



Catálogo de Especialidades Formativas

PROGRAMA FORMATIVO

CIBERSEGURIDAD AVANZADA EN ENTORNOS DE LAS TECNOLOGÍAS DE LA
OPERACIÓN

Septiembre 2023

IDENTIFICACIÓN DE LA ESPECIALIDAD Y PARÁMETROS DEL CONTEXTO FORMATIVO

Denominación de la especialidad:	CIBERSEGURIDAD AVANZADA EN ENTORNOS DE LAS TECNOLOGÍAS DE LA OPERACIÓN
Familia Profesional:	INFORMÁTICA Y COMUNICACIONES
Área Profesional:	SISTEMAS Y TELEMÁTICA
Código:	IFCT0050
Nivel de cualificación profesional:	3

Objetivo general

Adquirir los conocimientos de ciberseguridad y la concienciación necesaria para dotar las redes industriales de los modelos de segmentación y securización de máquinas y dispositivos conectados, así como realizar ciberejercicios de ciberseguridad industrial.

Relación de módulos de formación

Módulo 1	INTRODUCCIÓN A LA CIBERSEGURIDAD	36 horas
Módulo 2	INTRODUCCIÓN A LOS FUNDAMENTOS INDUSTRIALES DE LAS TECNOLOGÍAS DE LA OPERACIÓN	36 horas
Módulo 3	INTRODUCCIÓN A LA CIBERSEGURIDAD INDUSTRIAL AVANZADA	24 horas
Módulo 4	CIBEREJERCICIOS BÁSICOS Y AVANZADOS DE CIBERSEGURIDAD INDUSTRIAL	24 horas

Modalidades de impartición

Presencial

Teleformación

Duración de la formación

Duración total en cualquier modalidad de impartición	120 horas
---	-----------

Teleformación Duración total de las tutorías presenciales: 16 horas

Requisitos de acceso del alumnado

Acreditaciones / titulaciones	Cumplir como mínimo alguno de los siguientes requisitos: -Título de Bachiller o equivalente -Título de Técnico Superior (FP Grado superior) o equivalente -Haber superado la prueba de acceso a Ciclos Formativos de Grado Superior -Certificado de profesionalidad de nivel 3
Experiencia profesional	No se requiere
Modalidad de teleformación	Además de lo indicado anteriormente, los participantes han de tener las destrezas suficientes para ser usuarios de la plataforma

Modalidad de teleformación	virtual en la que se apoya la acción formativa.
-----------------------------------	---

Prescripciones de formadores y tutores

Acreditación requerida	Cumplir como mínimo alguno de los siguientes requisitos: • Licenciatura, Ingeniería o Título de Grado correspondiente u otros títulos equivalentes en Ingeniería Industrial, Ingeniería Informática, Ingeniería Digital • Diplomatura, Ingeniería Técnica o Título de Grado correspondiente u otros títulos equivalentes en Fabricación Avanzada, Mecatrónica, Electrónica, Redes y Sistemas
Experiencia profesional mínima requerida	Poseer experiencia profesional acreditable en ocupaciones relacionadas con la especialidad a impartir de al menos un año.
Competencia docente	• Certificado de Profesionalidad de Docencia de la formación profesional para el empleo. • Experiencia docente contrastada de al menos 300 horas en los últimos 3 años de formación profesional para el empleo o del sistema educativo. • Titulaciones universitarias de Licenciatura en Pedagogía, Psicopedagogía o de Maestro o un Título Universitario Oficial de Posgrado en el ámbito educativo. • CAP (Curso de Actitud Pedagógica) o Master del Profesorado
Modalidad de teleformación	Además de cumplir con las prescripciones establecidas anteriormente, los tutores-formadores deben acreditar una formación, de al menos 30 horas, o experiencia, de al menos 60 horas, en esta modalidad y en la utilización de las tecnologías de la información y comunicación.

Requisitos mínimos de espacios, instalaciones y equipamientos

Espacios formativos	Superficie m² para 15 participantes	Incremento Superficie/ participante (Máximo 30 participantes)
Aula de informática	45.0 m ²	2.4 m ² / participante

Espacio formativo	Equipamiento
Aula de informática	• Mesa y silla para el formador • Mesas y sillas para el alumnado • Material de aula • Pizarra • PC instalado en red con posibilidad de impresión de documentos, cañón con proyección e Internet para el formador. • PCs instalados en red e Internet con posibilidad de impresión para los alumnos. • Todos los ordenadores han de tener las siguientes características mínimas: Procesador i5 0 Memoria RAM 8 GB 0 Disco SSD 256 GB 0 Tarjeta de red 10/100/1000 Mbps 0 Tarjeta de sonido 0 Periféricos: Teclado, Ratón y Monitor color 15,6" 0 • Software específico para el aprendizaje de cada acción formativa: Windows 11 actualizado 0

La superficie de los espacios e instalaciones estarán en función de su tipología y del número de participantes. Tendrán como mínimo los metros cuadrados que se indican para 15 participantes y el equipamiento suficiente para los mismos.

En el caso de que aumente el número de participantes, hasta un máximo de 30, la superficie de las aulas se incrementará proporcionalmente (según se indica en la tabla en lo relativo a m²/participante) y el equipamiento estará en consonancia con dicho aumento.

No debe interpretarse que los diversos espacios formativos identificados deban diferenciarse necesariamente mediante cerramientos.

Las instalaciones y equipamientos deberán cumplir con la normativa industrial e higiénico-sanitaria correspondiente y responderán a medidas de accesibilidad y seguridad de los participantes.

En el caso de que la formación se dirija a personas con discapacidad se realizarán las adaptaciones y los ajustes razonables para asegurar su participación en condiciones de igualdad.

Si la especialidad se imparte en **modalidad de teleformación**, cuando haya tutorías presenciales, se utilizarán los espacios formativos y equipamientos necesarios indicados anteriormente.

Para impartir la formación en **modalidad de teleformación**, se ha de disponer del siguiente equipamiento.

Plataforma de teleformación

La plataforma de teleformación que se utilice para impartir acciones formativas deberá alojar el material virtual de aprendizaje correspondiente, poseer capacidad suficiente para desarrollar el proceso de aprendizaje y gestionar y garantizar la formación del alumnado, permitiendo la interactividad y el trabajo cooperativo, y reunir los siguientes requisitos técnicos de infraestructura, software y servicios:

- **Infraestructura:**

Tener un rendimiento, entendido como número de alumnos que soporte la plataforma, velocidad de respuesta del servidor a los usuarios, y tiempo de carga de las páginas Web o de descarga de archivos, que permita:

- a) Soportar un número de alumnos equivalente al número total de participantes en las acciones formativas de formación profesional para el empleo que esté impartiendo el centro o entidad de formación, garantizando un hospedaje mínimo igual al total del alumnado de dichas acciones, considerando que el número máximo de alumnos por tutor es de 80 y un número de usuarios
- b) Disponer de la capacidad de transferencia necesaria para que no se produzca efecto retardo en la comunicación audiovisual en tiempo real, debiendo tener el servidor en el que se aloja la plataforma un ancho de banda mínimo de 300 Mbs,

Estar en funcionamiento 24 horas al día, los 7 días de la semana.

- **Software:**

- Compatibilidad con el estándar SCORM y paquetes de contenidos IMS.
- Niveles de accesibilidad e interactividad de los contenidos disponibles mediante tecnologías web que como mínimo cumplan las prioridades 1 y 2 de la Norma UNE 139803:2012 o posteriores actualizaciones, según lo estipulado en el capítulo III del Real Decreto 1494/2007, de 12 de noviembre.
- El servidor de la plataforma de teleformación ha de cumplir con los requisitos establecidos en la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales, por lo que el responsable de dicha plataforma ha de identificar la localización física del servidor y el cumplimiento de lo establecido sobre transferencias internacionales de datos en los artículos 40 a 43 de la citada Ley Orgánica 3/2018, de 5 de diciembre, así como, en lo que resulte de aplicación, en el Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas respecto del tratamiento de datos personales y la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE.
- Compatibilidad tecnológica y posibilidades de integración con cualquier sistema operativo, base de datos, navegador de Internet de los más usuales o servidor web, debiendo ser posible utilizar las funciones de la plataforma con complementos (plug-in) y visualizadores compatibles. Si se requiriese la instalación adicional de algún soporte para funcionalidades avanzadas, la plataforma debe facilitar el

- Disponibilidad del servicio web de seguimiento (operativo y en funcionamiento) de las acciones formativas impartidas, conforme al modelo de datos y protocolo de transmisión establecidos en el anexo V de la Orden/TMS/369/2019, de 28 de marzo.

- **Servicios y soporte:**

- Sustentar el material virtual de aprendizaje de la especialidad formativa que a través de ella se imparta.
- Disponibilidad de un servicio de atención a usuarios que de soporte técnico y mantenga la infraestructura tecnológica y que, de forma estructurada y centralizada, atienda y resuelva las consultas e incidencias técnicas del alumnado. Las formas de establecer contacto con este servicio, que serán mediante teléfono y mensajería electrónica, tienen que estar disponibles para el alumnado desde el inicio hasta la finalización de la acción formativa, manteniendo un horario de funcionamiento de mañana y de tarde y un tiempo de demora en la respuesta no
- Personalización con la imagen institucional de la administración laboral correspondiente, con las pautas de imagen corporativa que se establezcan.

Con el objeto de gestionar, administrar, organizar, diseñar, impartir y evaluar acciones formativas a través de Internet, la plataforma de teleformación integrará las herramientas y recursos necesarios a tal fin, disponiendo, específicamente, de

- Comunicación, que permitan que cada alumno pueda interaccionar a través del navegador con el tutor-formador, el sistema y con los demás alumnos. Esta comunicación electrónica ha de llevarse a cabo mediante herramientas de comunicación síncronas (aula virtual, chat, pizarra electrónica) y asíncronas (correo electrónico, foro, calendario, tablón de anuncios, avisos). Será obligatorio que cada acción formativa en modalidad de teleformación disponga, como mínimo, de un servicio de mensajería, un foro y un chat.
- Colaboración, que permitan tanto el trabajo cooperativo entre los miembros de un grupo, como la gestión de grupos. Mediante tales herramientas ha de ser posible realizar operaciones de alta, modificación o borrado de grupos de alumnos, así como creación de «escenarios virtuales» para el trabajo cooperativo de los miembros de un grupo (directorios o «carpetas» para el intercambio de archivos, herramientas para la publicación de los contenidos, y foros o chats
- Administración, que permitan la gestión de usuarios (altas, modificaciones, borrado, gestión de la lista de clase, definición, asignación y gestión de permisos, perfiles y roles, autenticación y asignación de niveles de seguridad) y
- Gestión de contenidos, que posibiliten el almacenamiento y la gestión de archivos (visualizar archivos, organizarlos en carpetas –directorios- y subcarpetas, copiar, pegar, eliminar, comprimir, descargar o cargar archivos), la publicación organizada y selectiva de los contenidos de dichos archivos, y la
- Evaluación y control del progreso del alumnado, que permitan la creación, edición y realización de pruebas de evaluación y autoevaluación y de actividades y trabajos evaluables, su autocorrección o su corrección (con retroalimentación), su calificación, la asignación de puntuaciones y la ponderación de las mismas, el registro personalizado y la publicación de calificaciones, la visualización de información estadística sobre los resultados y el progreso de cada alumno y la obtención de informes de seguimiento.

Material virtual de aprendizaje:

El material virtual de aprendizaje para el alumnado mediante el que se imparta la formación se concretará en el curso completo en formato multimedia (que mantenga una estructura y funcionalidad homogénea), debiendo ajustarse a todos los elementos de la programación (objetivos y resultados de aprendizaje) de este programa formativo que figura en el Catálogo de Especialidades Formativas y cuyo contenido

- Como mínimo, ser el establecido en el citado programa formativo del Catálogo de Especialidades Formativas.
- Estar referido tanto a los objetivos como a los conocimientos/ capacidades cognitivas y prácticas, y habilidades de gestión, personales y sociales, de manera que en su conjunto permitan conseguir los resultados de aprendizaje
- Organizarse a través de índices, mapas, tablas de contenido, esquemas, epígrafes o titulares de fácil discriminación y secuenciarse pedagógicamente de tal manera que permitan su comprensión y retención.
- No ser meramente informativos, promoviendo su aplicación práctica a través de actividades de aprendizaje (autoevaluables o valoradas por el tutor-formador) relevantes para la adquisición de competencias, que sirvan para verificar el progreso del aprendizaje del alumnado, hacer un seguimiento de sus dificultades
- No ser exclusivamente textuales, incluyendo variados recursos (necesarios y relevantes), tanto estáticos como interactivos (imágenes, gráficos, audio, video, animaciones, enlaces, simulaciones, artículos, foro, chat, etc.). de forma
- Poder ser ampliados o complementados mediante diferentes recursos adicionales a los que el alumnado pueda acceder y consultar a voluntad.
- Dar lugar a resúmenes o síntesis y a glosarios que identifiquen y definan los términos o vocablos básicos, relevantes o claves para la comprensión de los
- Evaluar su adquisición durante y a la finalización de la acción formativa a través de actividades de evaluación (ejercicios, preguntas, trabajos, problemas, casos, pruebas, etc.), que permitan medir el rendimiento o desempeño del alumnado.

Ocupaciones y puestos de trabajo relacionados

- 2711 ANALISTAS DE SISTEMAS
- 27111046 INGENIEROS TÉCNICOS EN INFORMÁTICA DE SISTEMAS
- 27191013 AUDITORES-ASESORES INFORMÁTICOS
- 27231014 ANALISTAS Y DESARROLLADORES DE REDES INFORMÁTICAS
- 27191022 INGENIEROS TÉCNICOS EN INFORMÁTICA, EN GENERAL
- 3811 TÉCNICOS EN OPERACIONES DE SISTEMAS INFORMÁTICOS
- 2723 ANALISTAS DE REDES INFORMÁTICAS
- 27111028 ANALISTAS DE SISTEMAS, NIVEL SUPERIOR (SENIOR)
- 3812 TÉCNICOS EN ASISTENCIA AL USUARIO DE TECNOLOGÍAS DE LA INFORMACIÓN
- 27111019 ANALISTAS DE SISTEMAS, NIVEL MEDIO (JUNIOR)

Requisitos oficiales de las entidades o centros de formación

Estar inscrito en el Registro de entidades de formación (Servicios Públicos de Empleo).

DESARROLLO MODULAR

MÓDULO DE FORMACIÓN 1: INTRODUCCIÓN A LA CIBERSEGURIDAD

OBJETIVO

Conocer los principios básicos de ciberseguridad, incluidos los aspectos técnicos, regulatorios y organizativos de la misma, incluyendo una aproximación al Hacking Ético para entender las principales amenazas y ataques, y cómo defenderse de ellos.

DURACIÓN EN CUALQUIER MODALIDAD DE IMPARTICIÓN:

36 horas

Teleformación:

Duración de las tutorías presenciales: 4 horas

RESULTADOS DE APRENDIZAJE

Conocimientos / Capacidades cognitivas y prácticas

- | | |
|--|---|
| • Conocimiento de los fundamentos de ciberseguridad | 0 |
| Modelos Organizativos | 0 |
| Conceptos básicos y tecnológicos | 0 |
| Role de las personas | 0 |
| • Identificación de amenazas, ataques y vulnerabilidades de los sistemas | 0 |
| Tipo de amenazas y actores relevantes en el Cibercrimen | 0 |

• Realización de una evaluación de seguridad y gestión de riesgos	0
Metodología Gestión Riesgos	0
Alcance, Activos críticos, Identificación y valoración riesgos negocio	0
Amenazas y salvaguardas.	0
Continuidad del Negocio	0
Ciclo gestión de riesgos.	0
Modelos de Gobernanza y Clasificación Información	0
Estándares y regulación:	0
• Information Security Management: ISO 2700, 27001, 27002, 27005.	
• Risk Management: ISO 31000, 31010, COBIT 5, NIST 800-39.	
• Risk Assessment: NIST 800-30.	
• Security Controls: NIST 800-53.	
• Specific: GDPR (Data Protection), OWASP (Web Application Security), PCI-DSS (payment cards), etc.	
• Risk Framework: NIST Framework.	
• Threats of ICS: NIST 800-82.	
• IACS standards: ISA/IEC-62443	0
Gestión de Incidentes	
• Conocimiento de la seguridad de los sistemas	0
Hardening: Software, Hardware y Redes	
• Sistemas Operativos	
• Aplicaciones	
• Servidores, Puestos de Trabajo, Dispositivos Móviles	
• Bases de Datos	
• Dispositivos de Red y Sistemas Industriales	
• Aproximación a los componentes de la seguridad en redes	0
Niveles OSI (Open System Interconnection Model)	0
Modelo TCP/IP: protocolos DNS, FTP, IMAP, TCP, IPv4, IPv6, HTTP.	0
Encapsulado	0
Componentes de Seguridad en Redes	
• Firewall	
• Sistemas de Detección de Intrusos (IDS)	
• Sistema Prevención Intrusiones (IPS)	
• Sistema de Detección y Prevención de Intrusiones Wireless (WIDPS)	
• Gestión de Amenazas Unificada (UTM)	

- Conocimiento y utilización de medidas de seguridad y defensa en profundidad 0
- Tipologías de Seguridad 0
- Seguridad Física: riesgos y medidas 0
- Seguridad Lógica: defensa en profundidad
- Control de Accesos: Identidad, Autenticación
- Protección
- Firewall
- Protección dispositivos
- Inteligencia
- Monitorización:
- Perímetro: pasiva/activa
- Interna: pasiva/activa
- Cadena de Suministro
- Implementación de herramientas de hacking ético 0
- Introducción al Hacking 0

Habilidades de gestión, personales y sociales

- Análisis e identificación de riesgos tecnológicos que pueden afectar a la empresa/organización.
- Capacidad para mejorar la resiliencia de los sistemas digitales que dan soporte a la empresa.
- Obtención de conocimientos para el desarrollo de una estrategia de securización de la información y generación de modelos digitales competitivos.

Resultados que tienen que adquirirse en presencial

Deberán realizarse de forma presencial las siguientes actividades:

- Utilización de herramientas de evaluación/escaneo de los niveles de seguridad de redes.
- Aplicación de herramientas de simulación de ataques
- Obtención de conocimientos para la automatización de la securización de sistemas.

OBJETIVO

Adquirir los conocimientos básicos de la industria y la transformación digital, incluida la terminología y los dispositivos utilizados en campo, los niveles ISA95, lo relacionado con la llamada industria 4.0, así como la capacitación práctica para adquirir las habilidades necesarias para programar un PLC.

DURACIÓN EN CUALQUIER MODALIDAD DE IMPARTICIÓN:

36 horas

Teleformación:

Duración de las tutorías presenciales: 4 horas

RESULTADOS DE APRENDIZAJE**Conocimientos / Capacidades cognitivas y prácticas**

- Introducción a los aspectos esenciales de la industria
 - Fabricación Industrial: sistemas comunes 0
 - Las revoluciones Industriales 0
 - Industria 4.0: digitalización 0
 - Industria Inteligente y conectada 0
- Reconocimiento de los fundamentos del control de procesos industriales
 - Tipos de procesos industriales 0
 - Fundamentos y tipos de Sistemas de Control 0
 - ICS: Sistemas de Control Industrial 0
- PID
- RTU
- HMI
- PLC
- SCADA
- DCS
- Implementación de instrumentación industrial
 - Sensores 0
 - Conversores 0
- Identificación de sistemas de comunicaciones industriales
 - 0

• ETHERCAT	
• Sistemas de producción integrados	0
Automatización Industrial	0
Gestión materiales y sistemas de identificación	0
Robotización Industrial	0
RFID y otros protocolos de identificación	0
• Implementación de sistemas avanzados de fabricación	0
Clasificación maquinaria industrial	0
Sistemas MES de fabricación asistida	0
Operaciones Industriales Digitalizadas: herramientas, evolución e implementación.	0
• Aproximación a la Industria X.0	0
Introducción a la Industria 4.0 y siguientes versiones	0

Habilidades de gestión, personales y sociales

- Conocimiento de las Redes Industriales y de los protocolos que dan soporte a los dispositivos y su conectividad
 - Obtención de habilidades para el entendimiento de la digitalización de la Industria y las tecnologías y componentes que dan soporte a estos procesos de transformación
 - Sensibilización sobre la importancia del trabajo en equipo colaborando con expertos de otras áreas y en distintos contextos para conseguir aumentar la seguridad de las instalaciones ante ataque informáticos.

Resultados que tienen que adquirirse en presencial

Deberán realizarse de forma presencial las siguientes actividades:

- Asimilación de los conocimientos y habilidades para la ejecución de programación de PLCs.
- Obtención de conocimientos para la automatización de la securización de sistemas.

OBJETIVO

Introducción a los aspectos específicos relacionados con la ciberseguridad en el entorno industrial, como sistemas ICS-SCADA, redes industriales, amenazas y estándares, para comprender todos los componentes que pueden comprometer la ciberseguridad industrial y la relación entre ellos.

DURACIÓN EN CUALQUIER MODALIDAD DE IMPARTICIÓN:

24 horas

Teleformación:

Duración de las tutorías presenciales: 4 horas

RESULTADOS DE APRENDIZAJE**Conocimientos / Capacidades cognitivas y prácticas**

• Identificación de los componentes ICS/SCADA	0
Diferencias entre la Ciberseguridad IT y OT	0
Componentes ICS	0
• Descripción de redes y protocolos industriales	0
Arquitecturas y Protocolos ICS	0
Amenazas Redes Industriales	0
• Reconocimiento de las amenazas y las vulnerabilidades industriales	0
ISA 95: Modelo Purdue clasificación	0
Escenario Riesgos Industriales	0
Introducción a Shodan	0
Protocolos y superficie de ataque	0
Historia de los ataques a redes industriales: modelos	0
Hacking Industrial	0
• Definición de los estándares y conocimiento de las mejores prácticas de ciberseguridad industrial	0
NIST SP 800-82 Securización Sistemas Control Industriales	0
NIST SP 800-53 Estrategia Gestión Riesgos	0
IEC 62443 Procesos, Personas y Tecnología	0
NERC CIP: Infraestructuras Criticas Energía (USA)	0

- Seguridad Redes
- Seguridad Activos/Dispositivos
- Seguridad datos y aplicaciones

Habilidades de gestión, personales y sociales

- Cumplimiento de las normas de seguridad y salud laboral, así como de las instrucciones técnicas de instalación.
- Apropiación del interés por la seguridad de la información y la tecnología aplicada a procesos industriales.
- Rigurosidad en el conocimiento de los conceptos de seguridad y sus riesgos asociados en plantas industriales
- Habilidad en la implementación de seguridad de redes industriales y sus controles asociados.

Resultados que tienen que adquirirse en presencial

Deberán realizarse de forma presencial las siguientes actividades:

- Utilización de herramientas de evaluación/escaneo de los niveles de seguridad de redes industriales.
- Aplicación de herramientas de simulación de ataques OT/IOT.

MÓDULO DE FORMACIÓN 4: CIBEREJERCICIOS BÁSICOS Y AVANZADOS DE CIBERSEGURIDAD INDUSTRIAL

OBJETIVO

Evaluar y reforzar los conocimientos de Ciberseguridad Industrial, mediante la ejecución de seis escenarios de ataque y defensa, definidos en la plataforma Cybertix-Cybring para redes industriales, para profundizar en los conocimientos de forma práctica.

DURACIÓN EN CUALQUIER MODALIDAD DE IMPARTICIÓN:

24 horas

Teleformación:

Duración de las tutorías presenciales: 4 horas

RESULTADOS DE APRENDIZAJE

Conocimientos / Capacidades cognitivas y prácticas

- | | |
|--|---|
| • Identificación de las vulnerabilidades ICS. | 0 |
| Detección y prevención de las mismas. | |
| • Simulación de ataques en Redes Industriales OT a través de Cyber Range | |
| • Identificación e implementación de Ataques DDOS | 0 |
| Origen | 0 |
| Detección | |

- Evaluación escenarios de Ransomware OT/IT
- Diseño seguro de redes industriales con gemelo digital
- Aplicación de herramientas de securización de redes industriales

Habilidades de gestión, personales y sociales

- Trabajo en equipo en escenarios virtuales de redes tecnológicas e infraestructuras industriales en situación de ataques y vulnerabilidades aplicable a entornos reales en tiempo real
 - Evaluación de las capacidades de anticipación y liderazgo en situaciones de riesgo en instalaciones industriales
 - Apropiación de cultura de Ciberseguridad Industrial de aplicación inmediata en procesos de digitalización en entornos operacionales.

Resultados que tienen que adquirirse en presencial

Deberán realizarse de forma presencial las siguientes actividades:

- Obtención de visión Red Team / Blue Team, entendiendo los modelos de ataque y desarrollando capacidades de protección y defensa.
- Aplicación de herramientas de simulación de ataques OT/IOT sobre el diseño de redes virtuales a priori seguras.
- Obtención de conocimientos para la automatización de la securización de sistemas.

EVALUACIÓN DEL APRENDIZAJE EN LA ACCIÓN FORMATIVA

- La evaluación tendrá un carácter teórico-práctico y se realizará de forma sistemática y continua, durante el desarrollo de cada módulo y al final del curso.
- Puede incluir una evaluación inicial de carácter diagnóstico para detectar el nivel de partida del alumnado.
- La evaluación se llevará a cabo mediante los métodos e instrumentos más adecuados para comprobar los distintos resultados de aprendizaje, y que garanticen la fiabilidad y validez de la misma.
- Cada instrumento de evaluación se acompañará de su correspondiente sistema de corrección y puntuación en el que se explicita, de forma clara e inequívoca, los criterios de medida para evaluar los resultados alcanzados por los participantes.
- La puntuación final alcanzada se expresará en términos de Apto/ No Apto.