**PROYECTO DE DECRETO POR EL QUE SE ESTABLECE EL CURRÍCULO CORRESPONDIENTE AL CURSO DE ESPECIALIZACIÓN EN CIBERSEGURIDAD EN ENTORNOS DE LAS TECNOLOGÍAS DE LA INFORMACIÓN EN LA COMUNIDAD DE CASTILLA Y LEÓN.**

La Constitución Española reserva al Estado, en el artículo 149.1.30ª, la competencia exclusiva en materia de regulación de las condiciones de obtención, expedición y homologación de 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.

El Estatuto de Autonomía de Castilla y León, en el artículo 73.1, atribuye a la Comunidad de Castilla y León 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 la normativa estatal.

La Ley Orgánica 5/2002, de 19 de junio, de las Cualificaciones y de la Formación Profesional, tras su modificación por la Ley Orgánica 4/2011, de 11 de marzo, complementaria de la Ley de Economía Sostenible, establece en el artículo 10.3 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.

La Ley Orgánica 2/2006, de 3 de mayo, de Educación, tras su modificación por la Ley Orgánica 8/2013, de 9 de diciembre, para la mejora de la calidad educativa, establece en el artículo 6.bis.4 que, en relación con la formación profesional, el Gobierno fijará los objetivos, competencias, contenidos, resultados de aprendizaje y criterios de evaluación del currículo básico, y en el artículo 39.6 que el Gobierno establecerá las titulaciones correspondientes a los estudios de formación profesional, así como los aspectos básicos del currículo de cada una de ellas.

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 el artículo 27 los cursos de especialización, e indica los requisitos y condiciones a que deben ajustarse dichos cursos de especialización. En el mismo artículo se indica que versarán sobre aspectos y 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 ello, en cada curso de especialización se deben especificar los títulos de formación profesional que dan acceso al mismo.

Asimismo, el artículo 9 del citado real decreto, establece la estructura de los cursos de especialización, y en el artículo 7 se recoge los elementos que definen el perfil profesional de cada enseñanza, que incluirá la competencia general que podrá estar referida al Catálogo Nacional de Cualificaciones Profesionales, las competencias profesionales, personales y sociales, las cualificaciones profesionales y, en su caso, las unidades de competencia, cuando se refieran al Catálogo Nacional de Cualificaciones Profesionales. Por otro lado, el artículo 8.2, dispone que las Administraciones educativas

establecerán los currículos correspondientes respetando lo en él dispuesto y en las normas que regulen las diferentes enseñanzas de formación profesional.

Mediante Real Decreto 479/2020, de 7 de abril, se establece el Curso de especialización en ciberseguridad en entornos de las tecnologías de la información y se fijan los aspectos básicos del currículo.

El presente decreto establece el currículo correspondiente al Curso de especialización en ciberseguridad en entornos de las tecnologías de la información en la Comunidad de Castilla y León, teniendo en cuenta los principios que han de orientar la actividad educativa según lo previsto en el artículo 1 de la Ley Orgánica 2/2006, de 3 de mayo, y pretende dar respuesta a las necesidades generales de cualificación de las personas.

El diseño del currículo de este curso de especialización garantiza el ejercicio real y efectivo de derechos por parte de las personas con discapacidad en igualdad de condiciones, previsto en la disposición final segunda 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, y el principio de igualdad de oportunidades previsto en la Ley Orgánica 3/2007, de 22 de marzo, para la igualdad efectiva de mujeres y hombres. .

Esta norma se ajusta a los principios de buena regulación previstos en el artículo 129 de la Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas. De acuerdo con los principios de necesidad y eficacia, este decreto se dicta en atención al cumplimiento y desarrollo de la normativa estatal básica y viene motivado por una razón de interés general al ser el objetivo básico del currículo 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 que dan acceso a este curso de especialización, avanzando en la integración de la formación profesional a las actuales necesidades de formación de personal cuya competencia general consiste en definir e implementar estrategias de seguridad en los sistemas de información 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, de acuerdo con el desarrollo económico y social de Castilla y León.

En relación con el principio de proporcionalidad este decreto contiene la regulación imprescindible para atender la necesidad que el interés general requiere y es acorde con el sistema constitucional de distribución de competencias puesto que, una vez aprobado por la Administración General del Estado un determinado curso de especialización y el currículo básico, compete a la Administración educativa autonómica el establecimiento de un currículo propio para Castilla y León en los términos determinados en la norma estatal y de acuerdo con el porcentaje de configuración autonómica en ella determinado. Asimismo, esta regulación responde a una de las acciones incluidas en el programa operativo 19/L4 del Plan General de Formación Profesional contenido en la II Estrategia Integrada de Empleo, Formación Profesional, Prevención de Riesgos Laborales e Igualdad y Conciliación

en el Empleo, 2016-2020, aprobada por Acuerdo del Consejo del Diálogo Social de Castilla y León autorizado el 27 de enero de 2016 por la Junta de Castilla y León, que consiste en la puesta en marcha de cursos especializados que faciliten la transición desde la formación, al empleo, de acuerdo con lo que establezca la normativa básica para titulados de Formación Profesional Inicial.

A fin de garantizar el principio de seguridad jurídica este decreto se ha elaborado de manera coherente con el resto del ordenamiento jurídico, fundamentalmente con la normativa estatal básica en la materia.

En relación con el principio de eficiencia ha de ponerse de manifiesto que la aprobación de este decreto no impone nuevas cargas administrativas y su aplicación supondrá una correcta racionalización de los recursos públicos.

El principio de transparencia se ha cumplido en la tramitación del decreto a través del Portal de Gobierno Abierto de la Junta de Castilla y León, de conformidad con lo previsto en el artículo 76 en relación con el artículo 75 de la Ley 3/2001, del Gobierno y de la Administración de la Comunidad de Castilla y León, así como del artículo 133 de la Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas, respecto de los trámites de consulta pública previa y de audiencia e información pública, y del artículo 16 de la Ley 3/2015, de 4 de marzo, de Transparencia y Participación Ciudadana de Castilla y León, respecto del trámite de participación ciudadana.

Por otro lado, en la elaboración de este decreto se ha contado con la colaboración de profesorado de las especialidades con atribución docente en los módulos profesionales del Curso de especialización en ciberseguridad en entornos de las tecnologías de la información de los centros educativos de Castilla y León. Asimismo se ha recabado dictamen del Consejo Escolar de Castilla y León de conformidad con el artículo 8.1.a) de la Ley 3/1999, de 17 de marzo, del Consejo Escolar de Castilla y León, e informe del Consejo de Formación Profesional de Castilla y León de conformidad con el artículo 2.g) del Decreto 82/2000, de 27 de abril, de creación de este Consejo.

En su virtud, la Junta de Castilla y León, a propuesta de la Consejera de Educación, de acuerdo con el dictamen del Consejo Consultivo de Castilla y León, y previa deliberación del Consejo de Gobierno en su reunión de

**DISPONE**

**Artículo 1.** *Objeto y ámbito de aplicación.*

1. El presente decreto tiene por objeto establecer el currículo correspondiente al Curso de especialización en ciberseguridad en entornos de las tecnologías de la información en la Comunidad de Castilla y León.

2. Será de aplicación en los centros públicos y privados de la Comunidad de Castilla y León que, cumpliendo con los requisitos establecidos en el Real Decreto 479/2020, de 7 de abril, por el que se establece el Curso de especialización en ciberseguridad en entornos

de las tecnologías de la información y se fijan los aspectos básicos del currículo, estén debidamente autorizados e impartan este curso de especialización.

**Artículo 2.** *Identificación del curso de especialización.*

El Curso de especialización en Ciberseguridad en entornos de las tecnologías de la información queda identificado en la Comunidad de Castilla y León por los elementos determinados en el artículo 2 del Real Decreto 479/2020, de 7 de abril, y por un código, de la forma siguiente:

DENOMINACIÓN: Ciberseguridad en entornos de las tecnologías de la información.
NIVEL: Formación Profesional de Grado Superior.
DURACIÓN: 720 horas.
FAMILIA PROFESIONAL: Informática y Comunicaciones (Únicamente a efectos de clasificación de las enseñanzas de formación profesional).
RAMAS DE CONOCIMIENTO: Ingeniería y Arquitectura.
CRÉDITOS ECTS: 43.
REFERENTE EUROPEO: P-5.5.4. (Clasificación Internacional Normalizada de la Educación).
CÓDIGO: IFC01E.

**Artículo 3.** *Acceso al curso de especialización y referentes de formación.*

1. Los títulos que dan acceso a la realización del Curso de especialización en ciberseguridad en entornos de las tecnologías de la información son los establecidos en el artículo 13 del Real Decreto 479/2020, de 7 de abril, cuyos currículos se encuentran implantados en la Comunidad de Castilla y León a través de los siguientes decretos:

a) Decreto 33/2010, de 26 de agosto, por el que se establece el currículo correspondiente al título de Técnico Superior en Administración de Sistemas Informáticos en Red en la Comunidad de Castilla y León.
b) Decreto 23/2011, de 9 de junio, por el que se establece el currículo correspondiente al título de Técnico Superior en Desarrollo de Aplicaciones Multiplataforma en la Comunidad de Castilla y León.
c) Decreto 43/2011, de 14 de julio, por el que se establece el currículo correspondiente al título de Técnico Superior en Desarrollo de Aplicaciones Web en la Comunidad de Castilla y León.
d) Decreto 45/2013, de 31 de julio, por el que se establece el currículo correspondiente al título de Técnico Superior en Sistemas de Telecomunicaciones e Informáticos en la Comunidad de Castilla y León.
e) Decreto 48/2013, de 31 de julio, por el que se establece el currículo correspondiente al título de Técnico Superior en Mantenimiento Electrónico en la Comunidad de Castilla y León.

2. El currículo del Curso de especialización en ciberseguridad en entornos de las tecnologías de la información en la Comunidad de Castilla y León tomará como referentes de formación los aspectos relativos al perfil profesional del curso determinado por la

competencia general y las competencias profesionales, personales y sociales, así como los aspectos referentes al entorno profesional y a la prospectiva del curso en el sector o sectores, establecidos en los artículos 4 a 7 del Real Decreto 479/2020, de 7 de abril.

**Artículo 4.** *Módulos profesionales del curso de especialización.*

Los módulos profesionales que componen el Curso de especialización en ciberseguridad en entornos de las tecnologías de la información serán los establecidos en el artículo 9 del Real Decreto 479/2020, de 7 de abril, que se indican a continuación:

5021. Incidentes de ciberseguridad.
5022. Bastionado de redes y sistemas.
5023. Puesta en producción segura.
5024. Análisis forense informático.
5025. Hacking ético.
5026. Normativa de ciberseguridad.

**Artículo 5.** *Objetivos, duración, contenidos, y orientaciones pedagógicas y metodológicas de cada módulo profesional.*

1. Los objetivos de los módulos profesionales relacionados en el artículo 4, expresados en términos de resultados de aprendizaje, y los criterios de evaluación, son los que se establecen en el anexo I del Real Decreto 479/2020, de 7 de abril.

2. Por su parte, la duración, los contenidos y las orientaciones pedagógicas y metodológicas de los módulos profesionales relacionados en el artículo 4 son los que se establecen en el anexo de este decreto.

**Artículo 6.** *Organización.*

Los módulos profesionales que forman las enseñanzas del Curso de especialización en ciberseguridad en entornos de las tecnologías de la información cuando se oferten en régimen presencial, se organizan en un curso académico.

**Artículo 7.** *Metodología.*

1. La metodología didáctica aplicada al Curso de especialización en ciberseguridad en entornos de las tecnologías de la información integrará los aspectos científicos, tecnológicos y organizativos que en cada caso correspondan, con el fin de que el alumnado adquiera una visión global de los procesos productivos propios de la actividad profesional.

2. En el desarrollo de las enseñanzas correspondientes al curso de especialización se deben aplicar metodologías activas de aprendizaje que favorezcan:

a) La participación, implicación y compromiso del alumnado en las tareas y su resolución de una manera creativa, innovadora y autónoma, estimulando su motivación.

b) La realización de proyectos o actividades coordinadas en los que intervengan diferentes módulos interrelacionando aquellos que permitan completar las competencias profesionales del curso de especialización.
c) La evaluación de las actitudes que el profesorado considere imprescindibles para el desempeño de una profesión y la integración en una sociedad cívica y ética.
d) La adquisición de competencias, tanto técnicas asociadas a los módulos profesionales que configuran el curso, como interpersonales o sociales (competencia digital, trabajo colaborativo, en equipo o cooperativo, otros).
e) El desarrollo de trabajos en el aula que versen sobre actividades que supongan al alumnado el ensayo de rutinas y destrezas de pensamiento y ejecución de tareas que simulen el ambiente real de trabajo en torno al perfil profesional del título, apoyándose en un aprendizaje basado en proyectos, retos o la resolución de problemas complejos que estimulen al alumnado.
f) La comprobación del nivel adquirido por el alumnado en las competencias asociadas al módulo profesional cursado, mediante la elaboración de pruebas con un componente práctico que evidencie dicho desempeño profesional.

**Artículo 8.** *Requisitos de los centros para impartir el curso de especialización.*

Todos los centros de titularidad pública o privada que oferten el Curso de especialización en ciberseguridad en entornos de las tecnologías de la información se ajustarán a lo establecido en la Ley Orgánica 2/2006, de 3 de mayo, de Educación y en las normas que la desarrollen, y en todo caso deberán cumplir los requisitos que se establecen en el artículo 46 del Real Decreto 1147/2011, de 29 de julio, por el que se establece la ordenación general de la formación profesional del sistema educativo, en el Real Decreto 479/2020, de 7 de abril, y en lo establecido en la normativa que los desarrolle.

**Artículo 9.** *Profesorado.*

Los aspectos referentes al profesorado con atribución docente en los módulos profesionales del curso de especialización, relacionados en el artículo 4, son los establecidos en el artículo 11 del Real Decreto 479/2020, de 7 de abril.

**Artículo 10.** *Espacios y equipamientos.*

Los espacios y los equipamientos necesarios para el desarrollo de las enseñanzas de este curso de especialización son los establecidos en el artículo 10 del Real Decreto 479/2020, de 7 de abril.

**Artículo 11.** *Vinculación a otros estudios.*

La vinculación a otros estudios son los que se establecen en el artículo 14 del Real Decreto 479/2020, de 7 de abril.

**Artículo 12.** *Autonomía de los centros.*

1. Los centros educativos dispondrán de la necesaria autonomía pedagógica, de organización y de gestión económica, para el desarrollo de las enseñanzas del Curso de especialización en ciberseguridad en entornos de las tecnologías de la información, y su adaptación a las características concretas del entorno socioeconómico, cultural y profesional.

2. Los centros autorizados para impartir estas enseñanzas concretarán y desarrollarán el currículo mediante las programaciones didácticas de cada uno de los módulos profesionales que componen el curso de especialización en los términos establecidos en el Real Decreto 479/2020, de 7 de abril, en este decreto, en el marco general del proyecto educativo de centro y en función de las características de su entorno productivo.

Las programaciones didácticas incluirán, al menos, los aspectos siguientes:

a) Las competencias profesionales asociadas, las capacidades profesionales u objetivos expresados en resultados de aprendizaje, contenidos y criterios de evaluación establecidos en el currículo de la Comunidad de Castilla y León para el curso de especialización.
b) La distribución temporal de los contenidos en el curso de especialización.
c) La metodología didáctica que se va a aplicar.
d) Los procedimientos de evaluación del aprendizaje del alumnado, recogiendo las actuaciones que se llevarán a cabo para evaluar los resultados de aprendizaje y los criterios de calificación de los módulos y el procedimiento y plazos a seguir para la presentación y tramitación de reclamaciones.
e) El número máximo de faltas de asistencia no justificadas o las actividades no realizadas que determinarán la imposibilidad de aplicar la evaluación continua y el procedimiento a seguir para la evaluación del alumnado en estos casos.
f) Los materiales y recursos didácticos que se vayan a utilizar, así como las referencias bibliográficas que se necesiten.
g) Las actividades complementarias y extraescolares que, en su caso, se pretendan realizar.
h) Las medidas necesarias que garanticen la atención a la diversidad para el alumnado que las precisen.
i) La planificación de las actividades de recuperación de los módulos profesionales pendientes de superación, y expresamente aquellas que puedan ser realizables de forma autónoma por el alumnado.
j) La utilización de las tecnologías de la información y comunicación (TIC) en la actividad docente.

3. La consejería competente en materia de educación favorecerá la elaboración de proyectos de innovación, así como de modelos de programación docente y de materiales didácticos que faciliten al profesorado el desarrollo del currículo.

4. De conformidad con el artículo 120.4 de la Ley Orgánica 2/2006, de 3 de mayo, los centros, en el ejercicio de su autonomía, podrán adoptar experimentaciones, planes de

trabajo, formas de organización, normas de convivencia y ampliación del calendario escolar o del horario lectivo de áreas o materias, en los términos que establezca la consejería competente en materia de educación y dentro de las posibilidades que permita la normativa aplicable, incluida la laboral, sin que, en ningún caso, se impongan aportaciones a las familias ni exigencias para la citada consejería.

**Artículo 13.** *Enseñanzas impartidas en lenguas extranjeras.*

1. Teniendo en cuenta que la promoción de la enseñanza y el aprendizaje de lenguas debe de constituir una prioridad de la acción comunitaria en el ámbito de la educación y la formación, la consejería competente en materia de educación podrá autorizar que todos o determinados módulos profesionales del currículo se impartan en lenguas extranjeras.

2. Los centros autorizados deberán incluir en su proyecto educativo los elementos más significativos de su proyecto lingüístico autorizado.

3. En todo caso, se exigirá al profesorado que imparta enseñanzas en lenguas extranjeras que acredite el dominio de las competencias correspondientes, al menos, al nivel B2 del Marco Común Europeo de Referencia para las lenguas.

**Artículo 14.** *Oferta a distancia del curso de especialización.*

1. Los módulos profesionales que forman las enseñanzas del curso de especialización, podrán ofertarse a distancia, siempre que se garantice que el alumnado puede conseguir los resultados de aprendizaje de los mismos, de acuerdo con lo dispuesto en el Real Decreto 479/2020, de 7 de abril, y en este decreto.

2. La consejería competente en materia de educación establecerá los módulos profesionales susceptibles de ser impartidos a distancia y el porcentaje de horas de cada uno de ellos que tienen que impartirse en régimen presencial.

## DISPOSICIÓN ADICIONAL

*Calendario de implantación.*

El currículo establecido en este decreto se podrá implantar a partir del curso escolar 2020/2021.

## DISPOSICIONES FINALES

**Primera.** *Desarrollo normativo.*

Se faculta al titular de la consejería competente en materia de educación para dictar cuantas disposiciones sean precisas para la interpretación, aplicación y desarrollo de lo dispuesto en este decreto.

**Segunda.** *Entrada en vigor.*

El presente decreto entrará en vigor a los veinte días de su publicación en el "Boletín Oficial de Castilla y León".

Valladolid, a 31 de julio de 2020

EL DIRECTOR GENERAL DE FORMACIÓN PROFESIONAL,
RÉGIMEN ESPECIAL Y EQUIDAD EDUCATIVA

Agustín Francisco Sigüenza Molina

ANEXO

**Objetivos, contenidos, duración y orientaciones pedagógicas y metodológicas de los módulos profesionales**

**Módulo profesional: Incidentes de ciberseguridad.**
**Equivalencia en créditos ECTS: 9.**
**Código: 5021**

*Duración: 144 horas.*

*Contenidos:*

1. Desarrollo de planes de prevención y concienciación en ciberseguridad:

- Principios generales en materia de ciberseguridad.
- Normativa de protección del puesto del trabajo.
- Plan de formación y concienciación en materia de ciberseguridad.
- Materiales de formación y concienciación.
- Auditorías internas de cumplimiento en materia de prevención.

2. Auditoría de incidentes de ciberseguridad:

- Taxonomía de incidentes de ciberseguridad.
- Controles, herramientas y mecanismos de monitorización, identificación, detección y alerta de incidentes: tipos y fuentes.
- Controles, herramientas y mecanismos de detección e identificación de incidentes de seguridad física.
- Controles, herramientas y mecanismos de monitorización, identificación, detección y alerta de incidentes a través de la investigación en fuentes abiertas (OSINT).
- Clasificación, valoración, documentación, seguimiento inicial de incidentes de ciberseguridad.

3. Investigación de los incidentes de ciberseguridad:

- Recopilación de evidencias.
- Análisis de evidencias.
- Investigación del incidente
- Intercambio de información del incidente con proveedores u organismos competentes.
- Medidas de contención de incidentes.

4. Implementación de medidas de ciberseguridad:

- Desarrollar procedimientos de actuación detallados para dar respuesta, mitigar, eliminar o contener los tipos de incidentes.
- Implantar capacidades de ciberresiliencia.
- Establecer flujos de toma de decisiones y escalado interno y/o externo adecuados.
- Tareas para reestablecer los servicios afectados por incidentes.
- Documentación.
- Seguimiento de incidentes para evitar una situación similar.

5. Detección y documentación de incidentes de ciberseguridad:

- Desarrollar procedimientos de actuación para la notificación de incidentes.
- Notificación interna de incidentes.
- Notificación de incidentes a quienes corresponda.

*Orientaciones pedagógicas y metodológicas.*

Este módulo profesional contiene la formación necesaria para desempeñar las funciones de análisis, detección y respuesta a los incidentes de ciberseguridad de la organización.

La función de análisis y detección de incidentes de ciberseguridad incluye aspectos como la monitorización de los sistemas para la recopilación de evidencias que permita dar una respuesta adecuada a los incidentes detectados.

Las actividades profesionales asociadas a esta función se aplican mediante la instalación y configuración de las herramientas necesarias para hacer frente a los ciberataques.

La formación del módulo contribuye a alcanzar los objetivos generales a), b), c), d), q), r), s), t), u) y v) y las competencias a), b), k), l), m), n) y ñ) del curso de especialización, recogidos en los artículos 8 y 5, respectivamente, del Real Decreto 479/2020, de 7 de abril.

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

- La elaboración de planes de prevención y concienciación de ciberseguridad.
- La detección de incidentes mediante distintas herramientas de monitorización.
- La implantación de las medidas necesarias para responder a los incidentes detectados.
- Identificación de la normativa nacional e internacional aplicable en la organización.
- La notificación de incidentes tanto interna como externa, si procede, mediante los procedimientos adecuados.

**Módulo profesional: Bastionado de redes y sistemas**
**Equivalencia en créditos ECTS: 10**
**Código: 5022.**

*Duración: 171 horas.*

*Contenidos:*

1. Diseño de planes de securización:

   - Análisis de riesgos.
   - Principios de la Economía Circular en la Industria 4.0.
   - Plan de medidas técnicas de seguridad.
   - Políticas de securización más habituales.
   - Guías de buenas prácticas para la securización de sistemas y redes.

- Estándares de securización de sistemas y redes.
- Caracterización de procedimientos, instrucciones y recomendaciones.
- Niveles, escalados y protocolos de atención a incidencias.

2. Configuración de sistemas de control de acceso y autenticación de personas:

   - Mecanismos de autenticación. Tipos de factores.
   - Autenticación basada en distintas técnicas.

3. Administración de credenciales de acceso a sistemas informáticos:

   - Gestión de credenciales.
   - Infraestucturas de Clave Pública (PKI).
   - Acceso por medio de Firma electrónica.
   - Gestión de accesos. Sistemas NAC (Network Access Control, Sistemas de Gestión de Acceso a la Red).
   - Gestión de cuentas privilegiadas.
   - Protocolos RADIUS y TACACS, servicio KERBEROS, entre otros.

4. Diseño de redes de computadores seguras:

   - Segmentación de redes.
   - Subnetting.
   - Redes virtuales (VLANs).
   - Zona desmilitarizada (DMZ).
   - Seguridad en redes inalámbricas (WPA2, WPA3, etc.).
   - Protocolos de red seguros (IPSec, etc.).

5. Configuración de dispositivos y sistemas informáticos:

   - Seguridad perimetral. Firewalls de Próxima Generación.
   - Seguridad de portales y aplicativos web. Soluciones WAF (Web Aplication Firewall).
   - Seguridad del puesto de trabajo y endpoint fijo y móvil. AntiAPT, antimalware.
   - Seguridad de entornos cloud. Soluciones CASB.
   - Seguridad del correo electrónico
   - Soluciones DLP (Data Loss Prevention)
   - Herramientas de almacenamiento de logs.
   - Protección ante ataques de denegación de servicio distribuido (DDoS).
   - Configuración segura de cortafuegos, enrutadores y proxies.
   - Redes privadas virtuales (VPNs), y túneles (protocolo IPSec).
   - Monitorización de sistemas y dispositivos.
   - Herramientas de monitorización (IDS, IPS).
   - SIEMs (Gestores de Eventos e Información de Seguridad).
   - Soluciones de Centros de Operación de Red, y Centros de Seguridad de Red: NOCs y SOCs.

6. Configuración de dispositivos para la instalación de sistemas informático:

   - Precauciones previas a la instalación de un sistema informático: aislamiento, configuración del control de acceso a la BIOS, bloqueo del orden de arranque de los dispositivos, entre otros.
   - Seguridad en el arranque del sistema informático, configuración del arranque seguro.
   - Seguridad de los sistemas de ficheros, cifrado, particionado, entre otros.

7. Configuración de los sistemas informáticos:

   - Reducción del número de servicios, Telnet, RSSH, TFTP, entre otros.
   - Hardening de procesos (eliminación de información de depuración en caso de errores, aleatorización de la memoria virtual para evitar exploits, etc.).
   - Eliminación de protocolos de red innecesarios (ICMP, entre otros).
   - Securización de los sistemas de administración remota.
   - Sistemas de prevención y protección frente a virus e intrusiones (antivirus, HIDS, etc.).
   - Configuración de actualizaciones y parches automáticos.
   - Sistemas de copias de seguridad.
   - Shadow IT y políticas de seguridad en entornos SaaS.

*Orientaciones pedagógicas y metodológicas.*

Este módulo profesional contiene la formación necesaria para desempeñar la función de bastionado de los sistemas y redes de la organización.

La función de bastionado incluye aspectos como la administración de los sistemas y redes contemplando la normativa, tanto a nivel nacional como internacional, de ciberseguridad en vigor.

Las actividades profesionales asociadas a esta función se aplican en el diseño de planes de securización y en el diseño de las redes contemplando los requisitos de seguridad que apliquen a la organización

La formación del módulo contribuye a alcanzar los objetivos generales e), f), g), h), i), j), q), r), s), t), u) y v) y las competencias c), d), e), k), l), m), n) y ñ) del curso de especialización, recogidos en los artículos 8 y 5, respectivamente, del Real Decreto 479/2020, de 7 de abril.

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

- El diseño de planes de securización de la organización.
- El diseño de redes de computadores.
- La administración de los sistemas de control de acces

**Módulo profesional: Puesta en producción segura**
**Equivalencia en créditos ECTS: 7**
**Código: 5023.**

*Duración: 117 horas.*

*Contenidos:*

1. Prueba de aplicaciones *web* y para dispositivos móviles:

   - Fundamentos de la programación.
   - Lenguajes de programación interpretados y compilados.
   - Código fuente y entornos de desarrollo.
   - Ejecución de software.
   - Elementos principales de los programas.
   - Pruebas. Tipos.
   - Seguridad en los lenguajes de programación y sus entornos de ejecución ("sandboxes").

2. Determinación del nivel de seguridad requerido por aplicaciones:

   - Fuentes abiertas para el desarrollo seguro.
   - Listas de riesgos de seguridad habituales: OWASP Top Ten (web y móvil).
   - Requisitos de verificación necesarios asociados al nivel de seguridad establecido.
   - Comprobaciones de seguridad a nivel de aplicación: ASVS (Application Security Verification Standard).

3. Detección y corrección de vulnerabilidades de aplicaciones web:

   - Desarrollo seguro de aplicaciones web.
   - Listas públicas de vulnerabilidades de aplicaciones web. OWASP Top Ten.
   - Entrada basada en formularios. Inyección. Validación de la entrada.
   - Estándares de autenticación y autorización.
   - Robo de sesión.
   - Vulnerabilidades web.
   - Almacenamiento seguro de contraseñas.
   - Contramedidas. HSTS, CSP, CAPTCHAs, entre otros.
   - Seguridad de portales y aplicativos web. Soluciones WAF (Web Application Firewall)

4. Detección de problemas de seguridad en aplicaciones para dispositivos móviles:

   - Modelos de permisos en plataformas móviles. Llamadas al sistema protegidas.
   - Firma y verificación de aplicaciones.
   - Almacenamiento seguro de datos.
   - Validación de compras integradas en la aplicación.
   - Fuga de información en los ejecutables.
   - Soluciones CASB.

5. Implantación de sistemas seguros de desplegado de software:

   - Puesta segura en producción.
   - Prácticas unificadas para el desarrollo y operación del software (DevOps).
   - Sistemas de control de versiones.
   - Sistemas de automatización de construcción (build).
   - Integración continua y automatización de pruebas.
   - Escalado de servidores. Virtualización. Contenedores.
   - Gestión automatizada de configuración de sistemas
   - Herramientas de simulación de fallos.
   - Orquestación de contenedores

*Orientaciones pedagógicas y metodológicas.*

Este módulo profesional contiene la formación necesaria para desempeñar la función de puesta en producción mediante el desarrollo de un sistema de despliegue de software seguro.

La función de implantación de un sistema de despliegue seguro incluye aspectos como la monitorización de aplicaciones y dispositivos para detectar los vectores de ataque más comunes.

Las actividades profesionales asociadas a esta función se aplican en el análisis de las aplicaciones web y dispositivos móviles así como en la configuración de servidores web.

La formación del módulo contribuye a alcanzar los objetivos generales k), l), q), r), s), t), u) y v) y las competencias f), g), k), l), m), n) y ñ) del curso de especialización, recogidos en los artículos 8 y 5, respectivamente, del Real Decreto 479/2020, de 7 de abril.

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

- El análisis de la estructura de aplicaciones y dispositivos móviles.
- Los vectores de ataque más comunes.
- El análisis del nivel de seguridad requerido por las aplicaciones.
- La configuración de servidores web seguros.
- La detección de los problemas de seguridad de las aplicaciones para los dispositivos móviles.
- La implantación de sistemas seguros de desplegado de software.

**Módulo profesional: Análisis forense informático.**
**Equivalencia en créditos ECTS: 7**
**Código: 5024.**

*Duración: 117 horas.*

*Contenidos:*

1. Aplicación de metodologías de análisis forenses:

- Identificación de los dispositivos a analizar.
- Recolección de evidencias (trabajar un escenario).
- Análisis de la línea de tiempo (TimeStamp).
- Análisis de volatilidad – Extracción de información (Volatility).
- Análisis de Logs, herramientas más usadas.

2. Realización de análisis forenses en dispositivos móviles:

   - Métodos para la extracción de evidencias.
   - Herramientas de mercado más comunes.

3. Realización de análisis forenses en Cloud:

   - Nube privada y nube pública o híbrida.
   - Retos legales, organizativos y técnicos particulares de un análisis en Cloud.
   - Estrategias de análisis forense en Cloud.
   - Realizar las fases relevantes del análisis forense en Cloud.
   - Utilizar herramientas de análisis en Cloud (Cellebrite UFED Cloud Analizer, Cloud Trail, Frost, OWADE, …).

4. Realización de análisis forenses en IoT:

   - Identificar los dispositivos a analizar.
   - Adquirir y extraer las evidencias.
   - Analizar las evidencias de manera manual y automática.
   - Documentar el proceso realizado.
   - Establecer la línea temporal.
   - Mantener la cadena de custodia.
   - Elaborar las conclusiones.
   - Presentar y exponer las conclusiones.

5. Documentación y elaboración de informes de análisis forenses. Apartados de los que se compone el informe:

   - Hoja de identificación (título, razón social, nombre y apellidos, firma).
   - Índice de la memoria.
   - Objeto (objetivo del informe pericial y su justificación).
   - Alcance (ámbito de aplicación del informe pericial - resumen ejecutivo para una supervisión rápida del contenido y resultados).
   - Antecedentes (aspectos necesarios para la comprensión de las alternativas estudiadas y las conclusiones finales).
   - Normas y referencias (documentos y normas legales y reglamentos citados en los distintos apartados).
   - Definiciones y abreviaturas (definiciones, abreviaturas y expresiones técnicas que se han utilizado a lo largo del informe).
   - Requisitos (bases y datos de partida establecidos por el cliente, la legislación, reglamentación y normativa aplicables).
   - Análisis de soluciones – resumen de conclusiones del informe pericial (alternativas estudiadas, qué caminos se han seguido para llegar a ellas, ventajas e inconvenientes de cada una y cuál es la solución finalmente elegida y su justificación).
   - Anexos.

*Orientaciones pedagógicas y metodológicas.*

Este módulo profesional contiene la formación necesaria para desempeñar la función de análisis forense.

La función de análisis forense incluye aspectos como el análisis de dispositivos de almacenamiento no volátil, de ficheros Logs, dispositivos móviles, Cloud e IoT.

Las actividades profesionales asociadas a esta función se aplican en la extracción de las evidencias para su análisis mediante la estrategia adecuada que garantice la disponibilidad de los recursos.

La formación del módulo contribuye a alcanzar los objetivos generales m), n), q), r), s), t), u) y v) y las competencias h), k), l), m), n) y ñ) del curso de especialización, recogidos en los artículos 8 y 5, respectivamente, del Real Decreto 479/2020, de 7 de abril.

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

- Las metodologías de análisis forense.
- Las herramientas de análisis forense.
- La toma de evidencias.
- El análisis de resultados.
- Los informes de resultados.
- Las fases del análisis Cloud y herramientas para llevarlo a cabo.
- La estrategia de análisis forense en IoT.

**Módulo profesional: Hacking ético.**
**Equivalencia en créditos ECTS: 7**
**Código: 5025.**

*Duración: 117 horas.*

*Contenidos:*

1. Determinación de las herramientas de monitorización para detectar vulnerabilidades:

    - Elementos esenciales del hacking ético.
    - Diferencias entre hacking, hacking ético, tests de penetración y hacktivismo.
    - Recolección de permisos y autorizaciones previos a un test de intrusión.
    - Fases del hacking.
    - Auditorías de caja negra y de caja blanca.
    - Documentación de vulnerabilidades.
    - Clasificación de herramientas de seguridad y hacking.
    - ClearNet, Deep Web, Dark Web, Darknets. Conocimiento, diferencias y herramientas de acceso: Tor. ZeroNet, FreeNet.

2. Ataque y defensa en entorno de pruebas, de las comunicaciones inalámbricas:

   - Comunicación inalámbrica.
   - Modo infraestructura, ad-hoc y monitor.
   - Análisis y recolección de datos en redes inalámbricas.
   - Técnicas de ataques y exploración de redes inalámbricas.
   - Ataques a otros sistemas inalámbricos.
   - Realización de informes de auditoría y presentación de resultados.

3. Ataque y defensa en entorno de pruebas, de redes y sistemas para acceder a sistemas de terceros:

   - Fase de reconocimiento (footprinting).
   - Fase de escaneo (fingerprinting).
   - Monitorizacion de tráfico.
   - Interceptación de comunicaciones utilizando distintas técnicas.
   - Manipulación e inyección de tráfico.
   - Herramientas de búsqueda y explotación de vulnerabilidades.
   - Ingeniería social. Phising.
   - Escalada de privilegios.

4. Consolidación y utilización de sistemas comprometidos:

   - Administración de sistemas de manera remota.
   - Ataques y auditorías de contraseñas.
   - Pivotaje en la red.
   - Instalación de puertas traseras con troyanos (RAT, Remote Access Trojan).

5. Ataque y defensa en entorno de pruebas, a aplicaciones web:

   - Negación de credenciales en aplicaciones web.
   - Recolección de información.
   - Automatización de conexiones a servidores web (ejemplo: Selenium).
   - Análisis de tráfico a través de proxies de intercepción.
   - Búsqueda de vulnerabilidades habituales en aplicaciones web.
   - Herramientas para la explotación de vulnerabilidades web.

*Orientaciones pedagógicas y metodológicas.*

Este módulo profesional contiene la formación necesaria para desempeñar la función de detectar las vulnerabilidades de la organización mediante *hacking* ético.

La función de *hacking* incluye aspectos como el ataque programado a las redes y a las aplicaciones *web* de la organización.

Las actividades profesionales asociadas a esta función se aplican en el ataque de las redes de comunicaciones para acceder a datos o funcionalidades no autorizadas con el propósito de encontrar vulnerabilidades

La formación del módulo contribuye a alcanzar los objetivos generales ñ), q), r), s), t), u) y v) y las competencias i), k), l), m), n) y ñ) del curso de especialización, recogidos en los artículos 8 y 5, respectivamente, del Real Decreto 479/2020, de 7 de abril.

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

- Los objetivos y las fases del hacking ético.
- Las herramientas de seguridad y hacking.
- La administración remota de sistemas.
- El ataque ético a redes de comunicaciones, a sistemas y a las aplicaciones web.

**Módulo profesional: Normativa de ciberseguridad.**
**Equivalencia en créditos ECTS: 3**
**Código: 5026.**

*Duración: 54 horas.*

*Contenidos:*

1. Puntos principales de aplicación para un correcto cumplimiento normativo:

   - Introducción al cumplimiento normativo (Compliance: objetivo, definición y conceptos principales).
   - Principios del buen gobierno y ética empresarial.
   - Compliance Officer: funciones y responsabilidades.
   - Relaciones con terceras partes dentro del Compliance.

2. Diseño de sistemas de cumplimiento normativo:

   - Sistemas de Gestión de Compliance.
   - Entorno regulatorio de aplicación.
   - Análisis y gestión de riesgos, mapas de riesgos.
   - Documentación del sistema de cumplimiento normativo diseñado.

3. Legislación para el cumplimiento de la responsabilidad penal:

   - Riesgos penales que afectan a la organización.
   - Sistemas de gestión de Compliance penal.
   - Sistemas de gestión anticorrupción.

4. Legislación y jurisprudencia en materia de protección de datos:

   - Principios de protección de datos.
   - Novedades del RGPD de la Unión Europea.
   - Privacidad por Diseño y por Defecto.
   - Análisis de Impacto en Privacidad (PIA), y medidas de seguridad.
   - Delegado de Protección de Datos (DPO).

5. Normativa vigente de ciberseguridad de ámbito nacional e internacional:

   - Normas nacionales e internacionales.
   - Sistema de Gestión de Seguridad de la Información (estándares internacionales) (ISO 27.001).
   - Acceso electrónico de los ciudadanos a los Servicios Públicos.

6. Esquema Nacional de Seguridad (ENS).

   - Planes de Continuidad de Negocio (estándares internacionales) (ISO 22.301).
   - Directiva NIS.
   - Legislación sobre la protección de infraestructuras críticas.

7. Ley PIC (Protección de infraestructuras críticas).

*Orientaciones pedagógicas y metodológicas.*

Este módulo profesional contiene la formación necesaria para desempeñar la función de diseñar el sistema de cumplimiento normativo de ciberseguridad en una organización.

La función de diseñar un sistema de cumplimiento normativo incluye aspectos como la caracterización de los principales aspectos de las diferentes normativas de ciberseguridad de obligado cumplimiento para la organización.

Las actividades profesionales asociadas a esta función se aplican en la integración, de las últimas actualizaciones en normativa de ciberseguridad a nivel nacional e internacional que apliquen, en el sistema de cumplimiento normativo de la organización.

La formación del módulo contribuye a alcanzar los objetivos generales o), p), q), r), s), t), u) y v) y las competencias j), k), l), m), n) y ñ) del curso de especialización, recogidos en los artículos 8 y 5, respectivamente, del Real Decreto 479/2020, de 7 de abril.

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

- La identificación de los cambios de la normativa de ciberseguridad, tanto nacional como internacional, que afectan a la organización.
- La elaboración de mapas de riesgos.
- La elaboración de materiales de formación y concienciación como presentaciones, guías, etc.
- La investigación de incidentes de ciberseguridad.
- La legislación y jurisprudencia en materia de protección de datos de carácter personal.
- La notificación, tanto interna como externa de los incidentes detectados.