Comunidad de Madrid

N.º Y AÑO DEL EXPEDIENTE
2021

REFERENCIA
NÚMERO

CONSEJERÍA DE EDUCACIÓN, UNIVERSIDADES, CIENCIA Y PORTAVOCÍA.

Proyecto de decreto del Consejo de Gobierno, por el que se establece para la Comunidad de Madrid el plan de estudios del curso de especialización de formación profesional en ciberseguridad en entornos de las tecnologías de la información.

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. Por su parte, el artículo 6 bis, apartado 1.c) de la Ley Orgánica 2/2006, de 3 de mayo, establece, en relación con la formación profesional, que el Gobierno fijará las enseñanzas mínimas.

La Ley Orgánica 5/2002, de 19 de junio, de las Cualificaciones y de la Formación Profesional, define en su artículo 9 la formación profesional como el conjunto de las acciones formativas que capacitan para el desempeño cualificado de las diversas profesiones, el acceso al empleo y la participación activa en la vida social, cultural y económica. Asimismo, en el apartado 1 de su artículo 10 establece que la Administración General del Estado, de conformidad con lo establecido en el artículo 149.1.30ª y 7ª de la Constitución Española y previa consulta al Consejo General de la Formación Profesional, determinará los títulos, los certificados de profesionalidad y demás ofertas formativas que constituirán las ofertas de formación profesional referidas al Catálogo Nacional de Cualificaciones Profesionales y en el apartado 2 del citado artículo determina que las Administraciones educativas, en el ámbito de sus competencias, podrán ampliar los contenidos de los correspondientes títulos de formación profesional.

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, podrá crear cursos de especialización para completar las competencias de quienes dispongan de un título de formación profesional. 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.

El Real Decreto 1147/2011, de 29 de julio, por el que se establece la ordenación general de la formación profesional del sistema educativo, dispone en su artículo 8 que sean las Administraciones educativas las que, respetando lo previsto en dicha norma y en aquellas que regulan las diferentes enseñanzas de formación profesional, establezcan los correspondientes currículos.

D E C I S I Ó N

El citado real decreto, regula, asimismo, en su artículo 27 los cursos de especialización de formación profesional y establece los requisitos y condiciones a que deben ajustarse dichas enseñanzas. En el mismo artículo se indica que estos cursos de especialización tendrán por objeto complementar las competencias de quienes ya dispongan de un título de formación profesional y facilitar el aprendizaje a lo largo de la vida y que versarán sobre los 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.

En cumplimiento, asimismo, de lo establecido en el artículo 23.5 del Decreto 63/2019, de 16 de julio, del Consejo de Gobierno, por el que se regula la ordenación y organización de la formación profesional en la Comunidad de Madrid, esta desarrollará los planes de estudios correspondientes a los cursos de especialización que se establezcan en disposiciones estatales y se adecúen a los sectores productivos y a las demandas laborales de la región.

El Gobierno ha aprobado 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. El plan de estudios de dicho curso, que se establece en este decreto, que se dicta de conformidad con lo establecido en los artículos 8 y 23 del Decreto 63/2019, de 16 de julio, pretende complementar las competencias de quienes ya dispongan de un título de formación profesional y atender a las necesidades formativas de las nuevas cualificaciones, con objeto de mejorar la empleabilidad de las personas y la competitividad de las empresas. Este curso de especialización supondrá una formación complementaria que permitirá profundizar y ampliar o, en su caso, especializarse en el ámbito de la ciberseguridad en el entorno de las tecnologías de la información. En consecuencia, el presente decreto tiene como objeto determinar y concretar los elementos curriculares que definen el plan de estudios correspondiente al Curso de especialización en ciberseguridad en entornos de las tecnologías de la información para que pueda ser impartido en los centros educativos, públicos y privados, de la Comunidad de Madrid, debidamente autorizados para ello. Asimismo, concreta las especialidades y titulaciones requeridas al profesorado y los requisitos en cuanto a los espacios y equipamientos mínimos deben reunir los centros para impartir esta formación.

Dicho plan de estudios requiere una posterior concreción del currículo en las programaciones didácticas en los términos que recoge el artículo 32 del citado Decreto 63/2019, de 16 de julio.

Por otra parte, el diseño del plan de estudios de este curso de especialización garantiza el ejercicio real y efectivo de derechos por parte de las personas con discapacidad en igualdad de condiciones con respecto al resto de la ciudadanía, así como el derecho a la igualdad de oportunidades y de trato, conforme previene el 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. Asimismo, hace efectivo el derecho de igualdad de oportunidades y de trato entre mujeres y hombres en cualquier ámbito de la vida, como dispone el artículo 1 de la Ley Orgánica 3/2007, de 22 de marzo, para la igualdad efectiva de mujeres y hombres, y garantiza la integración del principio de igualdad y no discriminación por razón de identidad de género o expresión de género, dando cumplimiento a lo que establece la Ley 3/2016, de 22 de

julio, de Protección Integral contra la LGTBIfobia y la Discriminación por Razón de Orientación e Identidad Sexual en la Comunidad de Madrid y la Ley 2/2016, de 29 de marzo, de Identidad y Expresión de Género e Igualdad Social y no Discriminación de la Comunidad de Madrid.

En el marco de lo dispuesto en el artículo 129 de la Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas, la presente disposición normativa se ajusta a las exigencias de los principios de necesidad y eficacia, puesto que desarrolla y completa el currículo básico de esta formación para que pueda ser impartida en el ámbito de la Comunidad de Madrid, sin que se acuda para ello a normas supletorias del Estado en esta materia, con el fin de mejorar la cualificación y formación de los ciudadanos y ofrecer mayores oportunidades de empleo en el sector productivo de la ciberseguridad, respondiendo a las demandas de cualificación de los profesionales en dicho sector. La norma no se extralimita en sus disposiciones respecto a lo establecido en el Real Decreto 479/2020, de 7 de abril, atiende a la necesidad originada de mejorar la cualificación y formación de los ciudadanos con respeto a lo establecido en la norma básica, y cumple con el principio de proporcionalidad establecido. Por otro lado, el rango de esta disposición responde a la importancia de la materia que regula, relacionada con el derecho a la educación y el desarrollo de sus bases. El cumplimiento de estos principios contribuye, además, a lograr un ordenamiento autonómico sólido y coherente en materia curricular que garantiza los principios de seguridad jurídica. Asimismo, se cumple con el principio de eficiencia al evitar cargas administrativas innecesarias o accesorias y establecer los requisitos que deben reunir los centros de forma que se facilita la racionalización de la gestión de los recursos públicos. También se cumple el principio de transparencia, conforme a lo establecido en la Ley 10/2019, de 10 de abril, de Transparencia y de Participación de la Comunidad de Madrid, así como se ha dado cumplimiento a los trámites de audiencia e información públicas a través del Portal de Transparencia de la Comunidad de Madrid, conforme a lo dispuesto en el artículo 26.6 de la Ley 50/1997, de 27 de noviembre, del Gobierno.

Asimismo, se ha emitido dictamen por el Consejo Escolar de la Comunidad de Madrid, y se han recabado los informes relativos al impacto por razón de género que se estima positivo, el impacto sobre la familia, la infancia y la adolescencia que se concluye no genera, así como en relación con el impacto por razón de orientación sexual e identidad de expresión de género que se estima positivo. Por otro lado, el presente decreto cuenta con el informe de Coordinación y Calidad Normativa, así como con los informes de la Dirección General de Presupuestos y la Dirección General de Recursos Humanos de la Consejería de Hacienda y Función Pública y el informe de la Abogacía General de la Comunidad de Madrid y de las secretarías generales técnicas de las diferentes consejerías.

De conformidad con el artículo 29 del Estatuto de Autonomía de la Comunidad de Madrid corresponde a la Comunidad Autónoma la competencia de desarrollo legislativo y ejecución de la enseñanza en toda su extensión, niveles y grados, modalidades y especialidades. El Consejo de Gobierno de la Comunidad de Madrid es competente para dictar el presente decreto, de acuerdo con lo establecido en el artículo 21.g) de la Ley 1/1983, de 13 de diciembre, de Gobierno y Administración de la Comunidad de Madrid.

En virtud de lo anterior, a propuesta del consejero de Educación, Universidades, Ciencia y Portavocía del Gobierno, oída/de acuerdo con la Comisión Jurídica Asesora de

la Comunidad de Madrid el Consejo de Gobierno, previa deliberación, en su reunión del día _____,

DISPONE

Artículo 1. *Objeto y ámbito de aplicación.*

1. El presente decreto establece el currículo de las enseñanzas de formación profesional correspondientes al curso de especialización de formación profesional en ciberseguridad en el entorno de las tecnologías de la información así como las especialidades y titulaciones requeridas al profesorado que las imparte y los requisitos en cuanto a espacios y equipamientos necesarios que deben reunir los centros.

2. Esta norma será de aplicación en los centros públicos y privados de la Comunidad de Madrid que, debidamente autorizados, impartan estas enseñanzas.

Artículo 2. *Referentes de la formación.*

Los aspectos relativos a la identificación del curso de especialización, el perfil y el entorno profesional, las competencias, la prospectiva del curso de especialización en el sector, los objetivos generales, los accesos y la vinculación con otros estudios son los que se definen 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.

Artículo 3. *Módulos profesionales del ciclo formativo.*

Los módulos profesionales que constituyen el currículo del curso de especialización en ciberseguridad, son los siguientes:

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 4. *Currículo.*

1. La contribución a la competencia general y a las competencias profesionales, personales y sociales, los objetivos expresados en términos de resultados de aprendizaje, los criterios de evaluación y las orientaciones pedagógicas del currículo del curso de especialización para los módulos profesionales relacionados en el artículo 3 son los definidos en el Real Decreto 479/2020, de 7 de abril.

2. Los contenidos y duración de los módulos profesionales impartidos en el centro educativo, relacionados en el artículo 3, se incluyen en el anexo I.

Artículo 5*. Adaptación al entorno educativo, social y productivo.*

1. Los centros educativos concretarán y desarrollarán el currículo de este curso de especialización mediante programaciones didácticas, en el contexto del proyecto educativo del centro.

2. Las programaciones didácticas se establecerán teniendo en cuenta las características socioeconómicas del sector y potenciarán la cultura de calidad, la excelencia en el trabajo, así como la formación en materia de prevención de riesgos laborales y de respeto medioambiental, atendiendo a la normativa específica del sector productivo o de servicios correspondiente.

3. Tanto en los procesos de enseñanza y de aprendizaje como en la realización de las actividades que desarrollen las programaciones didácticas se integrará el principio de igualdad de oportunidades entre mujeres y hombres y la prevención de la violencia de género, el respeto y la no discriminación por motivos de orientación sexual y diversidad sexual e identidad o expresión de género.

4. Los centros desarrollarán el currículo establecido en este decreto integrando el principio de «diseño universal o diseño para todas las personas». En las programaciones didácticas se tendrán en consideración las características del alumnado, con especial atención a las necesidades de quienes presenten una discapacidad reconocida, para facilitar el acceso al currículo y la adquisición de las competencias incluidas en el mismo y la evaluación.

Artículo 6. *Organización y distribución horaria.*

1. Los módulos profesionales de este curso de especialización en ciberseguridad en entornos de las tecnologías y la información se impartirán dentro del calendario escolar establecido para cada curso académico.

2. Los centros docentes organizarán el desarrollo de las actividades formativas con una duración de un curso académico y podrán establecer un calendario de evaluaciones parciales similar al correspondiente al primer curso de los ciclos formativos de formación profesional, que en todo caso quedará reflejado en la programación didáctica de estas enseñanzas. Para ello se seguirá el cuadro de distribución horaria que se recoge en el anexo II.

3. Asimismo, con el fin de ofrecer la formación de manera secuencial, los centros podrán organizar la impartición de determinados módulos profesionales por trimestres o cuatrimestres, dentro del calendario escolar establecido para las enseñanzas de formación profesional. En todo caso se garantizará el cumplimiento de la duración asignada a cada módulo profesional.

Artículo 7. *Enseñanza semipresencial.*

1. Los centros podrán organizar estas enseñanzas dentro del régimen a distancia en modalidad semipresencial. Su organización y distribución horaria se recogerá en la programación didáctica y se atendrá a lo siguiente:

a) En el módulo profesional Incidentes en ciberseguridad (código 5021) se programarán, al menos, 50 horas con actividades presenciales, en las 30 horas restantes podrán programarse actividades a distancia.

b) El módulo profesional Bastionado de redes y sistemas (código 5022) se programarán, al menos, 165 horas con actividades presenciales, en las 15 horas restantes podrán programarse actividades a distancia.

c) El módulo profesional Puesta en producción segura (código 5023) será impartido de forma presencial en su totalidad.

d) El módulo profesional Análisis forense informático (código 5024) se programarán, al menos, 125 horas con actividades presenciales, en las 15 horas restantes podrán programarse actividades a distancia.

e) El módulo profesional *Hacking* ético (código 5025) será impartido de forma presencial en su totalidad.

f) En el módulo profesional Normativa de ciberseguridad (código 5026) se programarán al menos 20 horas con actividades presenciales, en las 20 horas restantes podrán programarse actividades a distancia.

2. La asistencia a las actividades presenciales será obligatoria para los alumnos. Las actividades que se programen a distancia contarán con el soporte de una plataforma virtual y su seguimiento se llevará a cabo mediante, al menos, una tutoría lectiva semanal por cada módulo profesional, que deberá impartirse durante el período que duren las actividades a distancia.

3. Sin perjuicio de lo recogido en los apartados anteriores las actividades formativas se impartirán dentro del calendario escolar establecido para cada curso académico y se programarán con una duración de un curso académico.

Artículo 8. *Profesorado.*

1. Las especialidades del profesorado de los cuerpos de Catedráticos de Enseñanza Secundaria, de Profesores de Enseñanza Secundaria y de Profesores Técnicos de Formación Profesional, así como del profesorado especialista, según proceda, con atribución docente en los módulos profesionales relacionados en el artículo 3 son las establecidas en el anexo III A) del Real Decreto 479/2020, de 7 de abril, o las titulaciones equivalentes a efectos de docencia establecidas en el anexo III B) del mismo real decreto.

2. Las titulaciones requeridas y habilitantes a efectos de docencia para el profesorado de los centros de titularidad privada o de titularidad pública de otras administraciones distintas de la educativa para impartir docencia en los módulos profesionales relacionados en el artículo 3 son las que se concretan en el anexo III C) del Real Decreto 479/2020, de 7 de abril. En todo caso, se exigirá que las enseñanzas conducentes a las titulaciones citadas engloben los objetivos de los módulos profesionales.

Si dichos objetivos no estuvieran incluidos en las enseñanzas conducentes a dichas titulaciones, además de ellas 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 con los resultados de aprendizaje.

3. Además de estas titulaciones requeridas, con las que el profesorado tendrá que acreditar una cualificación específica que garantice la capacitación adecuada para impartir el currículo de los módulos profesionales, se deberá acreditar la formación pedagógica y didáctica necesaria para ejercer la docencia, según se establece en el artículo 100 de la Ley Orgánica 2/2006, de 3 de mayo, de Educación.

4. En todos aquellos aspectos no contemplados en los apartados anteriores, se estará a lo dispuesto en el artículo 11 del Real Decreto 479/2020, de 7 de abril.

Artículo 9. *Requisitos de los centros.*

Los espacios y equipamientos que deben reunir los centros educativos para permitir el desarrollo de las actividades de enseñanza del curso de especialización en ciberseguridad en entornos de las tecnologías de la información deberán ajustarse a lo dispuesto en el artículo 10 y en el anexo II del Real Decreto 479/2020, de 7 de abril. Asimismo, de conformidad con el artículo 12 del citado real decreto los centros docentes deberán impartir alguno de los títulos que dan acceso al curso de especialización para poder ser autorizados a ofertar esta formación.

Además, deberán cumplir la normativa sobre diseño para todos y accesibilidad universal, sobre prevención de riesgos laborales y seguridad y salud en el trabajo.

Artículo 10. *Requisitos de acceso al curso de especialización.*

Para acceder al curso de especialización en ciberseguridad en entornos de las tecnologías de la información es necesario estar en posesión de alguno de los siguientes títulos:

a) Técnico Superior en Administración de Sistemas Informáticos en Red.
b) Técnico Superior en Desarrollo de Aplicaciones Multiplataforma.
c) Técnico Superior en Desarrollo de Aplicaciones Web.
d) Técnico Superior en Sistemas de Telecomunicaciones e Informáticos.
e) Técnico Superior en Mantenimiento Electrónico.

Disposición final primera. *Implantación del nuevo currículo*.

Las enseñanzas que se determinan en el presente decreto se podrán implantar a partir del curso escolar 2021-2022.

Disposición final segunda. *Habilitación para el desarrollo normativo.*

Se autoriza al titular de la consejería competente en materia de Educación a dictar las disposiciones que sean precisas para el desarrollo y la aplicación de lo dispuesto en este decreto.

Disposición final tercera. *Entrada en vigor.*

El presente decreto entrará en vigor el día siguiente al de su publicación en el «Boletín Oficial de la Comunidad de Madrid».

EL CONSEJERO DE EDUCACIÓN, UNIVERSIDADES CIENCIA Y PORTAVOZ DEL GOBIERNO

LA PRESIDENTA DE LA COMUNIDAD DE MADRID

Fdo.: Enrique Ossorio Crespo

Fdo.: Isabel Díaz Ayuso

ANEXO I

Relación de los contenidos y duración de los módulos profesionales del currículo

01. Módulo Profesional: Incidentes de ciberseguridad
Código: 5021
Duración: 80 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: objetivos e importancia, elementos esenciales.
     - Planificación e implementación.
     - Monitorización y evaluación.
   - Materiales de formación y concienciación.
     - Identificar las necesidades de sensibilización con la ciberseguridad.
     - Detectar las debilidades.
     - Técnicas y herramientas para la formación y concienciación: carteles, alertas, correos electrónicos, sesiones y charlas específicas, entre otros.
     - Actividades para la evaluación del plan.
   - Auditorías internas de cumplimiento en materia de prevención.
   - Criptografía, certificados y firmas digitales:
     - Criptografía de clave sistémica y de clave privada.
     - Funciones resumen (Hash).
     - Infraestructura PKI.
     - Intercambio de Diffie-Hellman.
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: anticipación, resistencia, recuperación y evolución.

- 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. Protocolos de actuación.
   - Notificación de incidentes a quienes corresponda.
   - Computer Emergency Response Team (CERT/CSIRT). Equipos de respuesta ante emergencias informáticas:
     - Definición, antecedentes históricos, organización, objetivos. Ámbito de actuación.
     - CERT nacionales. Mecanismos de colaboración a nivel nacional e internacional.

02. Módulo Profesional: Bastionado de redes y sistemas.
Código: 5022
Duración: 210 horas.

Contenidos

1. Diseño de planes de securización:
   - Análisis de riesgos.
   - Principios de la Economía Circular en la Industria 4.0. Aplicación del internet de las cosas y análisis de datos para la optimización de los recursos y eficiencia de los sistemas.
   - Plan de medidas técnicas de seguridad.
   - Políticas de securización más habituales. Protocolos, reglamentos y vías de comunicación.
   - 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:
     - *Tokens* de contraseña única (OTP) y *Tokens* USB.
     - Tarjetas inteligentes.
     - Por correo electrónico, SMS y datos biométricos.
     - Certificados digitales.
     - Autenticación de dos factores (2FA).
     - Autenticación de múltiples factores (MFA).
     - Conmutación de circuitos y de paquetes.
3. Administración de credenciales de acceso a sistemas informáticos:
   - Creación de cuentas de acceso. Perfiles de usuarios, roles y perfiles. Configuración del acceso a los recursos: derechos y privilegios.
   - Gestión de credenciales.
   - Infraestucturas de Clave Pública (PKI).
   - Módulos de seguridad hardware (HSM). Niveles de seguridad. Clasificación según estándares (FIPS, ISO/IEC, etc).
   - 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 segura de dispositivos y sistemas informáticos:
   - Seguridad perimetral. Firewalls de Próxima Generación (FWNG):
     - Identificación de aplicaciones.
     - Vinculación del uso de la aplicación a la identidad del usuario con independencia de la IP.
     - Prevención de amenazas.
     - Simplificación de la administración de políticas.
   - 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. Protección frente spam, phising y malware. Herramientas para el encriptado del correo.
   - 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 segura de dispositivos para la instalación de sistemas informáticos:
   - 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 segura 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 (*Software as a Service*).

03. Módulo Profesional: Puesta en producción segura.
Código: 5023
Duración: 140 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. Interoperabilidad y normalización. Soporte técnico y mantenimiento.
   - 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. Ataque por fuerza bruta, *sniffing*, propagación en URL, servidores compartidos. Métodos de prevención.
   - Vulnerabilidades web.
   - Almacenamiento seguro de contraseñas. Gestores 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. Apps de almacenamiento seguro.
   - Validación de compras integradas en la aplicación. Configuración de restricciones en el dispositivo.
   - Fuga de información en los ejecutables. Confidencialidad, integridad y disponibilidad de la información.
   - Soluciones CASB (*Cloud Access Security Manager*).
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.

04. Módulo Profesional: Análisis forense informático.
Código: 5024
Duración: 110 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 (*Time Stamp*).
   - Análisis de volatilidad – Extracción de información (*Volatility*).
   - Análisis de *Logs*, herramientas más usadas.
2. Realización de análisis forenses en dispositivos móviles y otros:
   - Métodos y fases para la extracción de evidencias:
     - Preparación. Identificación de elementos físicos y aislamiento de señales externas.
     - Adquisición de elementos de hardware y software: manual (capturas de pantalla), lógica (copia de archivos y directorios) y física (copias bit a bit, tipos de memorias).
     - Gestión de evidencias. Cadena de custodia.
     - Examen: particiones, sistemas de archivos existentes y borrados
     - Análisis de archivos binarios ejecutables, sistemas de ficheros, espacio borrado, memoria y *backup*.
     - Datos de interés: caché del teclado, contraseñas y configuraciones, conectividad, calendario, mensajes de texto, contactos y llamadas, datos geográficos, imágenes, vídeos, entre otros.
     - Presentación. *Suites* forenses. Herramientas de mercado más comunes.
     - En dispositivos móviles y sistemas operativos de escritorio, discos SSD (malware y amenazas), dispositivos en red y aplicaciones.
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, entre otros).
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.

05. Módulo Profesional: *Hacking* ético.
Código: 5025
Duración: 140 horas.

Contenidos

1. Determinación de las herramientas de monitorización para detectar vulnerabilidades:
   - Elementos esenciales del *hacking* ético. Concepto de *hacking*. Tipos de ataques sobre un sistema.
   - Diferencias entre *hacking*, *hacking* ético, test de penetración y *hacktivismo*.
   - Recolección de permisos y autorizaciones previos a un test de intrusión.
   - Fases del hacking: reconocimiento (pasivo y activo), escanear, obtener acceso, mantener acceso, cubrir los pasos (*Covering Tracks*).
   - Auditorías de caja negra y de caja blanca.
   - Documentación de vulnerabilidades.
   - Clasificación de herramientas de seguridad y hacking.
   - *ClearNet, Deep Web, Dark Web, Dark Net*. Conocimiento, diferencias y herramientas de acceso: *Tor, ZeroNet, FreeNet*.
2. Ataque y defensa en entorno de pruebas, de las comunicaciones inalámbricas:
   - Comunicación inalámbrica.
     - Tipos de redes inalámbricas. Estándares.
     - Modos de autenticación con wifi.
     - Cifrados en entornos inalámbricos. Estándares y protocolos.
   - 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:
   - Estructura de un ataque y procedimiento. Metodología para un *pentest* ofensivo
   - Fase de reconocimiento (*footprinting*). Herramientas *footprinting* para realizar búsquedas.
   - Fase de escaneo (*fingerprinting*).
     - Escaneo de redes locales y direcciones IP.
     - Escaneo de puertos abiertos.
     - Escaneo de servidores.
     - Recolección de información en redes abiertas OSINT (*Open Source Intelligence*).
     - Uso y configuración de herramientas enfocadas a OSINT.
   - Monitorizacion de tráfico.
   - Interceptación de comunicaciones utilizando distintas técnicas.
   - Manipulación e inyección de tráfico.
   - Ataques en infraestructuras: envenenamiento y suplantación.
   - 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.

06. Módulo Profesional: Normativa en ciberseguridad.
Código: 5026
Duración: 40 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.
   - 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 Reglamento General de Protección de Datos 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, europeas 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 (*Security Network and Information System*).
   - Legislación sobre la protección de infraestructuras críticas.
   - Ley PIC (Protección de infraestructuras críticas).

ANEXO II

Organización académica y distribución horaria semanal

Familia profesional: **INFORMÁTICA Y COMUNICACIONES**					
Curso de especialización: **Ciberseguridad en entornos de las tecnologías y la información**					
Nivel: **Curso de especialización**		Duración: **720 horas**			Código: **IFCE01**
MÓDULOS PROFESIONALES					DISTRIBUCIÓN HORARIA
Clave	*Código*	*Denominación*	*Créditos ECTS*	*Duración del currículo (horas)*	*Carga lectiva semanal (horas/semana)*
01	5021	Incidentes de ciberseguridad	9	80	2
02	5022	Bastionado de redes y sistemas	10	210	6
03	5023	Puesta en producción segura	7	140	4
04	5024	Análisis forense informático	7	110	3
05	5025	*Hacking* ético	7	140	4
06	5026	Normativa de ciberseguridad	3	40	1
		TOTALES	**43**	**720**	**20**