividades realizadas.

Criterios de evaluación:

a) Se han identificado mejoras de ciberseguridad sobre la instalación.
b) Se han implementado mejoras de ciberseguridad sobre la instalación.
c) Se ha implantado un proceso de gestión de cambio para introducir las mejoras operacionales que puedan afectar a la gestión de la ciberseguridad.
d) Se han implementado actividades de ciberseguridad correspondientes a la fase de operación.
e) Se han implementado actividades de ciberseguridad correspondientes a la fase de mantenimiento.
f) Se han documentado los procedimientos de ciberseguridad para las fases de operación y mantenimiento de un proyecto industrial.
g) Se han implementado planes de concienciación y formación de ciberseguridad.

Contenidos: Actividades de ciberseguridad en la fase de operación y mantenimiento de un proyecto industrial.

- Período de optimización y seguimiento inicial de la operación.
- Proceso de gestión de cambio.
- Actividades de seguridad correspondientes a la fase de operación y mantenimiento.
  - Actividades de seguridad correspondientes a la fase de operación: control y gestión de hardware, software, redes, accesos, gestión de vulnerabilidades y monitorización de vectores de ataque.
  - Actividades de seguridad correspondiente a la fase de mantenimiento: copias de seguridad y restauración, monitorización y gestión de incidentes, planes de contingencia.
- Documentación de la fase de operación y mantenimiento.
- Plan de concienciación y formación.

RA5. Implementa las actividades de ciberseguridad en el desmantelamiento de las instalaciones cumpliendo con los requisitos establecidos en destrucción y/o conservación de los sistemas de una manera segura.

Criterios de evaluación:

a) Se han definido las actividades de ciberseguridad en el desmontaje, descontaminación, desclasificación, demolición y reposición de las instalaciones del proyecto.
b) Se han implementado las medidas de destrucción de los sistemas.
c) Se han verificado las medidas de destrucción de los sistemas.
d) Se han implementado las medidas de conservación de los sistemas.
e) Se han verificado las medidas de conservación de los sistemas.
f) Se han documentado las incidencias detectadas en el proceso de implementación y verificación.
g) Se han documentado las medidas implementadas en el proceso de conservación.

Contenidos: Actividades de ciberseguridad en el desmantelamiento de las instalaciones.

- Actividades de desmontaje, descontaminación, desclasificación, demolición y reposición.
- Gestión de la destrucción de los sistemas desde el punto de vista de la ciberseguridad.
- Gestión de la conservación desde el punto de vista de la ciberseguridad.

Módulo Profesional 2: Sistemas de control industrial seguros.

Código: 5028.
Duración: 144 horas.
Créditos ECTS: 7.

Resultados de aprendizaje, criterios de evaluación y contenidos.

RA1: Determina los cambios para la convergencia de las tecnologías *IT* (Tecnologías de la información) y *OT* (Tecnologías de la operación) analizando la situación de dichos entornos en organizaciones.

Criterios de evaluación:

a) Se han caracterizado los procesos de transformación digital en la industria.
b) Se han analizado y diferenciado los conceptos de tecnologías de la información (IT), y las tecnologías de la operación (OT).
c) Se han detectado las necesidades tecnológicas en los entornos IT y OT.
d) Se han identificado tecnologías avanzadas de aplicación.
e) Se han identificado los retos que conlleva para los departamentos de IT y OT en lo relativo al trabajo con las tecnologías avanzadas.
f) Se ha realizado un análisis de convergencia a nivel de prácticas de trabajo, de organización y de compartición de datos con IT.
g) Se han determinado los cambios relevantes que exigirán una alta profesionalización, visión de futuro, liderazgo y eficiencia.

Contenidos: Cambios para la convergencia de las tecnologías *IT* y *OT*.

- Tecnologías de la operación (OT), detección y/o realización de cambios en los procesos físicos a través de la monitorización y el control de dispositivos.
- Tecnologías de la información (IT, equipos informáticos para tratar datos).
- Cambios relevantes en entornos IT y OT para favorecer la convergencia.

RA2: Reconoce los dispositivos programables que intervienen en el control de sistemas dinámicos, sistemas de control de movimiento, identificando los componentes que los forman, identificando su funcionalidad y determinando sus aplicaciones en entornos industriales automatizados.

Criterios de evaluación:

a) Se han reconocido aplicaciones automáticas para la lectura y el control de señales dinámicas e identificado la estructura del sistema de control programado.

b) Se han determinado las características técnicas de los dispositivos programables según la aplicación requerida.

c) Se han identificado aplicaciones industriales en las que se justifica el uso de robots y de sistemas de control de movimiento y se han determinado la tipología y las características de los robots y manipuladores industriales.

d) Se han relacionado las funciones que ofrece un sistema de supervisión y control con aplicaciones industriales de automatización.

e) Se ha realizado una puesta en marcha de todo el sistema automático, verificando el funcionamiento de los programas de control, adquisición y supervisión diseñados conforme a los requerimientos del sistema automático.

Contenidos: Dispositivos programables y sistemas de control industrial SCI.

- Estructura de los sistemas de control.
  - Pirámide de automatización.
  - Tecnologías de automatización.
  - Modelo Perdue:
    - Nivel 0: Tecnología de instrumentación.
    - Nivel1: Controladores y DCS.
    - Nivel 2: Scada, HMI.
    - Nivel 3: EMS.
    - Nivel4 ERP.
- Aplicaciones automáticas para la lectura y el control de señales dinámicas.
- Características técnicas de los dispositivos programables.
- Redes y protocolos industriales.
- Sistemas de control de movimiento, tipología y características de los robots industriales.
- Sistema de supervisión y control con aplicaciones industriales de automatización.
- Puesta en marcha de un sistema automático.
- Definición e identificación de los distintos términos y conceptos claves en ciberseguridad industrial. Infraestructuras críticas, estratégicas y servicios esenciales.

RA3. Evalúa escenarios de riesgo tecnológico en sistemas de control de instalaciones industriales aplicando metodologías reconocidas.

Criterios de evaluación:

a) Se ha definido una metodología de Análisis de Riesgos (AR).

b) Se han identificado los diferentes tipos de activos que componen una instalación industrial.

c) Se han caracterizado diferentes tipos de amenazas para los diferentes activos.

d) Se han localizado datos de interés sobre vulnerabilidades conocidas en sistemas de control

industrial.

e) Se han comparado diferentes herramientas de diagnóstico.

f) Se han identificado y evaluado la seguridad de credenciales y los medios de control de acceso.

g) Se ha evaluado el firmware y/o configuración de un dispositivo mediante procedimientos de ingeniería inversa.

h) Se han automatizado acciones de verificación de la configuración de dispositivos y sistemas.

i) Se ha creado un testbed gemelo de un sistema de control industrial significativo imitando su configuración.

j) Se ha elaborado y ordenado una lista de riesgos asociados a los sistemas de control de una instalación industrial.

Contenidos: Evaluación de escenarios de riesgo tecnológico.

- Tipos de sistemas de control industrial.
- Amenaza y tipos de amenaza.
- Evaluación del riesgo.
- Riesgos externos.
- Tipos de credenciales y sistemas de control de acceso.
- Búsqueda de información sobre vulnerabilidades conocidas en sistemas de control Industrial.
- Herramientas de diagnóstico.
- Creación de *testbeds* gemelos.

RA 4. Documenta los procesos de diagnósticos, análisis y otros relativos a sistemas de una instalación industrial con relación a la ciberseguridad, generando informes de distintos niveles de complejidad.

Criterios de evaluación:

a) Se han identificado los elementos de los informes dirigidos a personal técnico y directivo, estableciendo las diferencias.

b) Se ha elaborado un informe técnico de diagnóstico de ciberseguridad destinado a personal directivo.

c) Se ha elaborado un informe técnico de diagnóstico de ciberseguridad destinado a personal técnico de operación.

d) Se han identificado los instrumentos, herramientas y técnicas de comunicación del informe técnico de acuerdo al destinatario.

e) Se han desarrollado las formas de gestionar conflictos y reticencias a la hora de presentar informes de resultados.

f) Se han analizado los informes técnicos de diagnóstico para obtener propuestas de mejora.

Contenidos: Documentación de los procesos en ciberseguridad.

- Elaboración de informes técnicos.

− Adaptación del lenguaje al receptor del informe.
− Elaboración de informes técnicos de diagnóstico de ciberseguridad destinado a personal directivo y personal técnico de operación.
− Elaboración de informes de las arquitecturas de red, configuraciones de sistemas de control y monitorización.
− Elaboración de informes con las políticas de seguridad del SGCI.
− Análisis de los informes técnicos de diagnóstico para obtener propuestas de mejora.
− Análisis de los informes de las arquitecturas de red, configuraciones de sistemas de control y monitorización para obtener propuestas de mejora.
− Presentación de resultados.

RA 5. Diseña políticas de seguridad para sistemas de control industrial teniendo en cuenta los análisis realizados, estándares del sector y la normativa de aplicación.

Criterios de evaluación:

a) Se han identificado diferentes mecanismos de autenticación de personas, dispositivos y sistemas.
b) Se han identificado los procedimientos necesarios en cuanto al alta, mantenimiento y baja de credenciales de acceso.
c) Se han realizado procesos de gestión de usuarios de una instalación industrial siguiendo las políticas de una organización.
d) Se han elaborado y justificado políticas de seguridad física y control de acceso a las diferentes zonas de una instalación industrial.

Contenidos: Diseño de políticas de seguridad.

− Identificación de personas, dispositivos y sistemas.
− Gestión de roles, usuarios y permisos.
− Políticas de seguridad física y de control de acceso.

RA 6. Configura sistemas de control industrial minimizando los posibles escenarios de riesgo.

Criterios de evaluación:

a) Se han identificado los requisitos de seguridad para la actualización y el parcheado de los sistemas de control industrial.
b) Se han identificado los requisitos de seguridad para la gestión de antivirus de los sistemas de control industrial basados en PC's.
c) Se han identificado los requisitos de seguridad para las copias de seguridad de las configuraciones e información de los sistemas de control industrial.
d) Se han configurado y parametrizado los sistemas de control industrial de acuerdo a los requisitos de protección establecidos.
e) Se han configurado y parametrizado los sistemas de control industrial de acuerdo a los controles

de auditoría establecidos.

Contenidos: Configuración de sistemas de control industrial.

- Configuración de usuarios y/o direcciones IP habilitadas a controlar los sistemas.
- Envío de registros (Logs) a sistemas externos.
- Gestión de actualizaciones de los sistemas.
- Copias de seguridad de una configuración deseada y su custodia.

RA 7. Detecta anomalías en sistemas de control industrial utilizando herramientas de monitorización y procedimientos de análisis.

Criterios de evaluación:

a) Se han identificado y caracterizado herramientas de monitorización de eventos de seguridad.
b) Se han configurado las herramientas de monitorización para el descubrimiento automático de sistemas de control industrial conectados.
c) Se han definido las reglas de actuación sobre las herramientas de monitorización para establecer los eventos a monitorizar.
d) Se han identificado los principios fundamentales de comportamiento de un gestor de eventos de seguridad (SIEM, Security Information and Event Management).
e) Se han detectado comportamientos sospechosos.
f) Se han documentado las anomalías encontradas.

Contenidos: Detección de anomalías en sistemas de control industrial.

- Monitorización de sistemas de control industrial.
- Herramientas de monitorización de eventos de seguridad.
- Herramientas de descubrimiento automático de activos.
- Reglas de actuación e inspección basadas en firmas.

Módulo Profesional 3: Redes de comunicaciones industriales seguras.

Código: 5029
Duración: 168 horas
Créditos ECTS: 9

Resultados de aprendizaje, criterios de evaluación y contenidos.

RA1: Integra elementos y equipamiento en redes cableadas e inalámbricas evaluando su campo de aplicación.

Criterios de evaluación:

a) Se han identificado los estándares para redes cableadas e inalámbricas.
b) Se han identificado equipos y elementos de redes.
c) Se han distinguido las funciones de los diferentes equipos de redes.
d) Se ha utilizado el sistema de direccionamiento lógico IP para asignar direcciones de red y máscaras de subred.
e) Se han configurado adaptadores de red cableados e inalámbricos bajo distintos sistemas operativos.
f) Se han identificado diferentes servicios y aplicaciones de redes.

Contenidos: Elementos y equipamiento en redes cableadas e inalámbricas.

− Identificación de estándares y protocolos más utilizados en redes: TCP/IP, Ethernet, IEEE 802 y sus derivados, para evaluar el campo de aplicación en una comunicación entre equipos informáticos.
− Identificación de equipos y dispositivos de red, tales como: NIC's, Switches, Routers, Firewalls, servidores de red, entre otros, y su campo de aplicación.
− Sistema de direccionamiento IP.
− Identificación de servicios y aplicaciones de redes tales como: servicios de acceso remoto, servicios web http y https, servicios de autenticación, servicios de asignación de direcciones IP (DHCP), servicio DNS, y otros servicios.

RA2: Determina los niveles de seguridad en un entorno industrial automatizado analizando las características de los protocolos y comunicaciones utilizados y proponiendo soluciones a nuevos requerimientos de seguridad.

Criterios de evaluación:

a) Se han caracterizado dispositivos de control de diferentes fabricantes en un entorno de automatización industrial.
b) Se han descrito los diferentes elementos de supervisión y sistemas SCADA (Sistemas de Supervisión, Control y Adquisición de Datos).
c) Se han identificado los diferentes sistemas de optimización y gestión.
d) Se han especificado los niveles de seguridad en los diferentes campos de automatización industrial (campo, control, supervisión, optimización y gestión).
e) Se han establecido las diferencias entre el sistema analizado y el sistema futuro en términos de seguridad.
f) Se han documentado las propuestas de adaptación en términos de seguridad de acuerdo a los nuevos requerimientos.

Contenidos: Niveles de seguridad en un entorno industrial automatizado.

− Niveles de automatización industrial. Pirámide de automatización.
- Nivel de proceso (dispositivos físicos como sensores, actuadores...).
- Nivel de control (dispositivos lógicos como PC's, PLC's, DCS, UTR, PAC...).

- Nivel de supervisión (sistemas de supervisión y adquisición de datos como SCADA, HMI...).
- Nivel de planificación (sistemas de ejecución de la fabricación MES).
- Nivel de gestión (sistemas de gestión y planificación integral ERP).

− Dispositivos de control y supervisión disponibles en el mercado.

− Opciones de comunicaciones y protocolos industriales avanzados existentes en el mercado: Common Industrial Protocol (CIP), MODBUS, DNP3, Profibus, Profinet, Powerlink Ethernet, OPC, therCAT, entre otros.

− Comunicación OPC UA que permite comunicación de equipos y sistemas industriales para la recolección y control de datos.

− Estándar ISA99/IEC62443.

RA3: Evalúa escenarios de riesgo tecnológico en redes industriales aplicando metodologías reconocidas.

Criterios de evaluación:

a) Se han identificado los diferentes tipos de dispositivos que componen la red de una instalación industrial.

b) Se ha caracterizado la arquitectura de red física y lógica de una instalación industrial.

c) Se han identificado las diferentes zonas de seguridad que deberían existir en la red de una instalación industrial.

d) Se han clasificado los riesgos, asociados a la red de una instalación industrial.

e) Se ha evaluado el nivel de riesgo asociado a la red de una instalación industrial.

Contenidos: Evaluación de escenarios de riesgo tecnológico en redes industriales.

− Tipos de dispositivos de una red industrial.

− Arquitectura de red física y lógica.

− Tipo de elementos y equipos en una red industrial.

− Zonificación (red de control, de supervisión, corporativa, etc.).

− Evaluación del riesgo.

− Riesgos externos (riesgo de drones en entornos industriales, riesgo de sistemas de automatización (IoT) de los edificios industriales, riesgo de los dispositivos propiedad de las personas empleadas (BYOD), riesgo por dispositivos con servicio de geolocalización activada, etc.).

RA4: Implementa redes industriales aplicando técnicas de switching y de enrutamiento.

Criterios de evaluación:

a) Se ha caracterizado el switching en redes industriales.

b) Se han implementado topologías en Ethernet industrial.

c) Se han implementado topologías en anillo.

d) Se han implementado acoplamientos de segmentos entre anillos de forma redundante.

e) Se han interconectado redes OT a redes IT.

f) Se ha examinado el tráfico de red con los analizadores de red.
g) Se ha caracterizado el enrutamiento en las redes industriales.
h) Se han implementado conexiones simples con redes ofimáticas (OT e IT).
i) Se han implementado conexiones redundantes con redes ofimáticas.
j) Se han implementado conexiones a redes legacy.
k) Se han implementado conexiones a redes con detección automática de camino.
l) Se han implementado restricciones de enrutado por medio de ACL´s.
m) Se han configurado protocolos y dispositivos de autenticación en redes privadas virtuales (VPN).
n) Se han documentado las intervenciones.

Contenidos: Implementación de redes industriales aplicando técnicas de switching y de enrutamiento.

− Analizar las técnicas de switching en redes industriales.
− LAN, MAN, WAN, GAN.
− Topologías típicas en Ethernet Industrial, representando las distintas zonas lógicas de red, las interconexiones entre ellas y los sistemas que contienen.
− Topologías en anillo con HRP Hihg-Speep Redundancy Protocol.
− Acoplamientos de segmentos entre anillos de forma redundante.
− RSTP (Rapid Spanning Tree Protocol).
− Conexiones redundantes entre RSTP y anillos.
- Acoplamiento entre segmentos de automatización y redes IT.

− Topologías con PRP (Parallel Redundancy Protocol) y HSR (High-Availability Seamless Redundancy Protocol).
− Enrutamiento en redes industriales.
− Conexiones simples con redes ofimáticas (OT e IT).
− Las tablas de enrutamiento.
− Uso de AAA y 802.1x para autenticar los terminales y los puntos terminales LAN y dispositivos.
− Conexiones redundantes con redes ofimáticas mediante VRRP (Virtual Router Redundancy Protocol).
− Conexiones a redes legacy mediante RIP (Routing Information Protocol).
− Pruebas de latencia con comandos como ping y traceroute.

RA5: Implementa redes industriales inalámbricas aplicando los estándares del sector.

Criterios de evaluación:

a) Se han caracterizado las tecnologías inalámbricas.
b) Se han implementado métodos de acceso y organización de las células.
c) Se ha implementado roaming.
d) Se ha identificado la localización de los puntos de acceso.
e) Se han seleccionado las antenas.

f) Se han diseñado redes Wifi para instalaciones industriales.
g) Se han implementado redes Wifi para instalaciones industriales.

Contenidos: Implementación de redes industriales inalámbricas.

− Tecnologías de Wireless (WIMAX, IWLAN, Bluetooth, WirelessHart).
− Estándar WLAN.
− Métodos de acceso y organización de las células.
− Roaming.
− Seguridad (TKIP y WPA2) y tasas de transmisión. Técnicas de autenticación.
− Encriptación.
− WDS (Wireless Distribution System).
− Diferencia entre PCF (Point Coordinated Function) versus DCF (Distributed Coordination Function).
− Comunicaciones Wifi en tiempo real – determinismo en Wifi (iPCF).
− Tablas ARP.
− Sistemas de administración para detectar dispositivos inalámbricos falsos.
− Sistemas RADIUS y otros sistemas de control de accesos.

RA6: Implementa accesos remotos en entornos industriales garantizando la seguridad de las comunicaciones.

Criterios de evaluación:

a) Se han caracterizado las comunicaciones remotas más utilizadas.
b) Se han implementado comunicaciones seguras a través de comunicaciones no seguras.
c) Se han conectado redes privadas industriales a redes públicas aplicando diferentes tecnologías.
d) Se han implementado accesos remotos basándose en el principio de mínima superficie.
e) Se han identificado y caracterizados los servicios cloud más utilizados, como IAAS, PAAS, SAAS y otros.
f) Se ha comprobado la integridad de las comunicaciones.

Contenidos: Implementación de accesos remotos seguros en entornos industriales.

− Comunicaciones remotas (LAN, WAN, MAN y GAN).
− Comunicaciones seguras vía redes no seguras (VPN).
− IPsec VPN y OpenVPN.
− Interconexión de redes privadas industriales a redes públicas: NAT (Network Address Translation).
− Principio de mínima superficie de ataque a la hora de implementar accesos remotos.
− Sistema de Inspección de paquetes con estado, visibilidad y control de aplicaciones.
− Filtrado de URL.
− Aplicaciones de acceso remoto como telnet, SSH, HTTPS y otros.

RA7: Diseña la red de automatización aplicando la segmentación necesaria en las redes de la organización.

Criterios de evaluación:

a) Se ha implementado la segmentación en redes de automatización.
b) Se han implementado VLAN´s para la estructuración de las redes.
c) Se han asignado equipos en VLAN´s estáticas y dinámicas.
d) Se han priorizado VLAN´s.
e) Se han realizado segmentaciones de células de automatización mediante cortafuegos industriales.
f) Se han realizado segmentaciones entre IT y OT mediante NGF (Next Generation Firewall).

Contenidos: Diseño de la red de automatización mediante segmentación.

− Segmentación en las redes de automatización.
− Segmentación en zonas: mínimo en 3 zonas para separar Red Control, DMZ y LAN corporativa. Zonas que pueden ser trusted o untrusted (de confianza o no).
− Estructuración de redes con VLAN's: estáticas y dinámicas.
− Cifrado de la comunicación y separación lógica entre segmentos de red, mediante el uso de tecnologías de VLAN y VPN.
− Segmentación de célula con cortafuegos industriales.
− Segmentación entre entornos IT y OT con NGF (Next Generation Firewall).
− Segmentación ISA 99-IEC 62443.

RA8: Identifica vulnerabilidades, amenazas y ataques en dispositivos de redes industriales proponiendo contramedidas.

Criterios de evaluación:

a) Se han identificado vulnerabilidades, amenazas y ataques conocidas en dispositivos y redes industriales.
b) Se ha valorado el alcance de las vulnerabilidades, amenazas y ataques.
c) Se han caracterizado diferentes herramientas de diagnóstico.
d) Se han relacionado las herramientas de diagnóstico con su aplicación a las diversas situaciones.
e) Se han automatizado acciones de verificación de la configuración de dispositivos y redes.
f) Se ha creado un testbed gemelo de un segmento significativo de una red industrial imitando la configuración tanto de los dispositivos como de la red.
g) Se han realizado tests de penetración exhaustivos en un testbed gemelo de una instalación industrial.

Contenidos: Identificación de vulnerabilidades y ataques en dispositivos de redes industriales.

− Búsqueda de información sobre vulnerabilidades conocidas en dispositivos de redes industriales.
− Herramientas de diagnóstico.
− Creación de testbeds gemelos.
− Tests de penetración no intrusivos que garantizan la continuidad del proceso productivo.
− Ataques a las tablas MAC y ataques de suplantación de direcciones.
− Ataques DoS.

RA9. Detecta incidentes en tiempo real en redes industriales aplicando procedimientos de análisis y utilizando las herramientas adecuadas.

Criterios de evaluación:

a) Se han caracterizado diferentes herramientas de análisis de tráfico en entornos industriales.
b) Se han seleccionado las herramientas en función de sus prestaciones.
c) Se ha diseñado, configurado e implementado un sistema de detección de intrusiones (IDS, Intrusion Detection System) para sistemas de control industrial.
d) Se han detectado e investigado comportamientos sospechosos en una infraestructura mediante el análisis del tráfico de red.
e) Se han documentado los comportamientos anómalos observados.

Contenidos: Detección de incidentes en tiempo real en redes industriales.

− Análisis de tráfico.
− Sistemas de detección de intrusiones (IDS, IPS).
− Sistemas de detección basados en los comportamientos de protocolos industriales.

RA10: Define procedimientos de verificación y supervisión obteniendo métricas de cumplimiento de las políticas de seguridad.

Criterios de evaluación:

a) Se han identificado métricas de cumplimiento de políticas de seguridad.
b) Se han analizado diferentes registros de sistemas de control industrial para detectar cambios no autorizados en las políticas de seguridad.
c) Se han caracterizado diferentes herramientas de monitorización de redes de automatización industrial.
d) Se han instalado herramientas de monitorización de red.
g) Se han documentado los resultados de la monitorización.

Contenidos: Definición de procedimientos de verificación y supervisión.

− Métricas de cumplimiento de políticas.
− Gestión de registros (Logs).
− Monitorización de los switches y otros dispositivos de las redes.
− Sistemas de monitorización de red (SNMP, SSH, web, etc): manual, automático.
− Sistemas de registros de la información de la infraestructura y gestión del servicio, como por ejemplo CMDB y otros tipos de sistemas de registros de información.

RA11: Configura dispositivos de redes industriales minimizando los posibles escenarios de riesgo.

Criterios de evaluación:

a) Se han definido los parámetros de protección de los dispositivos.
b) Se han configurado dispositivos de red para poder ser auditados a posteriori.
c) Se han identificado los requisitos de seguridad para las actualizaciones del firmware de los dispositivos de red.
d) Se han identificado los requisitos de seguridad para las copias de seguridad de las configuraciones de los dispositivos de red.
e) Se han configurado los dispositivos de red acorde a los parámetros de protección definidos.

Contenidos: Configuración de dispositivos de redes industriales.

− Configuración de usuarios y/o direcciones IP habilitadas a controlar los dispositivos.
− Configuración de firewalls y registros de eventos (logs).
− Gestión de actualizaciones del firmware de los dispositivos.
− Copias de seguridad de una configuración deseada y su custodia.

Módulo Profesional 4: Análisis forense en ciberseguridad industrial.

Código: 5030.
Duración: 192 horas
Créditos ECTS: 11.

Resultados de aprendizaje, criterios de evaluación y contenidos.

RA1. Aplica metodologías de análisis forense caracterizando las fases de preservación, adquisición, análisis y documentación.

Criterios de evaluación:

a) Se han identificado los dispositivos a analizar para garantizar la preservación de evidencias.
b) Se han utilizado los mecanismos y las herramientas adecuadas para la adquisición y extracción de las evidencias.
c) Se ha asegurado la escena y conservado la cadena de custodia.

d) Se ha documentado el proceso realizado de manera metódica.
e) Se ha considerado la línea temporal de las evidencias.
f) Se ha elaborado un informe de conclusiones a nivel técnico y ejecutivo.
g) Se han presentado y expuesto las conclusiones del análisis forense realizado.

Contenidos: Aplicación de metodologías de análisis forenses.

− Identificación de los dispositivos a analizar.
− Requisitos de investigación forense: aceptabilidad, integridad, credibilidad, relación causa-efecto, repetible y documentada.
− Etapas del análisis forense.
− Consideraciones previas a la adquisición.
− Orden de volatilidad.
− Recolección de evidencias (trabajar un escenario).
− Análisis de la línea de tiempo (TimeStamp).
− Análisis de volatilidad.
– Extracción de información (Volatility).
− Análisis de Logs, herramientas más usadas.

RA2. Desarrolla procesos de análisis forense en sistemas de control industrial aplicando metodologías reconocidas.

Criterios de evaluación:

a) Se han identificado los dispositivos a analizar para garantizar la preservación de evidencias.
b) Se han utilizado mecanismos y herramientas adecuadas para la adquisición y extracción de las evidencias.
c) Se han realizado análisis de las evidencias de manera manual.
d) Se han realizado análisis de las evidencias mediante herramientas automáticas para dar respuesta a la investigación forense.
e) Se ha documentado el proceso de análisis realizado de manera metódica y detallada para garantizar la reproducción de todos los pasos.
f) Se ha considerado la línea temporal de las evidencias, el mantenimiento de la cadena de custodia y la elaboración de conclusiones a nivel técnico y ejecutivo.
g) Se han comunicado las conclusiones del análisis forense realizado a los interlocutores pertinentes.

Contenidos: Proceso de análisis forense en sistemas de control industrial.

− Principio de Locard.
− Tipos de análisis forenses.
− Cadena de custodia.

− Funciones Hash.
− Sistemas de ocultación.
− Volcado de memoria.
− Extracción de evidencias volátiles, no volátiles y en tránsito.
− Análisis de evidencias volátiles, no volátiles y en tránsito con herramientas manuales.
− Análisis de evidencias volátiles, no volátiles y en tránsito con herramientas automatizadas.
− Borrado seguro de soportes.

RA3. Desarrolla el proceso de análisis forense en sistemas de control y controladores lógicos programables aplicando metodologías reconocidas.

Criterios de evaluación:

a) Se han identificado los sistemas de control de supervisión y adquisición de datos (SCADA), sistemas de control distribuido (DCS), y controladores lógicos programables (PLC) a analizar para garantizar la preservación de las evidencias.
b) Se han empleado mecanismos y herramientas adecuadas para la adquisición y extracción de evidencias que garanticen su autenticidad, completitud, fiabilidad y legalidad.
c) Se han analizado las evidencias de manera manual y mediante herramientas automáticas para dar respuesta a investigaciones forenses.
d) Se ha documentado el proceso de análisis realizado para garantizar la reproducción de todos los pasos.
e) Se ha considerado la línea temporal de las evidencias, el mantenimiento de la cadena de custodia y la elaboración de conclusiones a nivel técnico y ejecutivo.
f) Se han comunicado formalmente las conclusiones del análisis forense realizado a los interlocutores pertinentes.

Contenidos: Proceso de análisis forense en sistemas de control y controladores lógicos programables.

− Funciones Hash en sistemas.
− Sistemas de ocultación en sistemas.
− Extracción de evidencias volátiles, no volátiles y en tránsito en sistemas.
− Análisis de evidencias volátiles, no volátiles y en tránsito con herramientas manuales en sistemas.
− Análisis de evidencias volátiles, no volátiles y en tránsito con herramientas automatizadas en sistemas.
− Borrado seguro de sistemas.

RA4. Desarrolla el proceso de análisis forense en robótica industrial aplicando metodologías reconocidas.

Criterios de evaluación:

a) Se han identificado los dispositivos industriales a analizar para garantizar la preservación de las evidencias.

b) Se han utilizado los mecanismos y las herramientas necesarias para la adquisición y extracción de evidencias adecuadas que garantizan su autenticidad, completitud, fiabilidad y legalidad.

c) Se han realizado análisis de evidencias de manera manual y mediante herramientas automáticas para dar respuesta a investigaciones forenses.

d) Se ha documentado el proceso de análisis realizado de manera metódica y detallada para garantizar la reproducción de todos los pasos.

e) Se ha considerado la línea temporal de las evidencias, el mantenimiento de la cadena de custodia y la elaboración de conclusiones a nivel técnico y ejecutivo.

f) Se han comunicado formalmente las conclusiones del análisis forense realizado a los interlocutores pertinentes.

Contenidos: Desarrollo del proceso de análisis forense en robótica industrial.

− Funciones Hash en dispositivos industriales.
− Sistemas de ocultación en dispositivos industriales.
− Extracción de evidencias volátiles, no volátiles y en tránsito en dispositivos industriales.
− Análisis de evidencias volátiles, no volátiles y en tránsito con herramientas manuales en dispositivos industriales.
− Análisis de evidencias volátiles, no volátiles y en tránsito con herramientas automatizadas en dispositivos industriales.
− Borrado seguro en dispositivos industriales.

RA5. Desarrolla el proceso de análisis forense en dispositivos del Internet de las cosas (IoT), de sectores industriales y otros como los de transporte, salud, construcción etc, aplicando metodologías reconocidas.

Criterios de evaluación:

a) Se han identificado los dispositivos a analizar para garantizar la preservación de las evidencias.

b) Se han utilizado los mecanismos y las herramientas necesarias para la adquisición y extracción de evidencias adecuadas que garanticen su autenticidad, completitud, fiabilidad y legalidad.

c) Se han realizado análisis de evidencias de manera manual y mediante herramientas automáticas para permitir dar respuesta a investigaciones forenses.

d) Se ha documentado el proceso de análisis para garantizar la reproducción de todos los pasos.

e) Se ha considerado la línea temporal de las evidencias, el mantenimiento de la cadena de custodia y la elaboración de conclusiones a nivel técnico y ejecutivo.

f) Se han comunicado formalmente las conclusiones del análisis forense realizado a los interlocutores pertinentes.

Contenidos: Proceso de análisis forense en dispositivos del Internet de las cosas (IoT), de sectores industriales y otros.

− Funciones Hash en dispositivos.
− Sistemas de ocultación de dispositivos.
− Extracción de evidencias volátiles, no volátiles y en tránsito en dispositivos.
− Análisis de evidencias volátiles, no volátiles y en tránsito con herramientas manuales en dispositivos.
− Análisis de evidencias volátiles, no volátiles y en tránsito con herramientas automatizadas en dispositivos.
− Borrado seguro en dispositivos.

RA6. Responde ante un incidente de ciberseguridad que afecta a la organización tomando las medidas necesarias.

Criterios de evaluación:

a) Se han desarrollado procedimientos de actuación para dar respuesta, mitigar, eliminar o contener los tipos de incidentes de ciberseguridad más habituales en sistemas de control industrial.
b) Se han preparado respuestas ciberresilientes para intervenir inmediatamente ante incidentes de ciberseguridad que permitan seguir prestando los servicios de la organización.
c) Se ha establecido un flujo de toma de decisiones y escalado interno y/o externo adecuados al incidente.
d) Se han llevado a cabo las tareas de restablecimiento de los servicios afectados por el incidente, hasta confirmar la vuelta a la normalidad.
e) Se han documentado las acciones realizadas incluyendo las conclusiones que permitan mantener un registro de lecciones aprendidas.
f) Se ha notificado el incidente formalmente a todos los involucrados o afectados: clientes, proveedores, personal interno, medios de comunicación y autoridades competentes, en los tiempos adecuados.
g) Se ha realizado un seguimiento adecuado del incidente para evitar que una situación similar se vuelva a repetir.

Contenidos: Respuesta ante un incidente de ciberseguridad.

− Desarrollo de procedimientos de actuación detallados para dar respuesta, mitigar, eliminar o contener los tipos de incidentes.
− Implantación de capacidades de ciberresiliencia.
− Tareas de restablecimiento de los servicios afectados por incidentes.
− Documentación y lecciones aprendidas.
− Notificación del incidente.
− Seguimiento del incidente.

Módulo Profesional 5: Seguridad integral.

Código: 5031.
Duración: 96 horas.
Créditos ECTS: 10.

Resultados de aprendizaje y criterios de evaluación.

RA1: Integra las normas y procedimientos de seguridad física en la ciberseguridad en entornos OT identificando los posibles riesgos.

Criterios de evaluación:

a) Se ha caracterizado el riesgo físico y la seguridad física.
b) Se han descrito los fundamentos y herramientas básicas de un esquema de seguridad física.
c) Se han definido los conceptos básicos de normas de seguridad física para entornos OT.
d) Se han caracterizado las normas de seguridad física aplicables en función de la actividad que hay que desarrollar.
e) Se han determinado los procedimientos de seguridad física en entornos OT que son de aplicación conforme a las normas aplicables.
f) Se han implementado los procedimientos de seguridad física determinados.
g) Se ha comprobado que la integración de las normas y procedimientos de seguridad física cumplen con los requisitos de ciberseguridad.

Contenidos: Normas y procedimientos de seguridad física en la ciberseguridad en entornos OT.

− Riesgos de seguridad física en un entorno OT.
− Normas de seguridad física aplicables a un entorno OT.
− Integración de la seguridad física en la seguridad OT.

RA2: Integra las normas y procedimientos de seguridad operacional en la ciberseguridad en entornos OT identificando los posibles riesgos.

Criterios de evaluación:

a) Se han caracterizado el riesgo operacional y la seguridad operacional.
b) Se han descrito los fundamentos y herramientas básicas de un esquema de seguridad operacional.
c) Se han definido los conceptos básicos de normas de seguridad operacional.
d) Se han caracterizado las normas de seguridad operacional aplicables en función de la actividad que hay que desarrollar.
e) Se han determinado los procedimientos de seguridad operacional que son de aplicación al entorno conforme a las normas aplicables.
f) Se han implementado los procedimientos de seguridad operacional determinados.
g) Se ha comprobado que la integración de las normas y procedimientos de seguridad operacional cumplen con los requisitos de ciberseguridad.

Contenidos: Normas y procedimientos de seguridad operacional en la ciberseguridad en entornos OT.

− Riesgos de seguridad operacional con un entorno OT.
− Entornos OT.
− Integración de la seguridad operacional en la seguridad OT.

RA3: Integra las normas y procedimientos de calidad en la ciberseguridad en entornos OT identificando los posibles riesgos.

Criterios de evaluación:

a) Se ha definido el concepto de riesgo y pérdida que afecta a la calidad.
b) Se han descrito los fundamentos y herramientas básicas de un esquema de calidad.
c) Se han definido los conceptos básicos relativos a normas de calidad.
d) Se han caracterizado las normas de calidad aplicables en función de la actividad que hay que desarrollar.
e) Se han determinado los procedimientos de calidad que son de aplicación al entorno conforme a las normas aplicables.
f) Se han implementado los procedimientos de calidad determinados.
g) Se ha comprobado que la integración de las normas y procedimientos de calidad cumplen con los requisitos de ciberseguridad.

Contenidos: Normas y procedimientos de calidad en la ciberseguridad en entornos OT.

− Riesgos que afecten a la calidad en un entorno OT.
− Normas de calidad aplicables a un entorno OT.
− Integración de la calidad en la ciberseguridad OT.

RA4: Aplica medidas de ciberseguridad en los sistemas instrumentados de seguridad (SIS) ajustándose a las normas aplicables.

Criterios de evaluación:

a) Se han caracterizado los tipos de fallos y de sistemas instrumentados de seguridad.
b) Se ha discriminado entre las diferentes plataformas de tecnologías SIS, seleccionando aquellas que se adecúen a la realidad industrial de la organización.
c) Se han seleccionado las normas aplicables en función de la actividad que hay que desarrollar (IEC 61508 o las que eventualmente la sustituyan).
d) Se han determinado los niveles de integridad de seguridad de aplicación al entorno conforme a

la norma aplicable (IEC 61508 o las que eventualmente la sustituyan).

e) Se han determinado las técnicas y medidas de seguridad de los SIS.

f) Se ha comprobado que los SIS cumplen con los requisitos de ciberseguridad.

Contenidos: Medidas de ciberseguridad en los sistemas instrumentados de seguridad (SIS).

− Tipologías de fallos y sistemas instrumentados de seguridad.
− Plataformas de tecnologías disponibles para implementar un sistema instrumentado seguro (SIS) y sus requisitos.
− Normativa aplicable (IEC 61508 o las que eventualmente la sustituyan).
− Métodos para determinar los niveles de integridad de seguridad (SIL).
− Técnicas y medidas de seguridad en los SIS.
− Requisitos de ciberseguridad en los sistemas instrumentados de seguridad.

RA5: Gestiona de forma integral los riesgos de seguridad aplicando metodologías reconocidas.

Criterios de evaluación:

a) Se ha caracterizado la gestión integral de riesgos.

b) Se han descrito las normas, marcos y metodologías de la gestión integral de los riesgos de seguridad.

c) Se ha implementado un marco de gestión de riesgos de acuerdo con la normativa aplicable (ISO 31000 o las que eventualmente la sustituyan).

d) Se han identificado y evaluado el riesgo de acuerdo con la normativa aplicable (ISO 31000 o las que eventualmente la sustituyan).

e) Se ha tratado, aceptado y comunicado el riesgo según la normativa aplicable (ISO 31000 o las que eventualmente la sustituyan).

Contenidos: Gestión integral de los riesgos de seguridad.

− Marco de Gestión de Riesgos conforme a la normativa aplicable (ISO 31000 o las que eventualmente la sustituyan).
− Identificación, evaluación, tratamiento, aceptación y comunicación del riesgo y vigilancia según la normativa aplicable (ISO 31000 o las que eventualmente la sustituyan).
− Normativa de Ciberseguridad Industrial. Normativa NIST SP800-X, NERC-ZIP, IEC 62443, BSI-100 o las que eventualmente la sustituyan.

Módulo Profesional 6: Formación Práctica Dual en Empresa
Código: E304
Duración: 270 horas

Las actividades a realizar en la empresa se programarán con la finalidad de completar las competencias del Curso de Especialización y sus objetivos generales, tanto para aquellas que se han alcanzado en el centro educativo, como para aquellas que son difíciles de conseguir en el mismo. Las actividades diseñadas deberán incluir:

- La aplicación de estrategias de ciberseguridad en las distintas fases de proyectos industriales.
- La evaluación y elaboración de informes relativos a sistemas y entornos industriales.
- La configuración de los sistemas de control industrial.
- La detección de vulnerabilidades en redes industriales y la configuración de sus dispositivos.
- La colaboración en análisis forenses en sistemas y redes industriales.
- La incorporación de normas y procedimientos de seguridad integral en entornos de operación.

5. Espacios y equipamientos.

5.1. Espacios:

ESPACIO FORMATIVO	SUPERFICIE M2 / 30 ALUMNOS O ALUMNAS	SUPERFICIE M2 / 20 ALUMNOS O ALUMNAS
Aula polivalente.	60	40
Aula de informática.	120	80
Laboratorio de sistemas automáticos.	180	120
Taller de sistemas automáticos.	200	130

5.2. Equipamientos:

ESPACIO FORMATIVO	EQUIPAMIENTO
Aula polivalente.	Sistema de proyección. Ordenadores en red y con acceso a Internet. Dispositivos de almacenamiento en red. Escáner. Sistemas de reprografía. Equipos audiovisuales
Aula de informática.	Sistema de proyección. Ordenadores en red y con acceso a Internet. Escáner. Plotter. Programas de gestión de proyectos. Sistemas de reprografía. Equipos audiovisuales. Software de diseño y simulación de sistemas de automatización y robótica industrial. Software de desarrollo de sistemas de control de la operación SCADA.
Laboratorio de sistemas automáticos.	Sistema de proyección. Ordenadores en red y con acceso a Internet. Sistemas de reprografía. Software de aplicación.

	Elementos medidores y captadores, especialmente con tecnologías integradas de comunicaciones, tipo IoT. Elementos actuadores, especialmente con tecnologías integradas de comunicaciones, tipo IoT. Switchs. Pantallas táctiles. Pasarelas. Tarjetas para sistemas de comunicaciones inalámbricas. Tarjetas de comunicaciones para diferentes tipos de buses. Tarjetas de comunicaciones para telegestión y telemantenimiento. Routers. Firewall. Elementos de mando y maniobra. Elementos de protección. Transformadores. Polímetros. Fuentes de alimentación. Frecuencímetros. Autómatas programables. Osciloscopios. Inyector de señales. Herramientas y máquinas portátiles de mecanizado para electricidad. Bancos de ensayos, control, regulación y acoplamiento de máquinas eléctricas estáticas y rotativas. Pinzas amperimétricas. Tacómetros. Diversos tipos de motores. Arrancadores progresivos. Elementos y entrenadores de comunicaciones industriales. Equipamientos y elementos de medición y control. Equipamiento para la realización de ensayos.
Taller de sistemas automáticos.	Sistema de proyección. Ordenadores en red y con acceso a Internet. Sistemas de reprografía. Equipos y herramientas de mecanizado manual. Equipamientos y elementos de medición y control. Equipamiento para la realización de mediciones y verificación de elementos. Mecanismos. Paneles modulares para el montaje de sistemas. Elementos para montaje y simulación de sistemas hidráulicos, neumáticos, electro-hidráulicos y electro-neumáticos. Herramientas portátiles para mecanizado. Simuladores de estaciones: distribución, verificación, procesamiento, robot y otros. Autómatas programables. Equipos de verificación y medida. Software de aplicación.

6. Profesorado.

6.1. Especialidades del profesorado con atribución docente en los módulos profesionales del Curso de Especialización de Ciberseguridad en entornos de las tecnologías de operación:

MÓDULO PROFESIONAL	ESPECIALIDAD DEL PROFESORADO	CUERPO
5027. Ciberseguridad en proyectos industriales.	Equipos Electrónicos. Instalaciones Electrotécnicas. Organización y Proyectos de Fabricación Mecánica.	Profesora o Profesor de Enseñanza Secundaria.
	Profesora o Profesor Especialista.	
5028. Sistemas de control industrial seguros.	Organización y Proyectos de Fabricación Mecánica. Sistemas Electrónicos. Sistemas Electrotécnicos y Automáticos.	Profesora o Profesor de Enseñanza Secundaria.
	Profesora o Profesor Especialista.	
5029. Redes de comunicaciones industriales seguras.	Equipos Electrónicos. Instalaciones Electrotécnicas.	Profesora Técnica o Profesor Técnico de Formación Profesional.
	Profesora o Profesor Especialista.	
5030. Análisis forense en ciberseguridad industrial.	Equipos Electrónicos. Instalaciones Electrotécnicas.	Profesora Técnica o Profesor Técnico de Formación Profesional.
	Profesora o Profesor Especialista.	
5031. Seguridad integral.	Organización y Proyectos de Fabricación Mecánica. Sistemas Electrónicos. Sistemas Electrotécnicos y Automáticos.	Profesora o Profesor de Enseñanza Secundaria.
	Profesora o Profesor Especialista.	
E304. Formación Práctica Dual en Empresa.	Organización y Proyectos de Fabricación Mecánica. Sistemas Electrónicos. Sistemas Electrotécnicos y Automáticos.	Profesora o Profesor de Enseñanza Secundaria.
	Equipos Electrónicos. Instalaciones Electrotécnicas.	Profesora Técnica o Profesor Técnico de Formación Profesional.

6.2. Titulaciones habilitantes a efectos de docencia:

CUERPO	ESPECIALIDAD	TITULACIONES
Profesora o Profesor de Enseñanza Secundaria.	Organización y Proyectos de Fabricación Mecánica.	Diplomada o Diplomado en Máquinas Navales. Ingeniera Técnica o Ingeniero Técnico Agrícola: especialidad en Explotaciones Agropecuarias, especialidad en Industrias Agrarias Alimentarias, especialidad en Mecanización y Construcciones Rurales. Ingeniera Técnica o Ingeniero Técnico Aeronáutico, especialidades en Aeronaves y especialidad en equipos y Materiales Aeroespaciales. Ingeniera Técnica o Ingeniero Técnico en Diseño Industrial. Ingeniera Técnica o Ingeniero Técnico Industrial, en todas sus especialidades. Ingeniera Técnica o Ingeniero Técnico de Minas, en todas sus especialidades. Ingeniera Técnica o Ingeniero Técnico Naval, en todas sus especialidades.

		Ingeniera Técnica o Ingeniero Técnico de Obras Públicas, especialidad en Construcciones Civiles.
	Sistemas Electrónicos. Sistemas Electrotécnicos y Automáticos.	Diplomada o Diplomado en Radioelectrónica Naval. Ingeniera Técnica o Ingeniero Técnico Aeronáutico, especialidad en Aeronavegación. Ingeniera Técnica o Ingeniero Técnico Industrial, especialidad en Electricidad, especialidad en Electrónica Industrial. Ingeniera Técnica o Ingeniero Técnico en Informática de Sistemas. Ingeniera Técnica o Ingeniero Técnico de Telecomunicación, en todas sus especialidades.

6.3. Titulaciones requeridas para impartir módulos profesionales que conforman el Curso de Especialización para los centros de titularidad privada, de otras Administraciones distintas a la educativa y orientaciones para la Administración educativa:

MÓDULOS PROFESIONALES	TITULACIONES
5027. Ciberseguridad en proyectos industriales. 5028. Sistemas de control industrial seguros. 5031. Seguridad integral.	Doctora o Doctor, Licenciada o Licenciado, Ingeniera o Ingeniero, Arquitecta o Arquitecto o título de Grado correspondiente u otros títulos equivalentes a efectos de docencia.
5029. Redes de comunicaciones industriales seguras. 5030. Análisis forense en ciberseguridad industrial.	Doctora o Doctor, Licenciada o Licenciado, Ingeniera o Ingeniero, Arquitecta o Arquitecto o título de Grado correspondiente u otros títulos equivalentes a efectos de docencia. Diplomada o Diplomado Universitario, Arquitecta Técnica u Arquitecto Técnico u otros títulos equivalentes a efectos de docencia.

6.4. Titulaciones habilitantes a efectos de docencia para impartir módulos profesionales que conforman el Curso de Especialización para los centros de titularidad privada, de otras Administraciones distintas a la educativa y orientaciones para la Administración educativa:

MÓDULOS PROFESIONALES	TITULACIONES
5027. Ciberseguridad en proyectos industriales. 5028. Sistemas de control industrial seguros. 5031. Seguridad integral.	Diplomada o Diplomado en Máquinas Navales Diplomada o Diplomado en Radioelectrónica Naval. Ingeniera Técnica o Ingeniero Técnico Aeronáutico, especialidades en Aeronaves, especialidad en equipos y Materiales Aeroespaciales, especialidad en Aeronavegación. Ingeniera Técnica o Ingeniero Técnico Agrícola: especialidad en Explotaciones Agropecuarias, especialidad en Industrias Agrarias Alimentarias, especialidad en Mecanización y Construcciones Rurales. Ingeniera Técnica o Ingeniero Técnico en Diseño Industrial. Ingeniera Técnica o Ingeniero Técnico Industrial, en todas sus especialidades. Ingeniera Técnica o Ingeniero Técnico en Informática de Sistemas.

	Ingeniera Técnica o Ingeniero Técnico de Minas, en todas sus especialidades. Ingeniera Técnica o Ingeniero Técnico Naval, en todas sus especialidades. Ingeniera Técnica o Ingeniero Técnico de Obras Públicas, especialidad en Construcciones Civiles. Ingeniera Técnica o Ingeniero Técnico de Telecomunicación, en todas sus especialidades.