Proyecto de Decreto xx/2022, de x de x de 2022, por el que se establece el currículo del Curso de especialización de Formación Profesional en Ciberseguridad en entornos de las tecnologías de operación en la Comunidad Autónoma de Castilla-La Mancha.

La Ley Orgánica 2/2006, de 3 de mayo, de Educación, modificada por la Ley Orgánica 3/2020, de 29 de diciembre establece en su artículo 39.6 que el Gobierno, previa consulta a las comunidades autónomas, establecerá las titulaciones correspondientes a los estudios de formación profesional, así como los aspectos básicos del currículo de cada una de ellas. Por su parte, el artículo 6 bis, apartado 1.c) de la citada ley, establece, en relación con la formación profesional, que el Gobierno fijará las enseñanzas mínimas.

El artículo 10.3 de la Ley Orgánica 5/2002, de 19 de junio, de las Cualificaciones y de la Formación Profesional, dispone que el Gobierno, previa consulta a las Comunidades Autónomas y mediante Real Decreto, podrá crear cursos de especialización para complementar las competencias de quienes ya dispongan de un título de formación profesional.

El Real Decreto 1147/2011, de 29 de julio, por el que se establece la ordenación general de la formación profesional del sistema educativo, regula en su artículo 27 los cursos de especialización de formación profesional e indica los requisitos y condiciones a que deben ajustarse dichos cursos de especialización. En el mismo artículo se indica que versarán sobre áreas que impliquen profundización en el campo de conocimiento de los títulos de referencia, o bien una ampliación de las competencias que se incluyen en los mismos. Por tanto, en cada curso de especialización se deben especificar los títulos de formación profesional que dan acceso al mismo.

En este sentido los cursos de especialización deben responder de forma rápida a las innovaciones que se produzcan en el sistema productivo, así como a ámbitos emergentes que complementen la formación incluida en los títulos de referencia.

Según establece el artículo 37.1 del Estatuto de Autonomía de Castilla-La Mancha, corresponde a la Comunidad Autónoma de Castilla-La Mancha la competencia de desarrollo legislativo y ejecución de la enseñanza en toda su extensión, niveles y grados, modalidades y especialidades, de acuerdo con lo dispuesto en el artículo 27 de la Constitución y leyes orgánicas que conforme al apartado 1 del artículo 81 de la misma lo desarrollen y sin perjuicio de las facultades que atribuye al Estado el número 30 del apartado 1 del artículo 149 y de la Alta Inspección para su cumplimiento y garantía.

La Ley 7/2010, de 20 de julio, de Educación de Castilla-La Mancha, establece en su artículo 69 que, en la planificación de la oferta de Formación Profesional, se tendrán en cuenta las necesidades del tejido productivo de Castilla-La Mancha y los intereses y expectativas de la ciudadanía.

Habiendo entrado en vigor el Real Decreto 478/2020, de 7 de abril, por el que se establece el curso de especialización en Ciberseguridad en entornos de las tecnologías de operación y se fijan los aspectos básicos del currículo, procede establecer el currículo del curso de especialización en Ciberseguridad en entornos de las tecnologías de operación, en el ámbito territorial de esta Comunidad Autónoma, teniendo en cuenta los aspectos definidos en la normativa citada anteriormente.

En Castilla-La Mancha, el perfil profesional de este curso de especialización define a un profesional que es capaz de 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.

El decreto se estructura en diez artículos relativos a aspectos específicos que regulan estas enseñanzas, una disposición adicional, tres disposiciones finales y tres anexos.

Se ha recurrido a una norma con rango de decreto para establecer el desarrollo de las bases pues corresponde al Consejo de Gobierno la potestad reglamentaria de acuerdo con la atribución que le confiere el artículo 13.1 del Estatuto de Autonomía. Asimismo, cabe mencionar que este decreto se ajusta a los principios de buena regulación contenidos en la Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas, principios de necesidad, eficacia, proporcionalidad, seguridad jurídica, transparencia y eficiencia, en tanto que la misma persigue el interés general al facilitar la adecuación de la oferta formativa a las demandas de los sectores productivos de Castilla-La Mancha, ampliar la oferta de formación profesional, avanzar en la integración de la formación profesional en el conjunto del sistema educativo de la Comunidad Autónoma, y su implicación con los agentes sociales y las empresas privadas; no existiendo ninguna alternativa regulatoria menos restrictiva de derechos, resulta coherente con el ordenamiento jurídico y permite una gestión más eficiente de los recursos públicos. Del mismo modo, durante el procedimiento de elaboración de la norma se ha permitido la participación activa de los potenciales destinatarios a través, en su caso, del trámite de audiencia e información pública o de los órganos específicos de participación y consulta y quedan justificados los objetivos que persigue la ley.

En el procedimiento de elaboración de este decreto se ha consultado a la Mesa Sectorial de Educación y han emitido dictamen el Consejo Escolar de Castilla-La Mancha y el Consejo de Formación Profesional de Castilla-La Mancha.

En su virtud, a propuesta de la Consejera de Educación, Cultura y Deportes, de acuerdo/oído el Consejo Consultivo y, previa deliberación del Consejo de Gobierno en su reunión de X de X de 2022,

Artículo 1. Objeto.

El decreto tiene como objeto establecer el currículo del curso de especialización de Formación Profesional en Ciberseguridad en entornos de las tecnologías de operación, en el ámbito territorial de la Comunidad Autónoma de Castilla-La Mancha, teniendo en cuenta sus características geográficas, socio-productivas, laborales y educativas, complementando lo dispuesto en el Real Decreto 478/2020, de 7 de abril, por el que se establece el Curso de especialización en Ciberseguridad en entornos de las tecnologías de operación y se fijan los aspectos básicos del currículo.

Artículo 2. Identificación.

De acuerdo con lo establecido en el artículo 2 del Real Decreto 478/2020, de 7 de abril, el curso de especialización de Formación Profesional en Ciberseguridad en entornos de las tecnologías de operación, queda identificado por los siguientes elementos:

Denominación: Ciberseguridad en entornos de las tecnologías de operación.
Nivel: Formación Profesional de Grado Superior.
Duración: 720 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.

Artículo 3. Requisitos de acceso al curso de especialización.

De acuerdo con lo establecido en el artículo 13 del Real Decreto 478/2020, de 7 de abril, para acceder al curso de especialización en Ciberseguridad en entornos de las tecnologías de operación es necesario estar en posesión de alguno de los siguientes títulos:

a) Título de Técnico Superior en Sistemas Electrotécnicos y Automatizados, establecido por el Real Decreto 1127/2010, de 10 de septiembre, por el que se establece el título de Técnico Superior en Sistemas Electrotécnicos y Automatizados y se fijan sus enseñanzas mínimas.
b) Título de Técnico Superior en Mecatrónica Industrial, establecido por el Real Decreto 1576/2011, de 4 de noviembre, por el que se establece el título de Técnico Superior en Mecatrónica Industrial y se fijan sus enseñanzas mínimas.
c) Título de Técnico Superior en Automatización y Robótica Industrial, establecido por el Real Decreto 1581/2011, de 4 de noviembre, por el que se establece el título de Técnico Superior en Automatización y Robótica Industrial y se fijan sus enseñanzas mínimas.
d) Título de Técnico Superior en Sistemas de Telecomunicaciones e Informáticos, establecido por el Real Decreto 883/2011, de 24 de junio, por el que se establece el título de Técnico Superior en Sistemas de Telecomunicaciones e Informáticos y se fijan sus enseñanzas mínimas.
e) Título de Técnico Superior en Mantenimiento Electrónico, establecido por el Real Decreto 1578/2011, de 4 de noviembre, por el que se establece el título de Técnico Superior en Mantenimiento Electrónico y se fijan sus enseñanzas mínimas.

Artículo 4. Referentes del curso de especialización.

En el Real Decreto 478/2020, de 7 de abril, quedan definidos el perfil profesional, la competencia general, las competencias profesionales, personales y sociales, entorno profesional, prospectiva en el sector o sectores, objetivos generales y accesos, correspondientes al curso.

Artículo 5. Módulos profesionales: Duración y distribución horaria.

1. Módulos profesionales del curso de especialización:

5027. Ciberseguridad en proyectos industriales.
5028. Sistemas de control industrial seguros.
5029. Redes de comunicaciones industriales seguras.
5030. Análisis forense en ciberseguridad industrial.
5031. Seguridad integral.

2. La duración y distribución horaria semanal ordinaria de los módulos profesionales del curso de especialización son las establecidas en el anexo I. El número de horas semanales está establecido para una duración del curso de especialización de dos trimestres o tres trimestres.

Artículo 6. Flexibilización de la oferta.

La Consejería con competencias en materia de educación podrá diseñar otras distribuciones horarias semanales de los módulos del curso de especialización distintas a las establecidas, encaminadas a la realización de una oferta más flexible y adecuada a la realidad social y económica del entorno. En todo caso, se mantendrá la duración total establecida para cada módulo profesional.

Artículo 7. Resultados de aprendizaje, criterios de evaluación, duración, contenidos y orientaciones pedagógicas de los módulos profesionales.

1. Los resultados de aprendizaje, criterios de evaluación, duración y contenidos de los módulos profesionales que forman parte del currículo del curso de especialización de Formación Profesional en Ciberseguridad en entornos de las tecnologías de operación, en Castilla-La Mancha son los establecidos en el anexo II de este decreto.

2. Las orientaciones pedagógicas de los módulos profesionales que forman parte del título del curso de especialización en Ciberseguridad en entornos de las tecnologías de operación son las establecidas en el anexo I del Real Decreto 478/2020, de 7 de abril.

Artículo 8. Profesorado.

1. La docencia de los módulos profesionales que constituyen las enseñanzas de este curso de especialización corresponde al profesorado del Cuerpo de Catedráticos de Enseñanza Secundaria, del Cuerpo de Profesores de Enseñanza Secundaria y del Cuerpo de Profesores Técnicos de Formación Profesional, según proceda, de las especialidades establecidas en el anexo III A) del Real Decreto 478/2020, de 7 de abril.

2. Las titulaciones requeridas para acceder a los cuerpos docentes citados son, con carácter general, las establecidas en el artículo 13 del Reglamento de ingreso, accesos y adquisición de nuevas especialidades en los cuerpos docentes a que se refiere la Ley Orgánica 2/2006, de 3 de mayo, de Educación, aprobado por el Real Decreto 276/2007 de 23 de febrero.

3. El profesorado especialista tendrá atribuida la competencia docente de los módulos profesionales especificados en el anexo III A) del Real Decreto 478/2020, de 7 de abril.

4. El profesorado especialista deberá cumplir los requisitos generales exigidos para el ingreso en la función pública docente establecidos en el artículo 12 del Reglamento de ingreso, accesos y adquisición de nuevas especialidades en los cuerpos docentes a que se refiere la Ley Orgánica 2/2006, de 3 de mayo, aprobado por el Real Decreto 276/2007, de 23 de febrero.

5. Además, con el fin de garantizar que se da respuesta a las necesidades de los procesos involucrados en el módulo profesional, es necesario que el profesorado especialista acredite al inicio de cada nombramiento una experiencia profesional reconocida en el campo laboral correspondiente, debidamente actualizada, de al menos dos años de ejercicio profesional en los cuatro años inmediatamente anteriores al nombramiento.

6. Para el profesorado de los centros de titularidad privada, de otras administraciones distintas de las educativas, las titulaciones requeridas y los requisitos necesarios para la impartición de los módulos profesionales que conforman el curso de especialización son las incluidas en el anexo III C) del Real Decreto 478/2020, de 7 de abril. En todo caso, se exigirá que las enseñanzas conducentes a las titulaciones citadas engloben los objetivos de los módulos profesionales expresados en resultados de aprendizaje y, si dichos objetivos no estuvieran incluidos, además de la titulación deberá acreditarse, mediante certificación, una experiencia laboral de, al menos, tres años en el sector vinculado a la familia profesional, realizando actividades productivas en empresas relacionadas implícitamente con los resultados de aprendizaje.

7. Para las titulaciones habilitantes a efectos de docencia, se atenderá a lo establecido en la disposición adicional tercera del Real Decreto 478/2020, de 7 de abril.

Artículo 9. Espacios y equipamientos.

1. Los espacios y equipamientos mínimos necesarios para el desarrollo de las enseñanzas del curso de especialización de Formación Profesional en Ciberseguridad en entornos de las tecnologías de operación, son los establecidos en el anexo III de este decreto.

2. Las condiciones de los espacios y equipamientos son las establecidas en el artículo 10 del Real Decreto 478/2020, de 7 de abril, que, en todo caso, deberán cumplir la normativa sobre igualdad de oportunidades, diseño para todos y accesibilidad universal, prevención de riesgos laborales y seguridad y salud en el puesto de trabajo.

Artículo 10. Requisitos de los centros que impartan los cursos de especialización.

Los centros docentes que oferten este curso de especialización deberán cumplir, además de lo establecido en este Decreto, el requisito de impartir alguno de los títulos que dan acceso al mismo y que figuran en el artículo 3 de este Decreto.

Disposición adicional única. Autonomía pedagógica de los centros.

Los centros autorizados para impartir el curso de especialización en Ciberseguridad en entornos de las tecnologías de operación concretarán y desarrollarán las medidas organizativas y curriculares que resulten más adecuadas a las características de su alumnado y de su entorno productivo, de manera flexible y en uso de su autonomía pedagógica, en el marco legal del proyecto educativo, en los términos establecidos por la Ley Orgánica 3/2020, de 29 de diciembre, por la que se modifica la Ley Orgánica 2/2006 de 3 de mayo, y en el Capítulo II del Título III de la Ley 7/2010, de 20 de julio, de Educación de Castilla-La Mancha, e incluirán los elementos necesarios para garantizar que las personas que cursen el ciclo formativo indicado desarrollen las competencias incluidas en el currículo en “diseño para todos”.

Disposición final primera. Implantación del currículo.

El currículo se implantará en todos los centros docentes de la Comunidad Autónoma de Castilla-La Mancha, autorizados para impartirlo, a partir del curso escolar 2022/2023.

Disposición final segunda. Desarrollo.

Se autoriza a la persona titular de la Consejería competente en materia educativa, para dictar las disposiciones que sean precisas para la aplicación de lo dispuesto en este decreto.

Disposición final tercera. Entrada en vigor.

Este decreto entrará en vigor a los veinte días de su publicación en el Diario Oficial de Castilla-La Mancha.

Dado en Toledo, el X de X de 2022

La Consejera de Educación, Cultura y Deportes

El Presidente

Rosa Ana Rodríguez Pérez Emiliano García-Page Sánchez

ANEXO I

Duración de los módulos profesionales y la asignación horaria semanal

Módulos Profesionales	Horas totales	Distribución horaria semanal (Tres trimestres: 32 semanas)	Distribución horaria semanal (Dos trimestres: 24 semanas)
5027. Ciberseguridad en proyectos industriales.	100	3	4
5028. sistemas de control industrial seguros.	117	4	5
5029. Redes de comunicaciones industriales seguras.	135	4	6
5030. Análisis forense en ciberseguridad industrial.	197	6	8
5031. Seguridad integral.	171	5	7
	720	**22**	**30**

ANEXO II

Módulos Profesionales

Módulo profesional: Ciberseguridad en proyectos industriales.
Código: 5027.
Créditos ECTS: 6.

Resultados de aprendizaje y criterios de evaluación.

1. 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.

2. 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 ha realizado el análisis y gestión de los riesgos asociados a la cadena de suministro.
d) Se han establecido los requisitos de ciberseguridad en el proceso de gestión de compras.

3. 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 han tenido en cuenta los principios de economía circular.
e) Se han incorporado criterios de ciberseguridad en las pruebas de aceptación en fábrica (*FAT*).
f) Se han incorporado criterios de seguridad en las pruebas de aceptación
g) Se han establecido los planes de control de calidad y las auditorías.
h) Se ha contemplado la evaluación de ciberseguridad.

4. 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 la fase de operación y mantenimiento de un proyecto industrial.
g) Se han implementado planes de concienciación y formación de ciberseguridad.

5. 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 detectada en el proceso de verificación.

Duración: 100 horas.
Contenidos:

Actividades de ciberseguridad en el diseño de un proyecto industrial:

− Diseño conceptual del proyecto.
− 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.

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.
− Análisis y gestión de riesgos en la cadena de suministro.
− Implementación de las medidas de ciberseguridad «extremo a extremo», especialmente.

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.
− Actualización de la documentación de ingeniería.
− Mediciones en las instalaciones.
− Compleción de la construcción de los sistemas.
− Ejecutar los planes de control de calidad y las auditorías.

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 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: Sistemas de control industrial seguros.
Código: 5028.
Créditos ECTS: 7.

Resultados de aprendizaje y criterios de evaluación.

1. 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 para 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.

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

Criterios de evaluación:

a) Se han identificado los diferentes tipos de activos que componen una instalación industrial.
b) Se han caracterizado diferentes tipos de amenazas para los diferentes activos.
c) Se han localizado datos de interés sobre vulnerabilidades conocidas en sistemas de control industrial.
d) Se han comparado diferentes herramientas de diagnóstico.
e) Se han identificado y evaluado la seguridad de credenciales y los medios de control de acceso.
f) Se ha evaluado el *firmware* y/o configuración de un dispositivo mediante procedimientos de ingeniería inversa.
g) Se han automatizado acciones de verificación de la configuración de dispositivos y sistemas.
h) Se ha creado un *testbed* gemelo de un sistema de control industrial significativo imitando su configuración.
i) Se ha elaborado y ordenado una lista de riesgos asociados a los sistemas de control de una instalación industrial.

3. 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.

4. 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.

5. 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.

6. 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.

Duración: 117 horas.
Contenidos:

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

− Tecnologías de la operación (*OT)*, detectar y/o cambiar 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.

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.

Documentación de los procesos en ciberseguridad:

− Elaboración de informes técnicos.
− Adaptación del lenguaje al receptor del informe.
− Presentación de resultados.

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.

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.

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: Redes de comunicaciones industriales seguras.
Código: 5029.
Créditos ECTS: 9.

Resultados de aprendizaje y criterios de evaluación.

1. 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 en un entorno de automatización industrial.
b) Se han descrito los diferentes elementos de supervisión y sistemas *SCADA*.
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.

2. 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.

3. Implementa redes industriales aplicando técnicas de *switching* y de enrutamiento.

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 ha 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 ha implementado conexiones simples con redes ofimáticas.
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.*

4. Implementa redes industriales inalámbricas aplicando los estándares del sector.

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 wifis para instalaciones industriales.

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

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.

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

a) Se ha implementado la segmentación en redes de automatización.
b) Se ha 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).*

7. Identifica vulnerabilidades en dispositivos de redes industriales proponiendo contramedidas.

Criterios de evaluación:

a) Se han identificado vulnerabilidades conocidas en dispositivos y redes industriales.
b) Se ha valorado el alcance de las vulnerabilidades.
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.

8. 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 y configurado 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.

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

Criterios de evaluación:

a) Se ha 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.

10. 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.

Duración: 135 horas.
Contenidos:

Niveles de seguridad en un entorno industrial automatizado:

− Niveles de automatización industrial.
− Dispositivos de control y supervisión disponibles en el mercado.
− Opciones de comunicaciones y protocolos industriales avanzados existentes en el mercado.
− Comunicación *OPC UA* que permite comunicación de equipos y sistemas industriales para la recolección y control de datos.

Evaluación de escenarios de riesgo tecnológico en redes industriales:

− Tipos de dispositivos de una red industrial.
− Arquitectura de red física y lógica.
− Zonificación (red de control, de supervisión, corporativa, etc.).
− Evaluación del riesgo.
− Riesgos externos.

Implementación de redes industriales aplicando técnicas de *switching* y de enrutamiento:

− Analizar la Técnicas de *switching* en redes industriales.
− *LAN, MAN, WAN, GAN.*
− Topologías típicas en *Ethernet* Industrial.

− 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.
  o 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.
− Las tablas de enrutamiento.
− Conexiones redundantes con redes ofimáticas mediante *VRRP (Virtual Router Redundancy Protocol).*
− Conexiones a redes *legacy* mediante *RIP (Routing Information Protocol*).

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.
− 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*).

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.

Diseño de la red de automatización mediante segmentación:

− Segmentación en las redes de automatización.
− Estructuración de redes con *VLAN*'s: estáticas y dinámicas.
− Segmentación de célula con cortafuegos industriales.
− Segmentación entre entornos *IT* y *OT* con *NGF (Next Generation Firewall).*

Identificación vulnerabilidades 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.

Detección de incidentes en tiempo real en redes industriales:

− Análisis de tráfico.
− Sistemas de detección de intrusiones (*IDS, IPS*).

Definición de procedimientos de verificación y supervisión:

− Métricas de cumplimiento de políticas.
− Gestión de registros (*Logs*).
− Monitorización de redes.

Configuración de dispositivos de redes industriales:

− Configuración de usuarios y/o direcciones *IP* habilitadas a controlar los dispositivos.
− Gestión de actualizaciones del *firmware* de los dispositivos.
− Copias de seguridad de una configuración deseada y su custodia.

Módulo profesional: Análisis forense en ciberseguridad industrial.
Código: 5030.
Créditos ECTS: 11.

Resultados de aprendizaje y criterios de evaluación.

1. 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.

2. 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.

3. 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.

4. 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.

5. 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.

Duración: 197 horas.
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.

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.

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.

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.

Respuesta ante un incidente de ciberseguridad:

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

Módulo profesional: Seguridad integral.
Código: 5031.
Créditos ECTS: 10.

Resultados de aprendizaje y criterios de evaluación.

1. 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.

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

Criterios de evaluación:

a) Se ha 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.

3. 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.

4. 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.

5. 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).

Duración: 171 horas.
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*.

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*.

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*.

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.

Gestión integral 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 SP*800-*X*, *NERC-ZIP*, *IEC* 62443, *BSI*-100 o las que eventualmente la sustituyan.

Anexo III

Espacios y equipamientos mínimos

Espacios:

Espacio formativo	Superficie m²	
	30 alumnos	20 alumnos
Aula polivalente.	60	40
Aula de informática.	120	80
Laboratorio de sistemas automáticos.	180	120
Taller de sistemas automáticos.	200	130

Equipamientos:

Espacio formativo	Equipamientos mínimos
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. 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. Fuentes de alimentación. Transformadores monofásicos. Transformadores trifásicos. 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.

Espacio formativo	Equipamientos mínimos
	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.