(V-1)

(27/06/2019)

Proyecto de Real Decreto EFP/XXX/2019, de XX de XXXXX 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.

La Ley Orgánica 2/2006, de 3 de mayo, de Educación, dispone 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.

La Ley Orgánica 4/2011, de 11 de marzo, complementaria de la Ley de Economía Sostenible, por la que se modifican las Leyes Orgánicas 5/2002, de 19 de junio, de las Cualificaciones y de la Formación Profesional, 2/2006, de 3 de mayo, de Educación, y 6/1985, de 1 de julio, del Poder Judicial, modificó determinados aspectos de la Ley Orgánica 5/2002, de 19 de junio. Entre ellos se encontraba la adición de un nuevo apartado 3 al artículo 10 de la misma, según el cual el Gobierno, previa consulta a las comunidades autónomas y mediante Real Decreto, podía crear cursos de especialización para completar las competencias de quienes dispusieran de un título de formación profesional.

Por tanto, y a efectos de la Clasificación Internacional Normalizada de la Educación (CINE-11), los cursos de especialización se considerarán un programa secuencial de los títulos de referencia que dan acceso a los mismos.

Por su parte, la Ley Orgánica 2/2006, de 3 de mayo en su artículo 6 bis, apartado 4, establece, en relación con la formación profesional, que el Gobierno fijará los objetivos, competencias, contenidos, resultados de aprendizaje y criterios de evaluación del currículo básico. Los contenidos del currículo básico requerirán el 55 por 100 de los horarios para las comunidades autónomas que tengan lengua cooficial y el 65 por 100 para aquellas que no la tengan.

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.

Asimismo, el artículo 9 del citado real decreto, establece la estructura de los cursos de especialización y se indica en el artículo 27, que dada la naturaleza de los mismos, se requiere la especificación completa de la formación; no obstante, las administraciones educativas podrán adaptar estas especificaciones al sector productivo de su territorio.

A estos efectos, procede determinar para cada curso de especialización de formación profesional su identificación, el perfil profesional, el entorno profesional, la prospectiva en el sector o sectores, las enseñanzas del curso de especialización y los parámetros básicos de contexto formativo.

Con el fin de facilitar el reconocimiento de créditos entre el curso de especialización y las enseñanzas conducentes a títulos universitarios y viceversa, y de acuerdo con el artículo 10 apartado 3.g) del Real Decreto 1147/2011, de 29 de julio, se establecerá la equivalencia de cada módulo profesional con créditos europeos ECTS para todo el estado.

Así, este real decreto, conforme a lo previsto en el Real Decreto 1147/2011, de 29 de julio, establece y regula, en los aspectos y elementos básicos antes indicados, el Curso de Especialización de formación profesional del sistema educativo en *Ciberseguridad en entornos de las tecnologías de operación*

Asimismo, este real decreto responde a los principios de eficiencia y austeridad que han de presidir el funcionamiento de los servicios públicos establecidos en el Real Decreto-Ley 14/2012, de 20 de abril, de medidas urgentes de racionalización del gasto público en el ámbito educativo, en cuanto a las posibilidades de su implantación.

Este real decreto tiene carácter de norma básica, al amparo de las competencias que atribuye al Estado el artículo 149.1.30.ª de la Constitución.

Se ha recurrido a una norma reglamentaria para establecer bases estatales conforme con el Tribunal Constitucional, que admite que “excepcionalmente” las bases puedan establecerse mediante normas reglamentarias en determinados supuestos, como ocurre en el presente caso, cuando “resulta complemento indispensable para asegurar el mínimo común denominador establecido en las normas legales básicas” (así, entre otras, en las (SSTC 25/1983, de 7 de abril, 32/1983, de 28 de abril, y 42/1988, de 22 de marzo).

Asimismo, cabe mencionar que este real decreto se ajusta a los principios de buena regulación contenidos en la Ley 39/2015, de 1 de octubre, 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, ampliar la oferta de formación profesional, avanzar en la integración de la formación profesional en el conjunto del sistema educativo y reforzar la cooperación entre las administraciones educativas, así como 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 del trámite de audiencia e información pública y quedan justificados los objetivos que persigue la ley.

En la tramitación de este real decreto se han cumplido los trámites establecidos en la Ley 50/2007, de 27 de noviembre, del Gobierno.

En el proceso de elaboración de este real decreto han sido consultadas las comunidades autónomas y ha emitido dictamen el Consejo Escolar del Estado e informes el Consejo General de la Formación Profesional y el Ministerio de Política Territorial y Función Pública.

En su virtud, a propuesta de la Ministra de Educación y Formación Profesional y previa deliberación del Consejo de Ministros en su reunión del día XXX.

DISPONGO:

CAPITULO I

Disposiciones generales

Artículo 1. Objeto.

Este real decreto tiene por objeto el establecimiento del Curso de Especialización de formación profesional en Ciberseguridad en entornos de las tecnologías de operación con carácter oficial y validez en todo el territorio nacional, así como de los aspectos básicos de su currículo.

CAPITULO II

Identificación del curso de especialización, títulos de referencia, perfil profesional, entorno profesional y prospectiva del curso de especialización en el sector o sectores

Artículo 2. Identificación.

El curso de especialización de Ciberseguridad en entornos de las tecnologías de operación queda identificado para todo el territorio nacional 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. Acceso al curso de especialización.

Los títulos que dan acceso a este curso de especialización son los siguientes:

a) 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.
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.

Artículo 4. *Perfil profesional del curso de especialización*.

El perfil profesional del Curso de Especialización en Ciberseguridad en entornos de las tecnologías de operación queda determinado por su competencia general y sus competencias profesionales, personales y sociales.

Artículo 5. 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.

Artículo 6. Competencias profesionales, personales y sociales.

Las competencias profesionales, personales y sociales de este curso de especialización son las que se relacionan a continuación:

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 tanto 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 los miembros 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.

Artículo 7. Entorno profesional.

1. 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.

2. Las ocupaciones y puestos de trabajo más relevantes (entendido el masculino como genérico) son los siguientes:

a) Experto en ciberseguridad en entornos de la operación.
b) Auditor de ciberseguridad en entornos de la operación.
c) Consultor de ciberseguridad en entornos de la operación.
d) Analista de ciberseguridad en entornos de la operación.

Artículo 8. Prospectiva del curso de especialización en el sector o sectores.

Las administraciones educativas tendrán en cuenta, para la implantación de la oferta, la valoración de las siguientes consideraciones en su territorio que:

a) La evolución de la industria hacia entornos con un nivel de interconexión cada vez más elevado hace necesaria la incorporación de la ciberseguridad desde el mismo diseño de los sistemas de producción, teniendo en cuenta el aumento de interacción entre los mundo reales y virtuales.
b) La demanda de integración de las organizaciones en todos sus ámbitos plantea nuevos retos de gestión y seguridad debido a la vinculación existente entre la producción de bienes y la generación de servicios de alta calidad.
c) Las actividades relacionadas con los sistemas productivos que se desarrollan en el ciberespacio aumentan de forma continua lo que requiere estrictos procedimientos de seguridad debido a que la información y los datos se han convertido en activos de elevado valor.
d) El incremento de la conectividad y la interdependencia de las redes y sistemas genera vulnerabilidades que es necesario prevenir para protegerlos de ciberataques o minimizar el impacto de estos.

e) Los sistemas estratégicos y las infraestructuras críticas deben de ser protegidos adecuadamente para garantizar la seguridad del ciberespacio y lograr una sociedad digital basada en la confianza.
f) La demanda de profesionales cualificados en ciberseguridad con conocimientos de las bases jurídicas que afectan a la informática y con el dominio de las metodologías y herramientas que ayuden a prevenir o esclarecer delitos informáticos será cada vez más elevada en los próximos años.

CAPÍTULO III

Enseñanzas del curso de especialización y parámetros básicos de contexto.

Artículo 9. Objetivos generales.

Los objetivos generales de este curso de especialización son los siguientes:

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.
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.
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.
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.
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.

Artículo 10. Módulos profesionales.

1. Los módulos profesionales de este curso de especialización:

a. Quedan desarrollados en el Anexo I de este real decreto, cumpliendo lo previsto en el artículo 10 apartado 3 del Real Decreto 1147/2011, de 29 de julio, por el que se establece la ordenación general de la formación profesional del sistema educativo.

b. Son los que a continuación se relacionan:

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. Las administraciones educativas adaptarán los currículos, respetando lo establecido en este real decreto y de acuerdo con lo dispuesto en el artículo 27 del Real Decreto 1147/2011, de 29 de julio.

Artículo 11. Espacios y equipamientos.

1. Los espacios necesarios para el desarrollo de las enseñanzas de este curso de especialización son los establecidos en el Anexo II de este real decreto.

2. Los espacios dispondrán de la superficie necesaria y suficiente para desarrollar las actividades de enseñanza que se deriven de los resultados de aprendizaje de cada uno de los módulos profesionales que se imparten en cada uno de los espacios. Además, deberán cumplir las siguientes condiciones:

a) La superficie se establecerá en función del número de personas que ocupen el espacio formativo y deberá permitir el desarrollo de las actividades de enseñanza aprendizaje con la ergonomía y la movilidad requeridas dentro del mismo.

b) Deberán cubrir la necesidad espacial de mobiliario, equipamiento e instrumentos auxiliares de trabajo.

c) Deberán respetar los espacios o superficies de seguridad que exijan las máquinas y equipos en funcionamiento.

d) Respetarán la normativa sobre prevención de riesgos laborales, la normativa sobre seguridad y salud en el puesto de trabajo y cuantas otras normas sean de aplicación.

3. Los espacios formativos establecidos podrán ser ocupados por diferentes grupos que cursen el mismo u otros cursos de especialización, o etapas educativas.

4. Los diversos espacios formativos identificados no deben diferenciarse necesariamente mediante cerramientos.

5. Los equipamientos que se incluyen en cada espacio han de ser los necesarios y suficientes para garantizar al alumnado la adquisición de los resultados de aprendizaje y la calidad de la enseñanza. Además deberán cumplir las siguientes condiciones:

a) El equipamiento (equipos, máquinas, etc.) dispondrá de la instalación necesaria para su correcto funcionamiento, cumplirá con las normas de seguridad y prevención de riesgos y con cuantas otras sean de aplicación.

b) La cantidad y características del equipamiento deberán estar en función del número de personas matriculadas y permitir la adquisición de los resultados de aprendizaje, teniendo en cuenta los criterios de evaluación y los contenidos que se incluyen en cada uno de los módulos profesionales que se impartan en los referidos espacios.

6. Las Administraciones competentes velarán para que los espacios y el equipamiento sean los adecuados en cantidad y características para el desarrollo de los procesos de enseñanza y aprendizaje que se derivan de los resultados de aprendizaje de los módulos correspondientes y garantizar así la calidad de estas enseñanzas.

Artículo 12. *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) de este real decreto.

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 y por el que se regula el régimen transitorio de ingreso a que se refiere la disposición transitoria decimoséptima de la citada ley, aprobado por al 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) de este real decreto.

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 y por el que se regula el régimen transitorio de ingreso a que se refiere la disposición transitoria decimoséptima de la citada ley, aprobado por al Real Decreto 276/2007, de 23 de febrero por el que se aprueba el 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, y se regula el régimen transitorio de ingreso a que se refiere la disposición transitoria decimoséptima de la citada ley.

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 o de titularidad pública 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) de este real decreto. En todo caso, se exigirá que las enseñanzas conducentes a las titulaciones citadas engloben los objetivos de los módulos profesionales 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. Las Administraciones competentes velarán para que el profesorado que imparta los módulos profesionales cumpla con los requisitos especificados y garantizar así la calidad de estas enseñanzas.

8. Dada la naturaleza de estos cursos de especialización, el profesorado de centros públicos y privados, deberá demostrar que posee los conocimientos suficientes sobre los contenidos de los módulos profesionales a impartir en dicho curso.

Artículo 13. Requisitos de los centros que impartan los cursos de especialización.

Los centros docentes que oferten estos cursos de especialización deberán cumplir, además de los establecidos en este real decreto, los siguientes requisitos:

a) Impartir alguno de los títulos que dan acceso a los mismos y que figuran en el artículo 3.
b) La existencia de organizaciones que se dediquen al desarrollo de productos que coincidan con los de la especialización en la zona de influencia del centro.

CAPITULO IV

Acceso, exenciones y vinculación a otros estudios.

Artículo 14. Requisitos de acceso al curso de especialización.

Para acceder al Curso de Especialización en Ciberseguridad en entornos de las tecnologías de operación es necesario estar en posesión de alguno de los títulos establecidos como referencia en el artículo 3 de este real decreto.

Artículo 15. Vinculación a otros estudios.

El Gobierno, oído el Consejo de Universidades, regulará, en norma específica, el reconocimiento de créditos entre los cursos de especialización vinculados a los cursos de especialización de la formación profesional y las enseñanzas universitarias de Grado. A efectos de facilitar el régimen de convalidaciones, en este real decreto se han asignado 43 créditos ECTS entre todos los módulos profesionales de este curso de especialización.

Disposición adicional primera. Referencia del curso de especialización en el marco europeo.

Una vez establecido el marco nacional de cualificaciones, de acuerdo con las recomendaciones europeas, se determinará el nivel correspondiente a los cursos de especialización en el marco nacional y su equivalente en el europeo.

Disposición adicional segunda. Regulación del ejercicio de la profesión.

El curso de especialización establecido en este real decreto no constituye una regulación del ejercicio de profesión regulada alguna.

Disposición adicional tercera. Accesibilidad universal en las enseñanzas de este curso de especialización.

1. Las administraciones educativas, en el ámbito de sus respectivas competencias, incluirán en el currículo de este curso de especialización los elementos necesarios para garantizar que las personas que lo cursen desarrollen las competencias incluidas en el currículo en «diseño para todas las personas».

2. Asimismo, dichas Administraciones adoptarán las medidas que estimen necesarias para que este alumnado pueda acceder y cursar dicho curso de especialización en las condiciones establecidas en la disposición final tercera del Real Decreto Legislativo 1/2013, de 29 de noviembre, por el que se aprueba el Texto Refundido de la Ley General de derechos de las personas con discapacidad y de su inclusión social.

Disposición adicional cuarta. Titulaciones habilitantes a efectos de docencia.

1. A los efectos del artículo 12.2 de este real decreto, y de conformidad con lo dispuesto en el artículo 95.1 de la Ley Orgánica, 2/2006, de 3 de mayo, de Educación y en la disposición adicional décimo quinta de la Ley Orgánica 4/2007, de 12 de abril, por la que se modifica la Ley Orgánica 6/2001, de 21 de diciembre, de Universidades habilitarán excepcionalmente a efectos de docencia las titulaciones recogidas en el anexo III B) de este real decreto para las distintas especialidades del profesorado.

2. A los efectos del artículo 12.6 de este real decreto, y de conformidad con la disposición adicional décimo quinta de la Ley Orgánica 4/2007, de 12 de abril, excepcionalmente habilitarán a efectos de docencia las titulaciones recogidas en el anexo III D) de este real decreto para las distintas especialidades del profesorado.

Disposición final primera. Título competencial.

Este real decreto tiene carácter de norma básica y se dicta al amparo de las competencias que atribuye al Estado el artículo 149.1.30ª de la Constitución, que atribuye al Estado las competencias para la regulación de las condiciones de obtención, expedición y homologación de los títulos académicos y profesionales y normas básicas para el desarrollo del artículo 27 de la Constitución, a fin de garantizar el cumplimiento de las obligaciones de los poderes públicos en esta materia.

Disposición final segunda. Entrada en vigor.

Este real decreto entrará en vigor el día siguiente al de su publicación en el Boletín Oficial del Estado.

Dado en Madrid, el de de 201X.

La Ministra de Educación y Formación Profesional
Mª ISABEL CELAÁ DIÉGUEZ

ANEXO I

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: 60 horas.

Contenidos básicos:

Determinación de las actividades de ciberseguridad a incluir 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.

Incorporación de los requisitos de ciberseguridad en el proceso de provisión a cumplir por los proveedores.

- 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:

Establecimiento de las 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.

Implementación de las actividades de ciberseguridad propias de 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:

Implementación de las 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:

Orientaciones pedagógicas.

Este módulo profesional contiene la formación necesaria para desempeñar la función de analista de ciberseguridad en entorno *OT.*

La función de analista incluye aspectos como determinar las actividades de ciberseguridad a incorporar en cada una de las fases del ciclo de vida de un proyecto industrial.

Las actividades profesionales asociadas a esta función se aplican incluyendo los requisitos y tomando las medidas necesarias para cumplir con los criterios de calidad exigidos por la normativa vigente en ciberseguridad.

La formación del módulo contribuye a alcanzar los objetivos generales a), m), n), ñ), o y q) y las competencias a), h), i), j), k) y l) del curso de especialización.

Las líneas de actuación en el proceso de enseñanza aprendizaje que permiten alcanzar los objetivos del módulo versarán sobre:

- Diseñar el proyecto industrial de acuerdo a la normativa de ciberseguridad.
- Gestionar los proveedores atendiendo a los requisitos de ciberseguridad.
- Implementar el proyecto.
- Documentar el proyecto.
- Gestionar la conservación de la información.

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* y *OT* 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: 65 horas.

Contenidos básicos:

Determinación de los cambios necesarios 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 en sistemas de control de instalaciones industriales.

- 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 de diagnósticos, análisis y otros, pertinentes 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 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.

Orientaciones pedagógicas.

Este módulo profesional contiene la formación necesaria para desempeñar la función de diseñar las políticas de seguridad de la organización cumpliendo las normas vigentes de ciberseguridad.

La función de diseñar incluye aspectos como la evaluación de escenarios de riesgo tecnológicos y la configuración de los sistemas de control industrial minimizando los riesgos.

Las actividades profesionales asociadas a esta función se aplican en el proceso de análisis para la detección de anomalías.

La formación del módulo contribuye a alcanzar los objetivos generales b), c), d), m), n), ñ), o), p) y q) y las competencias b), c), h), i), j), k) y l) del curso de especialización.

Las líneas de actuación en el proceso de enseñanza aprendizaje que permiten alcanzar los objetivos del módulo versarán sobre:

- Adaptar el entorno industrial a las tecnologías 4.0.
- Evaluar los riesgos tecnológicos en sistemas de control industrial.
- Diseñar e implementar políticas de seguridad.
- Monitorizar los sistemas de control.

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: 75 horas.

Contenidos básicos:

Determinación de los 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.
    - 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.

Orientaciones pedagógicas.

Este módulo profesional contiene la formación necesaria para desempeñar la función de administrador de redes en un entorno industrial automatizado garantizando la seguridad de las comunicaciones.

La función de administrador incluye aspectos como la implementación de estándares de redes y la detección de posibles incidentes en tiempo real.

Las actividades profesionales asociadas a esta función se aplican en el proceso de diseño e implementación de la red, incluyendo las medidas de seguridad que permitan detectar incidentes en tiempo real.

La formación del módulo contribuye a alcanzar los objetivos generales e), f), g), h), m), n), ñ), o), p) y q) y las competencias d), e), h), i), j), k) y l) del curso de especialización.

Las líneas de actuación en el proceso de enseñanza aprendizaje que permiten alcanzar los objetivos del módulo versarán sobre:

- Establecer los niveles de seguridad en un entorno industrial
- Evaluar de escenarios de riesgo tecnológico en redes industriales.
- Implementar distintos estándares de redes.
- Identificar vulnerabilidades y detectar incidentes.
- Supervisar el cumplimiento de las políticas de seguridad implementadas.

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 de 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: 105 horas.

Contenidos básicos:

Desarrollo del 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.

Desarrollo del 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.

Desarrollo del 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 que afecta a la organización.

- 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.

Orientaciones pedagógicas.

Este módulo profesional contiene la formación necesaria para desempeñar la función de análisis forense en sistemas de control industrial.

La función de análisis forense incluye aspectos como la respuesta a los incidentes que afecten a la organización tomando las medidas necesarias.

Las actividades profesionales asociadas a esta función se aplican en la extracción de las evidencias para su análisis aplicando las metodologías pertinentes que garantice la disponibilidad de los sistemas.

La formación del módulo contribuye a alcanzar los objetivos generales i), j), m), n), ñ), o), p) y q) y las competencias f), h), i), j), k) y l) del curso de especialización.

Las líneas de actuación en el proceso de enseñanza aprendizaje que permiten alcanzar los objetivos del módulo versarán sobre:

- Analizar evidencias
- Utilizar herramientas automatizadas en dispositivos.
- Desarrollar procedimientos de actuación ante los incidentes detectados.
- Implantar capacidades de ciberresiliencia.
- Documentar y notificar los incidentes.

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: 95 horas.

Contenidos básicos:

Integración de las 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*.

Integración de las 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*.

Integración de las 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*.

Aplicación de las 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).

Orientaciones pedagógicas.

Este módulo profesional contiene la formación necesaria para desempeñar la función de integrar las normas de ciberseguridad en la organización.

La función de integración de las normas de ciberseguridad incluye aspectos como la implementación de los procedimientos de seguridad física y operacional con los requisitos de calidad exigidos.

Las actividades profesionales asociadas a esta función se aplican en el análisis y evaluación de riesgo de la ciberseguridad en entornos *OT*.

La formación del módulo contribuye a alcanzar los objetivos generales k), l), m), n), ñ), o), p) y q) y las competencias g), h), i), j), k) y l) del curso de especialización.

Las líneas de actuación en el proceso de enseñanza aprendizaje que permiten alcanzar los objetivos del módulo versarán sobre:

- Implementar procedimientos de seguridad física.
- Implementar los procedimientos de seguridad operacional.
- Implementar los procedimientos de calidad.
- Aplicar técnicas y medidas de seguridad de los *SIS*.
- Gestionar los riesgos de acuerdo a la normativa en ciberseguridad en vigor.

ANEXO II

Espacios y equipamientos mínimos

Espacios:

Espacio formativo
Aula de informática
Laboratorio de sistemas automáticos
Taller de sistemas automáticos
Aula polivalente

Equipamientos:

Espacio formativo	Equipamiento
Aula polivalente	- Sistema de proyección. - Ordenadores en red y con acceso a Internet. - Dispositivos de almacenamiento en red. - Escáner. Impresoras. - Equipos audiovisuales
Aula de informática	- Sistema de proyección. - Ordenadores en red y con acceso a Internet. - Escáner. - Plotter. - Programas de gestión de proyectos. - Impresoras. - 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. - Impresoras. - *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. Impresoras. - 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.

ANEXO III A)

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.	- Sistemas electrotécnicos y automáticos. - Sistemas electrónicos. - Organización y Proyectos de Fabricación Mecánica.	- Catedrático de Enseñanza Secundaria. - Profesor de Enseñanza Secundaria.
	Profesor Especialista.	
5028. Sistemas de control industrial seguros.	- Sistemas electrotécnicos y automáticos. Sistemas electrónicos. - Organización y Proyectos de Fabricación Mecánica.	- Catedrático de Enseñanza Secundaria. - Profesor de Enseñanza Secundaria
	Profesor Especialista.	
5029. Redes de comunicaciones industriales seguras.	- Instalaciones electrotécnicas. Equipos electrónicos.	Profesores Técnicos de Formación Profesional.
	Profesor Especialista.	
5030. Análisis forense en ciberseguridad	- Instalaciones electrotécnicas.	- Profesores Técnicos de Formación Profesional.

Módulo Profesional	Especialidad del profesorado	Cuerpo
industrial.	- Equipos electrónicos.	
	Profesor Especialista.	
5031. Seguridad integral.	- Sistemas electrotécnicos y automáticos. - Sistemas electrónicos. - Organización y Proyectos de Fabricación Mecánica.	- Catedrático de Enseñanza Secundaria. - Profesor de Enseñanza Secundaria.
	Profesor Especialista.	

ANEXO III B)

Titulaciones habilitantes a efectos de docencia

Cuerpos	Especialidades	Titulaciones
Profesores de Enseñanza Secundaria	Sistemas Electrónicos	- Diplomado en Radioelectrónica Naval. - Ingeniero Técnico Aeronáutico, especialidad en Aeronavegación. - Ingeniero Técnico en Informática de Sistemas. - Ingeniero Técnico Industrial, especialidad en Electricidad, especialidad en Electrónica industrial. - Ingeniero Técnico de Telecomunicación, en todas sus especialidades.
	Sistemas Electrotécnicos y Automáticos	- Diplomado en Radioelectrónica Naval. - Ingeniero Técnico Aeronáutico, especialidad en Aeronavegación. - Ingeniero Técnico en Informática de Sistemas. - Ingeniero Técnico Industrial, especialidad en Electricidad, especialidad en Electrónica Industrial. - Ingeniero Técnico de Telecomunicación, en todas sus especialidades.

ANEXO III C)

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. 5029. Redes de comunicaciones industriales seguras. 5030 Análisis forense en ciberseguridad industrial. 5031. Seguridad integral.	– Licenciado, Ingeniero, Arquitecto o el título de grado correspondiente u otros títulos equivalentes. – Diplomado, Ingeniero Técnico, Arquitecto Técnico o el título de Grado correspondiente, u otros títulos equivalentes.

ANEXO III D)

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. 5029. Redes de comunicaciones industriales seguras. 5030. Análisis forense en ciberseguridad industrial. 5031. Seguridad integral.	– Licenciado, Ingeniero, Arquitecto o el título de grado correspondiente u otros títulos equivalentes. – Diplomado, Ingeniero Técnico, Arquitecto Técnico o el título de Grado correspondiente, u otros títulos equivalentes.