ANEXO I AL DECRETO XXX DE XXX DE 2021

CURSO DE ESPECIALIZACIÓN EN CIBERSEGURIDAD EN ENTORNOS DE LAS TECNOLOGÍAS DE LA INFORMACIÓN

1. Identificación.

Denominación: Ciberseguridad en Entornos de las Tecnologías de la Información.
Nivel: Formación Profesional de Grado Superior.
Duración: 990 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.

2. Acceso al Curso de Especialización.

Estar en posesión de alguno de los títulos siguientes o su equivalente a efectos académicos:

- Técnico Superior en Administración de Sistemas Informáticos en Red establecido por el Decreto 244/2010, de 21 de septiembre, por el que se establece el currículo correspondiente al título de Técnico Superior en Administración de Sistemas Informáticos en Red.
- Técnico Superior en Desarrollo de Aplicaciones Multiplataforma, establecido por el Decreto 207/2011, de 7 de octubre, por el que se establece el currículo correspondiente al título de Técnico Superior en Desarrollo de Aplicaciones Multiplataforma.
- Técnico Superior en Desarrollo de Aplicaciones Web, establecido por el Decreto 245/2011, de 29 de noviembre, por el que se establece el currículo correspondiente al título de Técnico Superior en Desarrollo de Aplicaciones Web.
- Técnico Superior en Sistemas de Telecomunicaciones e Informáticos, establecido por el Decreto 118/2012, de 3 de julio, por el que se establece el currículo correspondiente al título de Técnico Superior en Sistemas de Telecomunicaciones e Informáticos.
- Técnico Superior en Mantenimiento Electrónico, establecido por el Decreto 341/2013, de 22 de abril, por el que se establece el currículo correspondiente al título de Técnico Superior en Mantenimiento Electrónico.

3. Perfil profesional.

3.1. Competencia general:

La competencia general de este curso de especialización consiste en definir e implementar estrategias de seguridad en los sistemas de información realizando diagnósticos de ciberseguridad, identificando vulnerabilidades e implementando las medidas necesarias para mitigarlas aplicando la normativa vigente y estándares del sector, siguiendo los protocolos de calidad, de prevención de riesgos laborales y respeto

ambiental.

3.2. Entorno profesional:

Esta o este profesional ejercerá su actividad en entidades de los sectores donde sea necesario establecer mecanismos y medidas para la protección de los sistemas de información y redes de comunicaciones.

Las ocupaciones y puestos de trabajo más relevantes son los siguientes:

– Experta o Experto en ciberseguridad.
– Auditora o Auditor de ciberseguridad.
– Consultora o Consultor de ciberseguridad.
– Hacker ético.

3.3. Competencias profesionales, personales y sociales:

a) Elaborar e implementar planes de prevención y concienciación en ciberseguridad en la organización, aplicando la normativa vigente.

b) Detectar e investigar incidentes de ciberseguridad, documentándolos e incluyéndolos en los planes de securización de la organización.

c) Diseñar planes de securización contemplando las mejores prácticas para el bastionado de sistemas y redes.

d) Configurar sistemas de control de acceso y autenticación en sistemas informáticos, cumpliendo los requisitos de seguridad y minimizando las posibilidades de exposición a ataques.

e) Diseñar y administrar sistemas informáticos en red y aplicar las políticas de seguridad establecidas, garantizando la funcionalidad requerida con un nivel de riesgo controlado.

f) Analizar el nivel de seguridad requerido por las aplicaciones y los vectores de ataque más habituales, evitando incidentes de ciberseguridad.

g) Implantar sistemas seguros de desplegado de software con la adecuada coordinación entre los desarrolladores y los responsables de la operación del software.

h) Realizar análisis forenses informáticos analizando y registrando la información relevante relacionada.

i) Detectar vulnerabilidades en sistemas, redes, aplicaciones y sistemas de control en la industria, evaluando los riesgos asociados.

j) Coordinar el área de seguridad de TI y el área de automatización de la organización, aportando medidas para mejorar la seguridad de entornos industriales.

k) Implantar entornos básicos de automatización y control seguros, configurando y desplegando cortafuegos industriales básicos.

l) Definir y aplicar procedimientos para el cumplimiento normativo en materia de ciberseguridad y de protección de datos personales, implementándolos tanto internamente como en relación con

terceros.

m) Elaborar documentación técnica y administrativa cumpliendo con la legislación vigente, respondiendo a los requisitos establecidos.

n) Adaptarse a las nuevas situaciones laborales, manteniendo actualizados los conocimientos científicos, técnicos y tecnológicos relativos a su entorno profesional, gestionando su formación y los recursos existentes en el aprendizaje a lo largo de la vida.

ñ) Resolver situaciones, problemas o contingencias con iniciativa y autonomía en el ámbito de su competencia, con creatividad, innovación y espíritu de mejora en el trabajo personal y en el de las personas integrantes del equipo.

o) Generar entornos seguros en el desarrollo de su trabajo y el de su equipo, supervisando y aplicando los procedimientos de prevención de riesgos laborales y ambientales, de acuerdo con lo establecido por la normativa y los objetivos de la organización.

p) Supervisar y aplicar procedimientos de gestión de calidad, de accesibilidad universal y de «diseño para todas las personas», en las actividades profesionales incluidas en los procesos de producción o prestación de servicios.

4. Enseñanzas del Curso de Especialización

4.1. Objetivos generales:

a) Identificar los principios de la organización y normativa de protección en ciberseguridad, planificando las acciones que es preciso adoptar en el puesto de trabajo para la elaboración del plan de prevención y concienciación.

b) Auditar el cumplimiento del plan de prevención y concienciación de la organización, definiendo las acciones correctoras que puedan derivarse para incluirlas en el plan de securización de la organización.

c) Detectar incidentes de ciberseguridad implantando los controles, las herramientas y los mecanismos necesarios para su monitorización e identificación.

d) Analizar y dar respuesta a incidentes de ciberseguridad, identificando y aplicando las medidas necesarias para su mitigación, eliminación, contención o recuperación.

e) Identificar vulnerabilidades y amenazas específicas de los sistemas de control de la industria y proponer medidas organizativas en entornos industriales.

e) Elaborar análisis de riesgos para identificar activos, amenazas, vulnerabilidades y medidas de seguridad.

f) Diseñar e implantar planes de medidas técnicas de seguridad a partir de los riesgos identificados para garantizar el nivel de seguridad requerido.

g) Configurar sistemas de control de acceso, autenticación de personas y administración de credenciales para preservar la privacidad de los datos.

h) Configurar la seguridad de sistemas informáticos para minimizar las probabilidades de exposición a ataques.

i) Diseñar la integración de las tecnologías de la información (IT) con las tecnologías operativas (OT) asegurando los dispositivos OT.

i) Configurar dispositivos de red para cumplir con los requisitos de seguridad.

j) Administrar la seguridad de sistemas informáticos en red aplicando las políticas de seguridad requeridas para garantizar la funcionalidad necesaria con el nivel de riesgo de red controlado.

k) Aplicar estándares de verificación requeridos por las aplicaciones para evitar incidentes de seguridad.

l) Automatizar planes de desplegado de software respetando los requisitos relativos a control de versiones, roles, permisos y otros para conseguir un desplegado seguro.

m) Aplicar técnicas de investigación forense en sistemas y redes en los ámbitos del almacenamiento de la información no volátil, de los ordenadores personales, de los dispositivos móviles, del Cloud y de los sistemas IoT (Internet de las cosas), entre otros, para la elaboración de análisis forenses.

n) Analizar informes forenses identificando los resultados de la investigación para extraer conclusiones y realizar informes.

ñ) Combinar técnicas de hacking ético interno y externo para detectar vulnerabilidades que permitan eliminar y mitigar los riesgos asociados.

o) Identificar el alcance de la aplicación normativa dentro de la organización, tanto internamente como en relación con terceros para definir las funciones y responsabilidades de todas las partes.

p) Revisar y actualizar procedimientos de acuerdo con normas y estándares actualizados para el correcto cumplimiento normativo en materia de ciberseguridad y de protección de datos personales.

q) Desarrollar manuales de información, utilizando herramientas ofimáticas y de diseño asistido por ordenador para elaborar documentación técnica y administrativa.

r) Analizar y utilizar los recursos y oportunidades de aprendizaje relacionados con la evolución científica, tecnológica y organizativa del sector y las tecnologías de la información y la comunicación, para mantener el espíritu de actualización y adaptarse a nuevas situaciones laborales y personales.

s) Desarrollar la creatividad y el espíritu de innovación para responder a los retos que se presentan en los procesos y en la organización del trabajo y de la vida personal.

t) Evaluar situaciones de prevención de riesgos laborales y de protección ambiental, proponiendo y aplicando medidas de prevención personales y colectivas, de acuerdo con la normativa aplicable en los procesos de trabajo, para garantizar entornos seguros.

u) Identificar y proponer las acciones profesionales necesarias para dar respuesta a la accesibilidad universal y al «diseño para todas las personas».

v) Identificar y aplicar parámetros de calidad en los trabajos y actividades realizados en el proceso de aprendizaje, para valorar la cultura de la evaluación y de la calidad y ser capaces de supervisar y mejorar procedimientos de calidad.

4.2. Módulos profesionales.

CÓDIGO	MÓDULO PROFESIONAL	ASIGNACIÓN HORARIA
5021	Incidentes de ciberseguridad.	84
5022	Bastionado de redes y sistemas.	192
5023	Puesta en producción segura.	120
5024	Análisis forense informático.	96
5025	Hacking ético.	120
5026	Normativa de ciberseguridad.	48
E300	Fundamentos básicos.	60
E301	Formación Práctica Dual en Empresa	270
TOTAL		990

4.3. Módulos profesionales: Resultados de Aprendizaje, Criterios de Evaluación y Contenidos.

Módulo Profesional 1: Incidentes de ciberseguridad.

Código: 5021.
Duración: 84 horas.
Créditos ECTS: 9.

Resultados de aprendizaje, criterios de evaluación y contenidos.

RA1. 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 norma de protección del puesto de trabajo.
c) Se ha definido un plan de concienciación de ciberseguridad dirigido a las empleadas y empleados.
d) Se ha desarrollado el material necesario para llevar a cabo las acciones de concienciación dirigidas a las empleadas y empleados.
e) Se ha realizado una auditoría para verificar el cumplimiento del plan de prevención y concienciación de la organización.

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

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

RA2. 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 los 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.

Contenidos: 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.

RA3. Investiga incidentes de ciberseguridad analizando los riesgos implicados y definiendo las posibles medidas a adoptar.

Criterios de evaluación:

a) Se han reconocido las distintas fases del proceso de recogida y análisis de evidencias.
b) Se han recopilado y almacenado de forma segura evidencias de incidentes de ciberseguridad que afectan a la organización.

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

Contenidos: Investigación de los incidentes de ciberseguridad.

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

RA4. 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 al incidente para evitar que una situación similar se vuelva a repetir.

Contenidos: Implementación de medidas de ciberseguridad.

− Desarrollo de procedimientos de actuación detallados para dar respuesta, mitigar, eliminar o contener los tipos de incidentes.
− Implantación de capacidades de ciberresiliencia.
− Establecimiento de flujos de toma de decisiones y escalado interno y/o externo adecuados.
− Tareas para restablecer los servicios afectados por incidentes.
− Documentación.
− Seguimiento de incidentes para evitar una situación similar.

RA5. 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.

Contenidos: Detección y documentación de incidentes de ciberseguridad.

− Desarrollo de procedimientos de actuación para la notificación de incidentes.
− Notificación interna de incidentes.
− Notificación de incidentes a quienes corresponda.

Módulo Profesional 2: Bastionado de redes y sistemas.

Código: 5022.
Duración: 192 horas.
Créditos ECTS: 10.

Resultados de aprendizaje, criterios de evaluación y contenidos.

RA1: Administra las funciones básicas de un router estableciendo opciones de configuración para su integración en la red.

Criterios de evaluación:

a) Se han utilizado distintos métodos para acceder al modo de configuración del router.
b) Se han configurado rutas estáticas.
c) Se han identificado los archivos que guardan la configuración del router y se han gestionado mediante los comandos correspondientes.
d) Se han utilizado los comandos proporcionados por el sistema operativo del router que permiten hacer el seguimiento de posibles incidencias.
e) Se ha descrito las capacidades de filtrado de tráfico.
f) Se han utilizado comandos para gestionar listas de control de acceso ACL.
g) Se han configurado sistemas de traducción de direcciones de red.

h) Se ha configurado el reenvío de puertos.

Contenidos: Configuración y administración básica del router.

− Diferentes métodos de acceso al router.
− Comandos para la configuración y administración del router.
− Configuración de rutas estáticas.
− Comandos para el seguimiento de incidencias y monitorización del estado del router.
− Configuración de filtros de tráfico del router.
− Gestión de listas de control de acceso (ACL)
− Traducción de direcciones de red: NAT y PAT.
− Reenvío de puertos.

RA2: Configura redes locales virtuales identificando su campo de aplicación.

Criterios de evaluación:

a) Se han implementado VLANs.
b) Se han configurado enlaces troncales.
c) Se ha utilizado un router o switch multilayer para interconectar diversas VLANs.
d) Se han configurado conmutadores para trabajar de acuerdo con los protocolos de administración centralizada.

Contenidos: Redes virtuales

- Implementación de VLANs.
- Diagnóstico de incidencias en VLANs.
- Configuración de enlace troncal entre dispositivos.
- Configuración de router o switch multilayer para interconectar diversas VLANs
- Protocolos de VLANs.

RA3. 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 han 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 han 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.

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.

RA 4. 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.
f) Se han establecido diferentes herramientas de gestores de contraseñas.

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

− Mecanismos de autenticación. Tipos de factores.
− Técnicas de autenticación: contraseñas, certificados digitales, tokens, contraseñas de un solo uso (OTP), características biométricas, combinaciones de las anteriores, etc.

RA 5. 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).

Contenidos: Administración de credenciales de acceso a sistemas informáticos.

− Gestión de credenciales.
− Infraestructuras de Clave Pública (PKI).
− Acceso por medio de Firma electrónica.
− Aplicación de firma digital.
− 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.

RA 6. 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.

f) Se han definido y configurado redes segmentadas aseguradas perimetralmente por firewalls virtuales, utilizando entornos de virtualización de servidores.

Contenidos: Diseño de redes de computadores seguras.

− Segmentación de redes.
− Montaje y configuración de redes en entornos de virtualización de servidores (Proxmox, OpenStack…)
− Subnetting.
− Redes virtuales (VLANs).
− Zona desmilitarizada (DMZ).
− Seguridad en redes inalámbricas (WPA2, WPA3, etc.).

− Protocolos de red seguros (IPSec, etc.).
− Diseño y definición de modelos para el establecimiento del perímetro de seguridad.
− Configuración de políticas y reglas de filtrado de cortafuegos.
− Configuración segura de servidores y servicios sobre la DMZ. Cortafuegos de contención y bastión.
− Firewalls virtuales (Sophos, por ejemplo).
− Implantación de honeynets.
− Instalación y configuración de un servidor web-proxy-cache.
− Utilización del servidor proxy para establecer restricciones de acceso web.
− Realización de pruebas de funcionamiento del proxy y monitorización de su actividad.
− Pruebas de acceso desde los clientes al proxy. Configuración de un proxy en modo transparente y modo inverso.

RA 7. 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 configurado y utilizado distintos tipos de cortafuegos.
c) Se han configurado las políticas y reglas de filtrado de un cortafuegos, auditando los registros de sucesos.
d) Se han configurado de forma segura servidores y servicios sobre la DMZ.
e) Se han detectado errores de configuración de dispositivos de red mediante el análisis de tráfico.
f) Se han identificado comportamientos no deseados en una red a través del análisis de los registros (Logs), de un cortafuego.
g) Se han implementado contramedidas frente a comportamientos no deseados en una red.
h) Se han caracterizado, instalado y configurado diferentes herramientas de monitorización.
i) Se han configurado y utilizado los distintos tipos de proxy.

Contenidos: 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.
− Motores de analítica de datos para análisis de logs (Elasticsearch, por ejemplo) .
− Herramientas de visualización de datos para muestra de logs analizados (Kibana, por ejemplo).
− 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. Protocolo SNMP.
− Herramientas de monitorización (IDS, IPS).
− SIEMs (Gestores de Eventos e Información de Seguridad).
− Análisis y normalización de eventos.
− Agregación de eventos. Gestión de log y procedimientos de actuación.
− Monitorización, documentación y respuesta ante incidentes de seguridad y amenazas.
− Soluciones de Centros de Operación de Red y Centros de Seguridad de Red: NOCs y SOCs.

RA 8. 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.
f) Se han implementado medidas de alta disponibilidad comprobando la continuidad operacional en caso de caída de algún dispositivo.
g) Se ha configurado una honeynet para atraer a potenciales atacantes y aprender de sus actuaciones.
h) Se ha instalado y configurado un sistema integral de procesamiento y visualización de logs.

Contenidos: 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, 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.
− Alta disponibilidad: clusters, redundancia de discos, bonding...

RA 9. 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.

Contenidos: 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.

RA 10. Diseña la integración de la parte IT con la parte OT asegurando los dispositivos OT ante posibles ataques internos o externos a la organización.

Criterios de evaluación:

a) Se ha generado un dossier con las principales amenazas en una red OT y posibles medidas de defensa.

b) Se ha diseñado una segmentación de red por capas que permite mantener asegurados los dispositivos OT.

c) Se han implantado medidas de seguridad para el acceso remoto seguro a dispositivos OT.

d) Se ha instalado y configurado un honeypot específico para conocer los intentos de ataques a los dispositivos industriales.

e) Se han analizado aspectos básicos de la ciberseguridad industrial.

f) Se ha recreado un entorno industrial básico, instalando y configurando al menos un dispositivo de control industrial y un software de supervisión y control remoto.

g) Se han analizado las características de los distintos componentes industriales, así como su lugar en el ámbito de la automatización, su funcionamiento y vulnerabilidades.

h) Se han utilizado herramientas básicas de explotación de vulnerabilidades de dispositivos industriales.

Contenidos: Sistemas de control industrial: amenazas y vulnerabilidades.

− Conceptos básicos de Infraestructuras industriales.

- Introducción a los sistemas de control industrial.

- Protocolos de comunicación en OT. Modbus, Profinet, etc.
- Instalación y configuración de un PLC simulado.
- Instalación y configuración de un SCADA básico.
- Configuración conectividad entre PLC y SCADA.
- Sistemas de control local: sensores, actuadores, servos y variadores, PLCs, RTUs, PCs industriales y DCS. Aspectos clave, puntos fuertes y puntos débiles.
- SCADA: funciones, arquitectura y componentes.
- Sistemas de seguridad, sistemas de seguridad instrumentados (SIS) y sistemas integrados de control y seguridad (ICSS).
- Otros sistemas específicos sectoriales: CNC, contadores inteligentes, robots, MES, etc.

− Integración de redes IT/OT. Vulnerabilidades de las redes OT.

- Principales amenazas en una red OT.
- Segmentación de redes. División IT/OT.
- Acceso remoto seguro a dispositivos OT.
- Configuración de honeypots industriales.
- Shodan: propósito y uso.
- Distribución Kali-Moki: herramientas para atacar sistemas de automatización y control a nivel de host.
- Uso de Metasploit.

Módulo Profesional 3: Puesta en producción segura

Código: 5023
Duración: 120 horas
Créditos ECTS: 7

Resultados de aprendizaje, criterios de evaluación y contenidos.

RA1: Realiza programas sencillos aplicando los fundamentos de la programación orientada a objetos.

Criterios de evaluación:

a) Se han identificado los fundamentos de programación orientado a objetos.
b) Se han instanciado objetos a partir de clases predefinidas.
c) Se han utilizado métodos y propiedades de los objetos.
d) Se han escrito llamadas a métodos estáticos.
e) Se han utilizado parámetros en las llamadas a métodos.
f) Se han incorporado y utilizado librerías de objeto.
g) Se han utilizado constructores.

Contenidos: Utilización de objetos.

− Características de los objetos y de las clases.
− Propiedades o atributos de los objetos.
− Concepto de método.
− Control de acceso a los miembros de una clase.
− Concepto de método estático.
− Parámetros y valores devueltos.

RA2: Desarrolla programas organizados en clases aplicando los principios de programación orientada a objetos.

Criterios de evaluación:

a) Se han identificado la sintaxis, estructura y componentes de una clase.
b) Se han definido clases.
c) Se han creado constructores.
d) Se han desarrollado programas que implementan y utilizan objetos de las clases creadas.
e) Se han utilizado mecanismos para controlar la visibilidad de las clases y sus miembros.
f) Se ha definido el concepto de herencia.
g) Se han definido y utilizado clases heredadas.
h) Se han creado y utilizado métodos estáticos.
i) Se han creado y utilizado librerías de clases.
j) Se han creado y definido interfaces.

Contenidos: Desarrollo de clases.

− Concepto de clase.
− Estructura y miembros de una clase.
− Herramientas de definición de los atributos y control de acceso.
− Herramientas de declaración de métodos y argumentos.
− Herramientas de diseño de constructores.
− Encapsulación y visibilidad.
− Concepto de herencia.
− Concepto de clase heredada.

RA3: Desarrolla programas aplicando características avanzadas de los lenguajes orientados a objetos.

Criterios de evaluación:

a) Se han identificado los conceptos superclase y subclase.

b) Se han diseñado y aplicado jerarquías de clases.
c) Se han probado y depurado las jerarquías de clases.
d) Se han realizado programas que implementan y utilizan jerarquías de clases.

Contenidos: Desarrollo de clases avanzadas.

− Jerarquía de clases: superclase y subclases.
− Concepto de polimorfismo.
− Constructores y destructores de subclases.
− Acceso de métodos de la superclase.
− Redefinición de métodos de la superclase.

RA4: 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 diferentes modelos de ejecución de software.
c) Se han reconocido los elementos básicos del código fuente, dándole significado.
d) Se han ejecutado diferentes tipos de pruebas de software.
e) Se han evaluado los lenguajes de programación de acuerdo a la infraestructura de seguridad que proporcionan.

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”).

RA5: 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.

Contenidos: 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).

RA6: 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 han explorado las vulnerabilidades de un sistema que permite al atacante fijar el identificador de sesión.
d) Se ha gestionado correctamente la sesión del usuario durante el uso de la aplicación.
e) Se ha verificado la autenticidad del usuario a la hora de acceder a los recursos y funcionalidades.
f) Se ha evitado la fuga de datos mediante el control de la autorización a los mismos.
g) Se ha hecho uso de roles para el control de acceso.
h) Se han utilizado algoritmos criptográficos seguros para almacenar las contraseñas de usuario.
i) Se han configurado servidores web para reducir el riesgo de sufrir ataques conocidos.
j) Se han incorporado medidas para evitar los ataques a contraseñas, envío masivo de mensajes o registros de usuarios a través de programas automáticos (bots).

Contenidos: 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.
− Fuga de datos. Revelación de información en mensajes de error. Path traversal.
− Almacenamiento seguro de contraseñas.
− Contramedidas. HSTS, CSP, CAPTCHAs, entre otros.
− Herramientas específicas de criptografía. Certificados digitales, protocolos seguros y firmas

digitales.

− Seguridad de portales y aplicativos web. Soluciones WAF (Web Application Firewall).

RA7: 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.

Contenidos: 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.

RA8: 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 de 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 grupo.

Contenidos: 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 4: Análisis forense informático.

Código: 5024.
Duración: 96 horas
Créditos ECTS: 7.

Resultados de aprendizaje, criterios de evaluación y contenidos.

RA1. 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.

Contenidos: Aplicación de metodologías de análisis forenses.

− Identificación de los dispositivos a analizar.
− Requisitos de investigación forense: aceptabilidad, integridad, credibilidad, relación causa-efecto, repetible y documentada.
− Etapas del análisis forense.
− Consideraciones previas a la adquisición.

− Orden de volatilidad.
− 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.

RA2. Realiza análisis forenses en ordenadores personales, aplicando metodologías establecidas, actualizadas y reconocidas.

Criterios de evaluación:

a) Se han analizado sistemas de ficheros, los datos que contienen y sus metadatos.
b) Se han recuperado ficheros borrados.
c) Se ha analizado el comportamiento del ransomware y del malware en general.
d) Se han analizado discos.
e) Se ha analizado la memoria RAM de los sistemas.
f) Se ha analizado el registro del sistema.
g) Se ha analizado la información y actividad del usuario en el sistema.

Contenidos: Realización de análisis forenses en ordenadores personales.

− Sistemas de ficheros. Datos y metadatos.
− Recuperación de ficheros borrados.
− Comportamiento del ransomware y del malware.
− Análisis de discos.
− Análisis de memoria. Volcados. Procesos en ejecución.
− Análisis del registro.
− Análisis e información de usuario: navegadores, correo electrónico, búsquedas, actividad...

RA3. 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.

Contenidos: Realización de análisis forenses en dispositivos móviles.

− Métodos para la extracción de evidencias.

− Herramientas de mercado más comunes.
− Análisis de tarjetas SIM y de tarjetas de memoria.

RA4. 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.

Contenidos: 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, …).

RA5. 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.

Contenidos: Realización de análisis forenses en IoT.

− Identificación de los dispositivos a analizar.
− Adquisición y extracción de las evidencias.
− Análisis de las evidencias de manera manual y automática.
− Elaboración de la documentación del proceso realizado.
− Establecimiento de la línea temporal.
− Mantenimiento de la cadena de custodia.
− Elaboración de las conclusiones.
− Presentación y exposición de las conclusiones.

RA6. 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.

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

− Introducción al peritaje. Legislación. Órdenes de registro. Juicios.
− 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 5: Hacking ético.

Código: 5025.
Duración: 120 horas.
Créditos ECTS: 7.

Resultados de aprendizaje, criterios de evaluación y contenidos.

RA1: 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 del 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 de vulnerabilidades.
g) Se han analizado y definido los tipos de ataques.
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.

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.
− ClearNeta, Deep Web, Dark Web, Darknets. Conocimiento, diferencias y herramientas de acceso: Tor, ZeroNet, FreeNet.

RA2: Ataca y defiende en entornos de prueba, comunicaciones inalámbricas consiguiendo acceso a las redes para demostrar 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 el 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 inalámbrica y sus vulnerabilidades.

f) Se han utilizado técnicas de “Equipo Rojo y Azul”.

g) Se han realizado informes sobre las vulnerabilidades detectadas y se han añadido las formas de mitigación de las mismas.

Contenidos: 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 ataques inalámbricos.
− Realización de informes de auditoría y presentación de resultados.

RA3: 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.

f) Se han realizado informes sobre las vulnerabilidades detectadas y se han añadido las formas de mitigación de las mismas.

Contenidos: 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).
− Monitorización de tráfico.
− Interceptación de comunicaciones utilizando distintas técnicas.
− Manipulación e inyección de tráfico.
− Herramientas de búsqueda y explotación de vulnerabilidades.
− Ingeniería social. Phishing.
− Escalada de privilegios.

− Informes de vulnerabilidades en redes y sistemas y propuestas de mejora.

RA4: Consolida y utiliza sistemas comprometidos garantizando accesos futuros.

Criterios de evaluación:

a) Se han administrado sistemas remotos a través de herramientas en 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.

Contenidos: 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).

RA5: Ataca y defiende 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 durante su uso normal.
d) Se han examinado manualmente aplicaciones web en busca de las vulnerabilidades más habituales.
e) Se han usado herramientas de búsqueda y explotación de vulnerabilidades web
f) Se ha realizado la búsqueda y explotación de vulnerabilidades web mediante herramientas software.
g) Se han realizado informes sobre las vulnerabilidades detectadas y se han añadido las formas de mitigación de las mismas.

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

− Negación de credenciales en aplicaciones web.
− Recolección de la 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.
− Informes de vulnerabilidades en aplicaciones web y propuestas de mejora.

RA6: Analiza aplicaciones de telefonía móvil demostrando si son seguras o no.

Criterios de evaluación:

a) Se han hecho análisis estáticos de la aplicación en lado cliente.
b) Se han analizado las comunicaciones.
c) Se ha analizado dinámicamente el comportamiento de la aplicación en el lado cliente.
d) Se han utilizado herramientas de pentesting para el análisis de aplicaciones móviles.

Contenidos: Análisis de aplicaciones para móviles.

− Herramientas de análisis de código fuente de aplicaciones para móviles tanto manuales como automáticas.
− Herramientas de análisis de tráfico de red.
− Herramientas de análisis dinámico de aplicaciones (por ejemplo DROZER)
− Herramientas de pentesting para móviles (OWASP - ZAP)

Módulo Profesional 6: Normativa de ciberseguridad.

Código: 5026.
Duración: 48 horas.
Créditos ECTS: 3.

Resultados de aprendizaje, criterios de evaluación y contenidos.

RA1: 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.

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 ético empresarial.
− Compliance Officer: funciones y responsabilidades.
− Relaciones con terceras partes dentro del Compliance.

RA2: 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 19600 entre otras).
c) Se han realizado análisis y evaluaciones de los riesgos de diferentes tipos de organizaciones de acuerdo con la normativa vigente (31000 entre otras).
d) Se ha documentado el sistema de cumplimiento normativo diseñado.

Contenidos: Diseño de sistemas de cumplimiento normativo.

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

RA3: Relaciona la normativa vigente 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 19601, 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 37001 entre otros).

Contenidos: 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.

RA4: 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 de 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.

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

− Principios de protección de datos.
− RGPD.
− Privacidad por Diseño y por Defecto.
− Análisis de Impacto en Privacidad (PIA) y medidas de seguridad.
− Delegado de Protección de Datos (DPO).
− LSSI.

RA5: 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 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

f) Se han determinado e implementado los controles necesarios explicitados en la ISO 27002 de buenas prácticas para asegurar la integridad, disponibilidad y confidencialidad de la información.

g) Se han descrito las fases para el desarrollo de un SGSI (Sistema de Gestión de Seguridad de la Información)

h) Se han diseñado zonas, conductos y canales según IEC 62443.

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

− Normas nacionales e internacionales.
− Sistemas de Gestión de la Seguridad de la Información (estándares internacionales ISO 27001).
− Código de Buenas Prácticas ISO 27002
− Acceso electrónico de los ciudadanos a los Servicios Públicos. Esquema Nacional de Seguridad (ENS).
− Planes de Continuidad de Negocio (estándares internacionales) (ISO 22301).
− IEC 62443
− Directiva NIS
− Legislación sobre la protección de infraestructuras críticas. Ley PIC (Protección de Infraestructuras críticas)

Módulo Profesional 7: Módulo profesional: Fundamentos básicos.

Código: E300

Duración: 60 horas

Resultados de aprendizaje, criterios de evaluación y contenidos.

RA1: Integra ordenadores y periféricos en redes cableadas e inalámbricas, evaluando su funcionamiento y prestaciones.

Criterios de evaluación:

a) Se han identificado los estándares para redes cableadas e inalámbricas.

b) Se ha utilizado el sistema de direccionamiento lógico IP para asignar direcciones de red y máscaras de subred.

c) Se han configurado adaptadores de red cableados e inalámbricos bajo distintos sistemas operativos.

Contenidos: Redes cableadas e inalámbricas.

− Configuración de direcciones IP y máscaras subred.
− Configuración de adaptadores de red cableados e inalámbricos bajo distintos sistemas operativos.
− Configuración de dispositivos de interconexión en redes cableadas e inalámbricas.

RA2: Adopta pautas y prácticas de tratamiento seguro de la información, reconociendo las vulnerabilidades de un sistema informático y la necesidad de asegurarlo.

Criterios de evaluación:

a) Se han descrito las diferencias entre seguridad física y lógica.
b) Se ha contrastado la incidencia de las técnicas de ingeniería social en los fraudes informáticos.
c) Se han valorado las ventajas que supone la utilización de sistemas biométricos.
d) Se han aplicado técnicas criptográficas en el almacenamiento y transmisión de la información.
e) Se han identificado los protocolos seguros de comunicación y sus ámbitos de utilización.

Contenidos: Pautas de seguridad informática.

− Seguridad física y seguridad lógica
− Principales causas de vulnerabilidad y su origen.
− Políticas de contraseña.
− Sistemas biométricos.
− Gestores de contraseñas
− Propiedades CIDAN
− Criptografía simétrica y asimétrica.
− Firma digital y certificados.
− Infraestructuras de Clave Pública (PKI).

RA3: Administra funciones avanzadas de los sistemas operativos atendiendo a su funcionamiento interno.

Criterios de evaluación:

a) Se han implantado políticas de seguridad de forma centralizada para todos los equipos y usuarios del dominio.
b) Se han identificado los procesos y ficheros involucrados en el arranque del sistema.
c) Se han administrado los ficheros de configuración del sistema.
d) Se han identificado los procesos que se ejecutan en el sistema.

e) Se han analizado los ficheros de log.

Contenidos: Sistemas Operativos en Red.

− Dominios. Seguridad. Directivas de grupo.
− Funcionamiento interno de los sistemas operativos.
- Arranque.
- Ficheros de configuración.
- Procesos.
- Ficheros de log.

RA4: Realiza programas sencillos accediendo a bases de datos.

Criterios de evaluación:

a) Se han definido variables de diferentes tipos y realizado diferentes operaciones con ellas.
b) Se han manejado estructuras condicionales y repetitivas.
c) Se han definido y utilizado estructuras de datos.
d) Se han utilizado funciones predefinidas y se han definido y utilizado funciones definidas por el usuario.
e) Se han creado y utilizado módulos y/o paquetes, así como utilizado bibliotecas standard.
f) Se han gestionado errores y excepciones.
g) Se ha accedido a bases de datos realizando operaciones básicas de inserción, selección, actualización y borrado de registros.

Contenidos: Creación de programas básicos.

− Variables, tipos y operadores.
− Estructuras condicionales y repetitivas.
− Estructuras de datos.
− Funciones predefinidas y funciones definidas por el usuario.
− Módulos y/o paquetes. Bibliotecas standard.
− Errores y excepciones.
− Bases de datos: inserción, selección, actualización y borrado de registros.
− Concepto de herencia.
− Concepto de clase heredada.

Módulo Profesional 8: Formación Práctica Dual en Empresa
Código: E301
Duración: 270 horas

Las actividades a realizar en la empresa se programarán con la finalidad de completar las competencias del Curso de Especialización y sus objetivos generales, tanto para aquellas que se han alcanzado en el centro educativo, como para aquellas que son difíciles de conseguir en el mismo. Las actividades diseñadas deberán incluir:

− La elaboración de planes de prevención y detección de incidentes en base a herramientas de monitorización e implantación de medidas correctivas.
− El diseño e implementación de planes de securización, diseño de redes de computadores y administración de los sistemas de control de acceso y autenticación.
− El análisis del nivel de seguridad requerido por las aplicaciones y dispositivos móviles, así como los vectores de ataque más habituales e implantación de sistemas seguros de desplegado de software.
− La colaboración en proyectos de análisis forenses informáticos.
− La detección de vulnerabilidades en sistemas, redes y aplicaciones.
− La definición y aplicación de procedimientos para el cumplimiento normativo y de protección de datos personales.

5. Espacios y equipamientos.

5.1. Espacios:

ESPACIO FORMATIVO	SUPERFICIE M2 / 30 ALUMNOS O ALUMNAS	SUPERFICIE M2 / 20 ALUMNOS O ALUMNAS
Aula técnica	60	40
Laboratorio.	180	140
Aula polivalente	60	40

5.2. Equipamientos:

ESPACIO FORMATIVO	EQUIPAMIENTO
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, proxies, 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, gestores de contraseña, entre otros.
Laboratorio	Mesas de trabajo individuales tipo taller (80-90 cm alto). Bastidor (rack) para la instalación de servidores y dispositivos adicionales. Ordenadores con sistema operativo de red y conexión a Internet. Software específico de diagnóstico, seguridad, antivirus y comunicaciones, honeypots/honeynets, entre otros. Controladores Lógicos Programables, simuladores de los mismos y sensores. Software específico de programación de Controladores Lógicos Programables, simuladores y visualización de datos. Equipo de automatización industrial y de procesos con actuadores electrónicos y neumáticos. Sistemas de reprografía y escáner. Servidores con capacidad para virtualizar distintos escenarios, con las tecnologías más avanzadas. Soportes de almacenamiento (discos, memorias USB, tarjetas de memoria, tarjetas SIM...). Switches y routers. 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.

6. Profesorado.

6.1. Especialidades del profesorado con atribución docente en los módulos profesionales del Curso de Especialización en Ciberseguridad en Entrondos de las Tecnologías de la Información:

MÓDULO PROFESIONAL	ESPECIALIDAD DEL PROFESORADO	CUERPO
5021. Incidentes de ciberseguridad.	Informática. Sistemas Electrónicos. Sistemas Electrotécnicos y Automáticos.	Profesora o Profesor de Enseñanza Secundaria.
	Profesora o Profesor Especialista.	
5022. Bastionado de redes y sistemas	Equipos Electrónicos. Sistemas y Aplicaciones Informáticos.	Profesora Técnica o Profesor Técnico de Formación Profesional.
5023. Puesta en producción segura.	Sistemas y Aplicaciones Informáticas.	Profesora Técnica o Profesor Técnico de Formación Profesional.
	Profesora o Profesor Especialista.	
5024. Análisis forense informático.	Sistemas y Aplicaciones Informáticas.	Profesora Técnica o Profesor Técnico de Formación Profesional.
	Profesora o Profesor Especialista.	
5025. Hacking ético.	Informática. Sistemas Electrónicos. Sistemas Electrotécnicos y Automáticos.	Profesora o Profesor de Enseñanza Secundaria.
	Profesora o Profesor Especialista.	

5026. Normativa de ciberseguridad.	Informática. Sistemas Electrónicos. Sistemas Electrotécnicos y Automáticos.	Profesora o Profesor de Enseñanza Secundaria.
	Profesora o Profesor Especialista.	
E300. Fundamentos básicos.	Informática.	Profesora o Profesor de Enseñanza Secundaria.
E301. Formación Práctica Dual en Empresa	Informática. Sistemas Electrónicos. Sistemas Electrotécnicos y Automáticos.	Profesora o Profesor de Enseñanza Secundaria.
	Equipos Electrónicos. Sistemas y Aplicaciones Informáticos.	Profesora Técnica o Profesor Técnico de Formación Profesional.

6.2. Titulaciones habilitantes a efectos de docencia:

CUERPO	ESPECIALIDAD	TITULACIONES
Profesora o Profesor de Enseñanza Secundaria.	Informática.	Diplomada o Diplomado en Estadística. Ingeniera Técnica o Ingeniero Técnico en Informática de Gestión. Ingeniera Técnica o Ingeniero Técnico en Informática de Sistemas. Ingeniera Técnica o Ingeniero Técnico en Telecomunicación, especialidad en Telemática.
	Sistemas Electrónicos. Sistemas Electrotécnicos y Automáticos.	Diplomada o Diplomado en Radioelectrónica Naval. Ingeniera Técnica o Ingeniero Técnico Aeronáutico, especialidad en Aeronavegación. Ingeniera Técnica o Ingeniero Técnico Industrial, especialidad en Electricidad, especialidad en Electrónica Industrial. Ingeniera Técnica o Ingeniero Técnico en Informática de Sistemas. Ingeniera Técnica o Ingeniero Técnico en Telecomunicación, en todas sus especialidades.

o cualquier otra titulación que pueda aparecer en normativa reguladora.

6.3. Titulaciones requeridas para impartir módulos profesionales que conforman el Curso de Especialización para los centros de titularidad privada, de otras Administraciones distintas a la educativa y orientaciones para la Administración educativa:

.

MÓDULOS PROFESIONALES	TITULACIONES
5021. Incidentes de ciberseguridad. 5025. Hacking ético. 5026. Normativa de ciberseguridad. E300. Fundamentos básicos de programación, redes, y sistemas operativos (y criptografía).	Doctora o Doctor, Licenciada o Licenciado, Ingeniera o Ingeniero, Arquitecta o Arquitecto o título de Grado correspondiente u otros títulos equivalentes a efectos de docencia.
5022. Bastionado de redes y sistemas 5023. Puesta en producción segura. 5024. Análisis forense informático.	Doctora o Doctor, Licenciada o Licenciado, Ingeniera o Ingeniero, Arquitecta o Arquitecto o título de Grado correspondiente u otros títulos equivalentes a efectos de docencia.

	Diplomada o Diplomado Universitario, Arquitecta Técnica u Arquitecto Técnico u otros títulos equivalentes a efectos de docencia.

6.4. Titulaciones habilitantes a efectos de docencia para impartir módulos profesionales que conforman el Curso de Especialización para los centros de titularidad privada, de otras Administraciones distintas a la educativa y orientaciones para la Administración educativa:

MÓDULOS PROFESIONALES	TITULACIONES
5021. Incidentes de ciberseguridad. 5025. Hacking ético. 5026. Normativa de ciberseguridad.	Diplomada o Diplomado en Estadística. Diplomada o Diplomado en Radioelectrónica Naval. Ingeniera Técnica o Ingeniero Técnico Aeronáutico, especialidad en Aeronavegación. Ingeniera Técnica o Ingeniero Técnico Industrial, especialidad en Electricidad, especialidad en Electrónica Industrial. Ingeniera Técnica o Ingeniero Técnico en Informática de Gestión. Ingeniera Técnica o Ingeniero Técnico en Informática de Sistemas. Ingeniera Técnica o Ingeniero Técnico en Telecomunicación, en todas sus especialidades.
E300. Fundamentos básicos.	Diplomada o Diplomado en Estadística. Ingeniera Técnica o Ingeniero Técnico en Informática de Gestión. Ingeniera Técnica o Ingeniero Técnico en Informática de Sistemas. Ingeniera Técnica o Ingeniero Técnico en Telecomunicación, especialidad en Telemática.