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

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

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

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

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

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

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

Habiendo entrado en vigor el Real Decreto 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, procede establecer el currículo del curso de especialización en Ciberseguridad en entornos de las tecnologías de la información, en el ámbito territorial de esta Comunidad Autónoma, teniendo en cuenta los aspectos definidos en la normativa citada anteriormente.

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

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

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

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

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

Artículo 1. Objeto.

El decreto tiene como objeto establecer el currículo del curso de especialización de Formación Profesional en Ciberseguridad en entornos de las tecnologías de la información, en el ámbito territorial de la Comunidad Autónoma de Castilla-La Mancha, teniendo en cuenta sus características geográficas, socio-productivas, laborales y educativas, complementando lo dispuesto en el Real Decreto 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 2. Identificación.

De acuerdo con lo establecido en el artículo 2 del Real Decreto 479/2020, de 7 de abril, el curso de especialización de Formación Profesional en Ciberseguridad en entornos de las tecnologías de la información, queda identificado por los siguientes elementos:

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).

Rama de conocimiento: Ingeniería y Arquitectura.
Créditos ECTS: 43.
Referente en la Clasificación Internacional Normalizada de la Educación: P-5.5.4.

Artículo 3. Requisitos de acceso al curso de especialización.

De acuerdo con lo establecido en el artículo 13 del Real Decreto 479/2020, de 7 de abril, 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 establecido por el Real Decreto 1629/2009, de 30 de octubre, por el que se establece el título de Técnico Superior en Administración de Sistemas Informáticos en Red y se fijan sus enseñanzas mínimas.
b) Técnico Superior en Desarrollo de Aplicaciones Multiplataforma, establecido por el Real Decreto 450/2010, de 16 de abril, por el que se establece el título de Técnico Superior en Desarrollo de Aplicaciones Multiplataforma y se fijan sus enseñanzas mínimas.
c) Técnico Superior en Desarrollo de Aplicaciones *Web*, establecido por el Real Decreto 686/2010, de 20 de mayo, por el que se establece el título de Técnico Superior en Desarrollo de Aplicaciones *Web* y se fijan sus enseñanzas mínimas.
d) Técnico Superior en Sistemas de Telecomunicaciones e Informáticos, establecido por el Real Decreto 883/2011, de 24 de junio, por el que se establece el título de Técnico Superior en Sistemas de Telecomunicaciones e Informáticos y se fijan sus enseñanzas mínimas.
e) Técnico Superior en Mantenimiento Electrónico, establecido por el Real Decreto 1578/2011, de 4 de noviembre, por el que se establece el Título de Técnico Superior en Mantenimiento Electrónico y se fijan sus enseñanzas mínimas.

Artículo 4. Referentes del curso de especialización.

En el Real Decreto 479/2020, de 7 de abril, quedan definidos el perfil profesional, la competencia general, las competencias profesionales, personales y sociales, entorno profesional, prospectiva en el sector o sectores, objetivos generales y accesos correspondientes al curso.

Artículo 5. Módulos profesionales: Duración y distribución horaria.

1. Módulos profesionales del curso de especialización:

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.

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

Artículo 6. Flexibilización de la oferta.

La Consejería con competencias en materia de educación podrá diseñar otras distribuciones horarias semanales de los módulos del curso de especialización distintas a las establecidas, encaminadas a la realización de una oferta más flexible y adecuada a la realidad social y

económica del entorno. En todo caso, se mantendrá la duración total establecida para cada módulo profesional.

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

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

2. Las orientaciones pedagógicas de los módulos profesionales que forman parte del título del curso de especialización en Formación Profesional Ciberseguridad en entornos de las tecnologías de la información son las establecidas en el anexo I del Real Decreto 479/2020, de 7 de abril.

Artículo 8. Profesorado.

1. La docencia de los módulos profesionales que constituyen las enseñanzas de este curso de especialización corresponde al profesorado del Cuerpo de Catedráticos de Enseñanza Secundaria, del Cuerpo de Profesores de Enseñanza Secundaria y del Cuerpo de Profesores Técnicos de Formación Profesional, según proceda, de las especialidades establecidas en el anexo III A) del Real Decreto 479/2020, de 7 de abril.

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

3. El profesorado especialista tendrá atribuida la competencia docente de los módulos profesionales especificados en el anexo III A) del Real Decreto 479/2020, de 7 de abril.

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

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

6. Para el profesorado de los centros de titularidad privada, de otras administraciones distintas de las educativas, las titulaciones requeridas y los requisitos necesarios para la impartición de los módulos profesionales que conforman el curso de especialización son las incluidas en el anexo III C) del Real Decreto 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 expresados en resultados de aprendizaje y, si dichos objetivos no estuvieran incluidos, además de la titulación deberá acreditarse, mediante certificación, una experiencia laboral de, al menos, tres años en el sector vinculado a la familia profesional,

realizando actividades productivas en empresas relacionadas implícitamente con los resultados de aprendizaje.

7. Para las titulaciones habilitantes a efectos de docencia, se atenderá a lo establecido en la disposición adicional tercera del Real Decreto 479/2020, de 7 de abril.

Artículo 9. Espacios y equipamientos.

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

2. Las condiciones de los espacios y equipamientos son las establecidas en el artículo 10 del Real Decreto 479/2020, de 7 de abril, que, en todo caso, deberán cumplir la normativa sobre igualdad de oportunidades, diseño para todos y accesibilidad universal, prevención de riesgos laborales y seguridad y salud en el puesto de trabajo.

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

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

Disposición adicional única. Autonomía pedagógica de los centros.

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

Disposición final primera. Implantación del currículo.

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

Disposición final segunda. Desarrollo.

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

Disposición final tercera. Entrada en vigor.

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

Dado en Toledo, el X de X de 2022

La Consejera de Educación, Cultura y Deportes

El Presidente

Rosa Ana Rodríguez Pérez

Emiliano García-Page Sánchez

ANEXO I

Duración de los módulos profesionales y la asignación horaria semanal

Módulos Profesionales	Horas totales	Distribución horaria semanal (Tres trimestres: 32 semanas)	Distribución horaria semanal (Dos trimestres: 24 semanas)
5021. Incidentes de ciberseguridad.	120	4	5
5022. Bastionado de redes y sistemas.	185	6	8
5023. Puesta en producción segura.	120	4	5
5024. Análisis forense informático.	120	4	5
5025. *Hacking* ético.	120	4	5
5026. Normativa de ciberseguridad.	55	2	2
	720	**24**	**30**

ANEXO II

Módulos Profesionales

Módulo Profesional: Incidentes de ciberseguridad.
Código: 5021.
Créditos ECTS: 9.

Resultados de aprendizaje y criterios de evaluación.

1. Desarrolla planes de prevención y concienciación en ciberseguridad, estableciendo normas y medidas de protección.

Criterios de evaluación:

a) Se han definido los principios generales de la organización en materia de ciberseguridad, que deben ser conocidos y apoyados por la dirección de la misma.
b) Se ha establecido una normativa de protección del puesto de trabajo.
c) Se ha definido un plan de concienciación de ciberseguridad dirigido a los empleados.
d) Se ha desarrollado el material necesario para llevar a cabo las acciones de concienciación dirigidas a los empleados.
e) Se ha realizado una auditoría para verificar el cumplimiento del plan de prevención y concienciación de la organización.

2. Analiza incidentes de ciberseguridad utilizando herramientas, mecanismos de detección y alertas de seguridad.

Criterios de evaluación:

a) Se ha clasificado y definido la taxonomía de incidentes de ciberseguridad que pueden afectar a la organización.
b) Se han establecido controles, herramientas y mecanismos de monitorización, identificación, detección y alerta de incidentes
c) Se han establecido controles y mecanismos de detección e identificación de incidentes de seguridad física.
d) Se han establecido controles, herramientas y mecanismos de monitorización, identificación, detección y alerta de incidentes a través de la investigación en fuentes abiertas (*OSINT: Open Source Intelligence*).
e) Se ha realizado una clasificación, valoración, documentación y seguimiento de los incidentes detectados dentro de la organización.

3. Investiga incidentes de ciberseguridad analizando los riesgos implicados y definiendo las posibles medidas a adoptar.

Criterios de evaluación:

a) Se han recopilado y almacenado de forma segura evidencias de incidentes de ciberseguridad que afectan a la organización.
b) Se ha realizado un análisis de evidencias.
c) Se ha realizado la investigación de incidentes de ciberseguridad.

d) Se ha intercambiado información de incidentes, con proveedores y/o organismos competentes que podrían hacer aportaciones al respecto.
e) Se han iniciado las primeras medidas de contención de los incidentes para limitar los posibles daños causados.

4. Implementa medidas de ciberseguridad en redes y sistemas respondiendo a los incidentes detectados y aplicando las técnicas de protección adecuadas.

Criterios de evaluación:

a) Se han desarrollado procedimientos de actuación detallados para dar respuesta, mitigar, eliminar o contener los tipos de incidentes de ciberseguridad más habituales.
b) Se han preparado respuestas ciberresilientes ante incidentes que permitan seguir prestando los servicios de la organización y fortaleciendo las capacidades de identificación, detección, prevención, contención, recuperación y cooperación con terceros.
c) Se ha establecido un flujo de toma de decisiones y escalado de incidentes interno y/o externo adecuados.
d) Se han llevado a cabo las tareas de restablecimiento de los servicios afectados por un incidente hasta confirmar la vuelta a la normalidad.
e) Se han documentado las acciones realizadas y las conclusiones que permitan mantener un registro de “lecciones aprendidas”.
f) Se ha realizado un seguimiento adecuado del incidente para evitar que una situación similar se vuelva a repetir.

5. Detecta y documenta incidentes de ciberseguridad siguiendo procedimientos de actuación establecidos.

Criterios de evaluación:

a) Se ha desarrollado un procedimiento de actuación detallado para la notificación de incidentes de ciberseguridad en los tiempos adecuados.
b) Se ha notificado el incidente de manera adecuada al personal interno de la organización responsable de la toma de decisiones.
c) Se ha notificado el incidente de manera adecuada a las autoridades competentes en el ámbito de la gestión de incidentes de ciberseguridad en caso de ser necesario.
d) Se ha notificado formalmente el incidente a los afectados, personal interno, clientes, proveedores, etc., en caso de ser necesario.
e) Se ha notificado el incidente a los medios de comunicación en caso de ser necesario.

Duración: 120 horas.
Contenidos:

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.

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.

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.

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.

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.

Módulo Profesional: Bastionado de redes y sistemas.
Código: 5022.
Créditos ECTS: 10.

Resultados de aprendizaje y criterios de evaluación.

1. Diseña planes de securización incorporando buenas prácticas para el bastionado de sistemas y redes.

Criterios de evaluación:

a) Se han identificado los activos, las amenazas y vulnerabilidades de la organización.
b) Se ha evaluado las medidas de seguridad actuales.
c) Se ha elaborado un análisis de riesgo de la situación actual en ciberseguridad de la organización
d) Se ha priorizado las medidas técnicas de seguridad a implantar en la organización teniendo también en cuenta los principios de la Economía Circular.
e) Se ha diseñado y elaborado un plan de medidas técnicas de seguridad a implantar en la organización, apropiadas para garantizar un nivel de seguridad adecuado en función de los riesgos de la organización.

f) Se han identificado las mejores prácticas en base a estándares, guías y políticas de securización adecuadas para el bastionado de los sistemas y redes de la organización.

2. Configura sistemas de control de acceso y autenticación de personas preservando la confidencialidad y privacidad de los datos.

Criterios de evaluación:

a) Se han definido los mecanismos de autenticación en base a distintos / múltiples factores (físicos, inherentes y basados en el conocimiento), existentes.
b) Se han definido protocolos y políticas de autenticación basados en contraseñas y frases de paso, en base a las principales vulnerabilidades y tipos de ataques.
c) Se han definido protocolos y políticas de autenticación basados en certificados digitales y tarjetas inteligentes, en base a las principales vulnerabilidades y tipos de ataques.
d) Se han definido protocolos y políticas de autenticación basados en *tokens, OTPs*, etc., en base a las principales vulnerabilidades y tipos de ataques.
e) Se han definido protocolos y políticas de autenticación basados en características biométricas, según las principales vulnerabilidades y tipos de ataques.

3. Administra credenciales de acceso a sistemas informáticos aplicando los requisitos de funcionamiento y seguridad establecidos.

Criterios de evaluación:

a) Se han identificado los tipos de credenciales más utilizados.
b) Se han generado y utilizado diferentes certificados digitales como medio de acceso a un servidor remoto.
c) Se ha comprobado la validez y la autenticidad de un certificado digital de un servicio *web*.
d) Se han comparado certificados digitales válidos e inválidos por diferentes motivos.
e) Se ha instalado y configurado un servidor seguro para la administración de credenciales (tipo *RADIUS - Remote Access Dial In User Service*).

4. Diseña redes de computadores contemplando los requisitos de seguridad.

Criterios de evaluación:

a) Se ha incrementado el nivel de seguridad de una red local plana segmentándola físicamente y utilizando técnicas y dispositivos de enrutamiento.
b) Se ha optimizado una red local plana utilizando técnicas de segmentación lógica (*VLANs*).
c) Se ha adaptado un segmento de una red local ya operativa utilizando técnicas de *subnetting* para incrementar su segmentación respetando los direccionamientos existentes.
d) Se han configurado las medidas de seguridad adecuadas en los dispositivos que dan acceso a una red inalámbrica (*routers*, puntos de acceso, etc.).
e) Se ha establecido un túnel seguro de comunicaciones entre dos sedes geográficamente separadas.

5. Configura dispositivos y sistemas informáticos cumpliendo los requisitos de seguridad.

Criterios de evaluación:

a) Se han configurado dispositivos de seguridad perimetral acorde a una serie de requisitos de seguridad.

b) Se han detectado errores de configuración de dispositivos de red mediante el análisis de tráfico.
c) Se han identificado comportamientos no deseados en una red a través del análisis de los registros (*Logs*), de un cortafuego.
d) Se han implementado contramedidas frente a comportamientos no deseados en una red.
e) Se han caracterizado, instalado y configurado diferentes herramientas de monitorización.

6. Configura dispositivos para la instalación de sistemas informáticos minimizando las probabilidades de exposición a ataques.

Criterios de evaluación:

a) Se ha configurado la *BIOS* para incrementar la seguridad del dispositivo y su contenido minimizando las probabilidades de exposición a ataques.
b) Se ha preparado un sistema informático para su primera instalación teniendo en cuenta las medidas de seguridad necesarias.
c) Se ha configurado un sistema informático para que un actor malicioso no pueda alterar la secuencia de arranque con fines de acceso ilegítimo.
d) Se ha instalado un sistema informático utilizando sus capacidades de cifrado del sistema de ficheros para evitar la extracción física de datos.
e) Se ha particionado el sistema de ficheros del sistema informático para minimizar riesgos de seguridad.

7. Configura sistemas informáticos minimizando las probabilidades de exposición a ataques.

Criterios de evaluación:

a) Se han enumerado y eliminado los programas, servicios y protocolos innecesarios que hayan sido instalados por defecto en el sistema.
b) Se han configurado las características propias del sistema informático para imposibilitar el acceso ilegítimo mediante técnicas de explotación de procesos.
c) Se ha incrementado la seguridad del sistema de administración remoto *SSH* y otros.
d) Se ha instalado y configurado un Sistema de detección de intrusos en un *Host* (*HIDS*) en el sistema informático.
e) Se han instalado y configurado sistemas de copias de seguridad.

Duración: 185 horas.
Contenidos:

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.

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

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

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.

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.).

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*.

Configuración 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/UEFI*, 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.

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*.

Módulo Profesional: Puesta en producción segura.
Código: 5023.
Créditos ECTS: 7.

Resultados de aprendizaje y criterios de evaluación.

1. Prueba aplicaciones *web* y aplicaciones para dispositivos móviles analizando la estructura del código y su modelo de ejecución.

Criterios de evaluación:

a) Se han comparado diferentes lenguajes de programación de acuerdo a sus características principales.
b) Se han descrito los diferentes modelos de ejecución de software.
c) Se han reconocido los elementos básicos del código fuente, dándoles significado.
d) Se han ejecutado diferentes tipos de prueba de software.
e) Se han evaluado los lenguajes de programación de acuerdo a la infraestructura de seguridad que proporcionan.

2. Determina el nivel de seguridad requerido por aplicaciones identificando los vectores de ataque habituales y sus riesgos asociados.

Criterios de evaluación:

a) Se han caracterizado los niveles de verificación de seguridad en aplicaciones establecidos por los estándares internacionales (*ASVS*, "*Application Security Verification Standard*").
b) Se ha identificado el nivel de verificación de seguridad requerido por las aplicaciones en función de sus riesgos de acuerdo a estándares reconocidos.
c) Se han enumerado los requisitos de verificación necesarios asociados al nivel de seguridad establecido.
d) Se han reconocido los principales riesgos de las aplicaciones desarrolladas, en función de sus características.

3. Detecta y corrige vulnerabilidades de aplicaciones *web* analizando su código fuente y configurando servidores *web*.

Criterios de evaluación:

a) Se han validado las entradas de los usuarios.
b) Se han detectado riesgos de inyección tanto en el servidor como en el cliente.
c) Se ha gestionado correctamente la sesión del usuario durante el uso de la aplicación.
d) Se ha hecho uso de roles para el control de acceso.
e) Se han utilizado algoritmos criptográficos seguros para almacenar las contraseñas de usuario.
f) Se han configurado servidores *web* para reducir el riesgo de sufrir ataques conocidos.
g) Se han incorporado medidas para evitar los ataques a contraseñas, envío masivo de mensajes o registros de usuarios a través de programas automáticos (*bots*).

4. Detecta problemas de seguridad en las aplicaciones para dispositivos móviles, monitorizando su ejecución y analizando ficheros y datos.

Criterios de evaluación:

a) Se han comparado los diferentes modelos de permisos de las plataformas móviles.
b) Se han descrito técnicas de almacenamiento seguro de datos en los dispositivos, para evitar la fuga de información.
c) Se ha implantado un sistema de validación de compras integradas en la aplicación haciendo uso de validación en el servidor.
d) Se han utilizado herramientas de monitorización de tráfico de red para detectar el uso de protocolos inseguros de comunicación de las aplicaciones móviles.
e) Se han inspeccionado binarios de aplicaciones móviles para buscar fugas de información sensible.

5. Implanta sistemas seguros de desplegado de software, utilizando herramientas para la automatización de la construcción de sus elementos.

Criterios de evaluación:

a) Se han identificado las características, principios y objetivos de la integración del desarrollo y operación del software.
b) Se han implantado sistemas de control de versiones, administrando los roles y permisos solicitados.
c) Se han instalado, configurado y verificado sistemas de integración continua, conectándolos con sistemas de control de versiones.
d) Se han planificado, implementado y automatizado planes de desplegado de software.
e) Se ha evaluado la capacidad del sistema desplegado para reaccionar de forma automática a fallos.
f) Se han documentado las tareas realizadas y los procedimientos a seguir para la recuperación ante desastres.
g) Se han creado bucles de retroalimentación ágiles entre los miembros del equipo.

Duración: 120 horas.
Contenidos:

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*”).

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).*

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*).

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.*

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.

Módulo Profesional: Análisis forense informático.
Código: 5024.
Créditos ECTS: 7.

Resultados de aprendizaje y criterios de evaluación.

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

Criterios de evaluación:

a) Se han identificado los dispositivos a analizar para garantizar la preservación de evidencias.
b) Se han utilizado los mecanismos y las herramientas adecuadas para la adquisición y extracción de las evidencias.
c) Se ha asegurado la escena y conservado la cadena de custodia.
d) Se ha documentado el proceso realizado de manera metódica.
e) Se ha considerado la línea temporal de las evidencias.
f) Se ha elaborado un informe de conclusiones a nivel técnico y ejecutivo.
g) Se han presentado y expuesto las conclusiones del análisis forense realizado.

2. Realiza análisis forenses en dispositivos móviles, aplicando metodologías establecidas, actualizadas y reconocidas.

Criterios de evaluación:

a) Se ha realizado el proceso de toma de evidencias en un dispositivo móvil.
b) Se han extraído, decodificado y analizado las pruebas conservando la cadena de custodia.
c) Se han generado informes de datos móviles, cumpliendo con los requisitos de la industria forense de telefonía móvil.
d) Se han presentado y expuesto las conclusiones del análisis forense realizado a quienes proceda.

3. Realiza análisis forenses en *Cloud*, aplicando metodologías establecidas, actualizadas y reconocidas.

Criterios de evaluación:

a) Se ha desarrollado una estrategia de análisis forense en *Cloud*, asegurando la disponibilidad de los recursos y capacidades necesarios una vez ocurrido el incidente.
b) Se ha conseguido identificar las causas, el alcance y el impacto real causado por el incidente.
c) Se han realizado las fases del análisis forense en *Cloud*.
d) Se han identificado las características intrínsecas de la nube (elasticidad, ubicuidad, abstracción, volatilidad y compartición de recursos).
e) Se han cumplido los requerimientos legales en vigor, RGPD (Reglamento general de protección de datos) y directiva *NIS* (Directiva de la UE sobre seguridad de redes y sistemas de información) o las que eventualmente pudieran sustituirlas.
f) Se han presentado y expuesto las conclusiones del análisis forense realizado.

4. Realiza análisis forense en dispositivos del *IoT*, aplicando metodologías establecidas, actualizadas y reconocidas.

Criterios de evaluación:

a) Se han identificado los dispositivos a analizar garantizando la preservación de las evidencias.
b) Se han utilizado mecanismos y herramientas adecuadas para la adquisición y extracción de evidencias
c) Se ha garantizado la autenticidad, completitud, fiabilidad y legalidad de las evidencias extraídas.
d) Se han realizado análisis de evidencias de manera manual y mediante herramientas.
e) Se ha documentado el proceso de manera metódica y detallada.
f) Se ha considerado la línea temporal de las evidencias.
g) Se ha mantenido la cadena de custodia
h) Se ha elaborado un informe de conclusiones a nivel técnico y ejecutivo.
i) Se han presentado y expuesto las conclusiones del análisis forense realizado.

5. Documenta análisis forenses elaborando informes que incluyan la normativa aplicable.

Criterios de evaluación:

a) Se ha definido el objetivo del informe pericial y su justificación.
b) Se ha definido el ámbito de aplicación del informe pericial.
c) Se han documentado los antecedentes.

d) Se han recopilado las normas legales y reglamentos cumplidos en el análisis forense realizado.
e) Se han recogido los requisitos establecidos por el cliente.
f) Se han incluido las conclusiones y su justificación.

Duración: 120 horas.
Contenidos:

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.

Realización de análisis forenses en dispositivos móviles:

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

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*, …).

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.

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.

Módulo Profesional: *Hacking* ético.
Código: 5025.
Créditos ECTS: 7.

Resultados de aprendizaje y criterios de evaluación.

1. Determina herramientas de monitorización para detectar vulnerabilidades aplicando técnicas de *hacking* ético.

Criterios de evaluación:

a) Se ha definido la terminología esencial del *hacking* ético.
b) Se han identificado los conceptos éticos y legales frente al ciberdelito.
c) Se ha definido el alcance y condiciones de un test de intrusión.
d) Se han identificado los elementos esenciales de seguridad: confidencialidad, autenticidad, integridad y disponibilidad.
e) Se han identificado las fases de un ataque seguidas por un atacante.
f) Se han analizado y definido los tipos vulnerabilidades.
g) Se han analizado y definido los tipos de ataque.
h) Se han determinado y caracterizado las diferentes vulnerabilidades existentes.
i) Se han determinado las herramientas de monitorización disponibles en el mercado adecuadas en función del tipo de organización.

2. Ataca y defiende en entornos de prueba, comunicaciones inalámbricas consiguiendo acceso a redes para demostrar sus vulnerabilidades.

Criterios de evaluación:

a) Se han configurado los distintos modos de funcionamiento de las tarjetas de red inalámbricas.
b) Se han descrito las técnicas de encriptación de las redes inalámbricas y sus puntos vulnerables.
c) Se han detectado redes inalámbricas y se ha capturado tráfico de red como paso previo a su ataque.
d) Se ha accedido a redes inalámbricas vulnerables.
e) Se han caracterizado otros sistemas de comunicación inalámbricos y sus vulnerabilidades.
f) Se han utilizado técnicas de “Equipo Rojo y Azul”.
g) Se han realizado informes sobre las vulnerabilidades detectadas.

3. Ataca y defiende en entornos de prueba, redes y sistemas consiguiendo acceso a información y sistemas de terceros.

Criterios de evaluación:

a) Se ha recopilado información sobre la red y sistemas objetivo mediante técnicas pasivas.

b) Se ha creado un inventario de equipos, cuentas de usuario y potenciales vulnerabilidades de la red y sistemas objetivo mediante técnicas activas.
c) Se ha interceptado tráfico de red de terceros para buscar información sensible.
d) Se ha realizado un ataque de intermediario, leyendo, insertando y modificando, a voluntad, el tráfico intercambiado por dos extremos remotos.
e) Se han comprometido sistemas remotos explotando sus vulnerabilidades.

4. Consolida y utiliza sistemas comprometidos garantizando accesos futuros.

Criterios de evaluación:

a) Se han administrado sistemas remotos a través de herramientas de línea de comandos.
b) Se han comprometido contraseñas a través de ataques de diccionario, tablas rainbow y fuerza bruta contra sus versiones encriptadas.
c) Se ha accedido a sistemas adicionales a través de sistemas comprometidos.
d) Se han instalado puertas traseras para garantizar accesos futuros a los sistemas comprometidos.

5. Ataca y defiende en entornos de prueba, aplicaciones *web* consiguiendo acceso a datos o funcionalidades no autorizadas.

Criterios de evaluación:

a) Se han identificado los distintos sistemas de autenticación *web*, destacando sus debilidades y fortalezas.
b) Se ha realizado un inventario de equipos, protocolos, servicios y sistemas operativos que proporcionan el servicio de una aplicación *web*.
c) Se ha analizado el flujo de las interacciones realizadas entre el navegador y la aplicación *web* durante su uso normal.
d) Se han examinado manualmente aplicaciones *web* en busca de las vulnerabilidades más habituales.
e) Se han usado herramientas de búsquedas y explotación de vulnerabilidades *web*.
f) Se ha realizado la búsqueda y explotación de vulnerabilidades *web* mediante herramientas software.

Duración: 120 horas.
Contenidos:

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*.

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.

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.

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*).

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*.

Módulo Profesional: Normativa de ciberseguridad.
Código: 5026.
Créditos ECTS: 3.

Resultados de aprendizaje y criterios de evaluación.

1. Identifica los puntos principales de aplicación para asegurar el cumplimiento normativo reconociendo funciones y responsabilidades.

Criterios de evaluación:

a) Se han identificado las bases del cumplimiento normativo a tener en cuenta en las organizaciones.
b) Se han descrito y aplicado los principios de un buen gobierno y su relación con la ética profesional.
c) Se han definido las políticas y procedimientos, así como la estructura organizativa que establezca la cultura del cumplimiento normativo dentro de las organizaciones.
d) Se han descrito las funciones o competencias del responsable del cumplimiento normativo dentro de las organizaciones.
e) Se han establecido las relaciones con terceros para un correcto cumplimiento normativo.

2. Diseña sistemas de cumplimiento normativo seleccionando la legislación y jurisprudencia de aplicación.

Criterios de evaluación:

a) Se han recogido las principales normativas que afectan a los diferentes tipos de organizaciones.
b) Se han establecido las recomendaciones válidas para diferentes tipos de organizaciones de acuerdo con la normativa vigente (*ISO* 19.600 entre otras).
c) Se han realizado análisis y evaluaciones de los riesgos de diferentes tipos de organizaciones de acuerdo con la normativa vigente (*ISO* 31.000 entre otras).
d) Se ha documentado el sistema de cumplimiento normativo diseñado.

3. Relaciona la normativa relevante para el cumplimiento de la responsabilidad penal de las organizaciones y personas jurídicas con los procedimientos establecidos, recopilando y aplicando las normas vigentes.

Criterios de evaluación:

a) Se han identificado los riesgos penales aplicables a diferentes organizaciones.
b) Se han implantado las medidas necesarias para eliminar o minimizar los riesgos identificados.
c) Se ha establecido un sistema de gestión de cumplimiento normativo penal de acuerdo con la legislación y normativa vigente (Código Penal y UNE 19.601, entre otros).
d) Se han determinado los principios básicos dentro de las organizaciones para combatir el soborno y promover una cultura empresarial ética de acuerdo con la legislación y normativa vigente (*ISO* 37.001 entre otros).

4. Aplica la legislación nacional de protección de datos de carácter personal, relacionando los procedimientos establecidos con las leyes vigentes y con la jurisprudencia existente sobre la materia.

Criterios de evaluación:

a) Se han reconocido las fuentes del Derecho de acuerdo con el ordenamiento jurídico en materia de protección de datos de carácter personal.
b) Se han aplicado los principios relacionados con la protección de datos de carácter personal tanto a nivel nacional como internacional.
c) Se han establecido los requisitos necesarios para afrontar la privacidad desde las bases del diseño.
d) Se han configurado las herramientas corporativas contemplando el cumplimiento normativo por defecto.
e) Se ha realizado un análisis de riesgos para el tratamiento de los derechos a la protección de datos.
f) Se han implantado las medidas necesarias para eliminar o minimizar los riesgos identificados en la protección de datos.
g) Se han descrito las funciones o competencias del delegado de protección de datos dentro de las organizaciones.

5. Recopila y aplica la normativa vigente de ciberseguridad de ámbito nacional e internacional, actualizando los procedimientos establecidos de acuerdo con las leyes y con la jurisprudencia existente sobre la materia.

Criterios de evaluación:

a) Se ha establecido el plan de revisiones de la normativa, jurisprudencia, notificaciones, etc. jurídicas que puedan afectar a la organización.
b) Se ha detectado nueva normativa consultando las bases de datos jurídicas siguiendo el plan de revisiones establecido.
c) Se ha analizado la nueva normativa para determinar si aplica a la actividad de la organización.
d) Se ha incluido en el plan de revisiones las modificaciones necesarias, sobre la nueva normativa aplicable a la organización, para un correcto cumplimiento normativo.
e) Se han determinado e implementado los controles necesarios para garantizar el correcto cumplimiento normativo de las nuevas normativas. incluidas en el plan de revisiones.

Duración: 55 horas.
Contenidos:

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*.

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.

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.

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).

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.

Esquema Nacional de Seguridad (ENS).

− Planes de Continuidad de Negocio (estándares internacionales) (*ISO* 22.301).
− Directiva *NIS*.

− Legislación sobre la protección de infraestructuras críticas. Ley PIC (Protección de infraestructuras críticas).

Anexo III

Espacios y equipamientos mínimos

Espacios:

Espacio formativo	Superficie m²	
	30 alumnos	20 alumnos
Aula técnica.	60	40
Laboratorio.	180	140
Aula polivalente.	60	40

Equipamientos:

Espacio formativo	Equipamientos mínimos
Aula técnica.	Ordenador profesor. Medios audiovisuales. Ordenadores alumnos. Sistemas de reprografía. Instalación de red con acceso a Internet. Software de control remoto Software básico (sistemas operativos en red). Software de aplicaciones ofimáticas, tratamiento de imágenes, entre otros. Software específico para virtualización, herramientas de monitorización basadas en protocolo snmp, herramientas de monitorización de servicios de alta disponibilidad, entre otros. Servidores de Ficheros, Web, Bases de datos y Aplicaciones. Herramientas de clonación de equipos. Cortafuegos, detectores de intrusos, aplicaciones de Internet, entre otras. Sistemas Gestores de Bases de Datos. Servidores y clientes. Entornos de desarrollo, compiladores e intérpretes, analizadores de código fuente, empaquetadores, generadores de ayudas, entre otros. Software específico para el análisis, monitorización y explotación de vulnerabilidades de redes y servicios. Software específico de diagnóstico, seguridad, antivirus entre otros.
Laboratorio.	Mesas de trabajo individuales tipo taller (80-90 cm alto). Bastidor (rack) para la instalación de servidores y dispositivos adicionales.

Espacio formativo	Equipamientos mínimos
	Ordenadores con sistema operativo de red y conexión a Internet. Software específico de diagnóstico, seguridad, antivirus y comunicaciones, entre otros. Sistemas de reprografía y escáner. Servidores con capacidad para virtualizar distintos escenarios, con las tecnologías más avanzadas. Sistemas de alimentación ininterrumpida. Medios audiovisuales. Cortafuegos Hardware con 8-12 puertos LAN, 2-4 puertos WAN, balanceo de carga, filtrado de contenidos, autenticación de usuarios, bloqueo de mensajería instantánea y de aplicaciones P2P, protección de negación del Servicio, conexión remota segura a través de VPN, entre otros. Puntos de acceso y dispositivos extraíbles de conexión a redes inalámbricas. Dispositivos móviles e *IoT*. Sistemas de control de acceso físico: lectores de DNI electrónico, tarjetas RFID (Identificación por radiofrecuencia), entre otros. Servidores de Ficheros, Web, Bases de datos y Aplicaciones. Sistemas Gestores de Bases de Datos. Servidores y clientes. Entornos de desarrollo, compiladores e intérpretes, analizadores de código fuente, control de versiones, empaquetadores, generadores de ayudas, entre otros. Sistemas de control de versiones. Simuladores de móviles e *IoT*. Software específico para el análisis, monitorización y explotación de vulnerabilidades de redes y servicios.
Aula polivalente.	Ordenador profesor. Medios audiovisuales. Ordenadores alumnos. Sistemas de reprografía. Instalación de red con acceso a Internet.