Catálogo de Especialidades Formativas

PROGRAMA FORMATIVO

SEGURIDAD INFORMÁTICA Y PROTECCIÓN DE REDES DE COMUNICACIÓN

Versión 1

Septiembre 2025

GOBIERNO DE ESPAÑA
MINISTERIO DE TRABAJO Y ECONOMÍA SOCIAL
SERVICIO PÚBLICO DE EMPLEO ESTATAL
SEPE

SISTEMA NACIONAL DE EMPLEO

IDENTIFICACIÓN DE LA ESPECIALIDAD Y PARÁMETROS DEL CONTEXTO FORMATIVO

Denominación de la especialidad:	SEGURIDAD INFORMÁTICA Y PROTECCIÓN DE REDES DE COMUNICACIÓN
Familia Profesional:	INFORMÁTICA Y COMUNICACIONES
Área Profesional:	SISTEMAS Y TELEMÁTICA
Código:	IFCT0215
Nivel de cualificación profesional:	2

Objetivo general

Proteger sistemas informáticos y redes de comunicación frente a amenazas avanzadas, garantizando el cumplimiento normativo y aplicando técnicas actualizadas de ciberseguridad.

Relación de módulos de formación

Módulo 1	Fundamentos y Principales Amenazas en Seguridad Informática	30 horas
Módulo 2	Gestión de la Seguridad y Cumplimiento Normativo	15 horas
Módulo 3	Seguridad en Sistemas Operativos y Protección ante Malware	40 horas
Módulo 4	Seguridad Física y Herramientas de Gestión de Seguridad	25 horas
Módulo 5	Seguridad Web y en Redes	30 horas
Módulo 6	Actualización Continua y Tendencias en Ciberseguridad	10 horas

Modalidades de impartición

Presencial
Teleformación

Duración de la formación

Duración total en cualquier modalidad de impartición	150 horas
Teleformación	Duración total de las tutorías presenciales: 0 horas

Requisitos de acceso del alumnado

Acreditaciones / titulaciones	Cumplir como mínimo alguno de los siguientes requisitos: -Certificado de profesionalidad de nivel 1 -Título Profesional Básico (FP Básica) -Título de Graduado en Educación Secundaria Obligatoria (ESO) o equivalente -Título de Técnico (FP Grado medio) o equivalente -Certificado de profesionalidad de nivel 2 -Haber superado la prueba de acceso a Ciclos Formativos de Grado Medio

Acreditaciones / titulaciones	-Haber superado cualquier prueba oficial de acceso a la universidad
Experiencia profesional	No se requiere
Otros	Cuando el alumnado aspirante al curso no posea el nivel académico indicado, demostrará conocimientos suficientes a través de una prueba de acceso sobre:- Conocimientos básicos de informática (al menos sistemas operativos y ofimática básica).
Modalidad de teleformación	Además de lo indicado anteriormente, los participantes han de tener las destrezas suficientes para ser usuarios de la plataforma virtual en la que se apoya la acción formativa.

Justificación de los requisitos del alumnado
La acreditación de la titulación se justificará mediante la presentación del título o certificado académico correspondiente. La acreditación de otros requisitos se realizará mediante una prueba o mediante aportación de cualquier evidencia documental de haber cursado una formación en la materia exigida.

Prescripciones de formadores y tutores

Acreditación requerida	Cumplir como mínimo alguno de los siguientes requisitos: -Licenciado/a, Ingeniero/a, Arquitecto/a o el Título de Grado correspondiente u otros títulos equivalentes en los ámbitos de conocimiento de ingeniería informática y de sistemas, ingeniería eléctrica, ingeniería electrónica, ingeniería de la telecomunicación, ingeniería industrial, matemáticas o estadística. -Diplomado/a, Ingeniero/a Técnico/a, Arquitecto/a Técnico/a o el Título de Grado correspondiente y otros títulos equivalentes en los ámbitos de conocimiento de ingeniería informática y de sistemas, ingeniería eléctrica, ingeniería electrónica, ingeniería de la telecomunicación, ingeniería industrial, matemáticas o estadística. -Técnico/a o Técnico/a Superior de la familia profesional de Informática y Comunicaciones en el área profesional de Sistemas y telemática. -Certificado de profesionalidad de nivel 3 de la familia profesional de Informática y Comunicaciones en el área profesional de Sistemas y telemática.
Experiencia profesional mínima requerida	La experiencia se acreditará en el ámbito de la especialidad (seguridad, programadores, sistemas o similar) y será de al menos 12 meses, cuando no se disponga de la titulación requerida.
Competencia docente	Se requiere acreditar un mínimo de 500 horas de experiencia docente o 250 horas si la experiencia está relacionada con especialidades o certificados de profesionalidad de la misma familia profesional en la que está encuadrada la presente especialidad.O estar en posesión de alguna de las siguientes titulaciones: -Certificado de Profesionalidad de Docencia de la Formación Profesional para el empleo (SSCE0110) o equivalente. -Certificado de Aptitud Pedagógica (CAP). -Título de licenciado en Pedagogía, Psicopedagogía o de

Competencia docente	Maestro en cualquiera de sus especialidades, graduado universitario en el ámbito de la Psicología o de la Pedagogía, o un título universitario oficial de posgrado en los citados ámbitos. -Título profesional de Especialización Didáctica, el Certificado de Cualificación Pedagógica, el Máster Universitario habilitante para el ejercicio de las Profesiones Reguladas de Profesor de Educación Secundaria Obligatoria y Bachillerato, Formación Profesional y Escuelas Oficiales de idiomas.
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.

Justificación de las prescripciones de formadores y tutores

La acreditación de la titulación se justificará mediante la presentación del título o certificación académica correspondiente. La experiencia profesional mediante vida laboral actualizada o certificado de funciones expedido por organización en la que prestó sus servicios. La competencia docente a través de vida laboral actualizada y/o alguna de las titulaciones acreditativas contempladas.

Requisitos mínimos de espacios, instalaciones y equipamientos

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

Espacio formativo	Equipamiento
Aula de gestión	- 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 participantes - Software específico para el aprendizaje de cada acción formativa. - Sistema operativo Kali Linux en última versión (en máquina física o virtual)- Herramientas de seguridad: Wireshark, Nessus, OpenVPN, etc.- Herramientas SIEM: OSSIM/AlienVault, Splunk, IBM QRadar, etc.

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.

Aula virtual

Características
• La impartición de la formación mediante aula virtual se ha de estructurar y organizar de forma que se garantice en todo momento que exista conectividad sincronizada entre las personas formadoras y el alumnado participante así como bidireccionalidad en las comunicaciones. • Se deberá contar con un registro de conexiones generado por la aplicación del aula virtual en que se identifique, para cada acción formativa desarrollada a través de este medio, las personas participantes en el aula, así como sus fechas y tiempos de conexión.

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 concurrentes del 40% de ese alumnado.

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, suficiente en bajada y subida.

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 cumplimento 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 acceso al mismo sin coste.
- 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 superior a 48 horas laborables.
- 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 herramientas 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 privados para los miembros de cada grupo).
- 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 la gestión de acciones formativas.
- 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 creación de contenidos.
- 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 cumpla estos requisitos:

- 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 previstos.
- Organizarse a través de índices, mapas, tablas de contenido, esquemas, epígrafes o titulares de fácil discriminación y secuenciase pedagógicamente de tal manera que permiten 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 de aprendizaje y prestarle el apoyo adecuado.

- 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 periódica.
- 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 aprendizajes.
- 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

- 27111019 ANALISTAS DE SISTEMAS, NIVEL MEDIO (JUNIOR)
- 27111028 ANALISTAS DE SISTEMAS, NIVEL SUPERIOR (SENIOR)
- 27111037 INGENIEROS INFORMÁTICOS
- 27111046 INGENIEROS TÉCNICOS EN INFORMÁTICA DE SISTEMAS
- 27191013 AUDITORES-ASESORES INFORMÁTICOS
- 27211018 ADMINISTRADORES DE SISTEMAS DE REDES
- 27231014 ANALISTAS Y DESARROLLADORES DE REDES INFORMÁTICAS
- 38111011 TÉCNICOS EN OPERACIONES DE SISTEMAS INFORMÁTICOS
- 38131017 TÉCNICOS DE SOPORTE DE REDES

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:	**Fundamentos y Principales Amenazas en Seguridad Informática**

OBJETIVO

Comprender los principios básicos de la seguridad informática y los tipos de amenazas comunes, así como las metodologías para prevenir y mitigar riesgos.

DURACIÓN EN CUALQUIER MODALIDAD DE IMPARTICIÓN: 30 horas

Teleformación: Duración de las tutorías presenciales: 0 horas

RESULTADOS DE APRENDIZAJE

Conocimientos / Capacidades cognitivas y prácticas

- Conocimiento de las bases de la Seguridad Informática - Definición y objetivos de la ciberseguridad - Principios de seguridad (confidencialidad, integridad y disponibilidad) - Conceptos básicos de criptografía - Diferencia entre seguridad física y lógica - Clasificación de la seguridad según medidas y controles aplicados
- Identificación de principales Problemas y Amenazas - Configuraciones de redes y su impacto en la seguridad - Identificación de tipos de vulnerabilidades - Clasificación de malware (ransomware, spyware, adware, etc.) - Amenazas avanzadas persistentes (APT) - Prácticas de ingeniería social y phishing - Ciberataques y técnicas de hacking ético
- Conocimiento de conceptos sobre sostenibilidad. -Optimización del consumo energético mediante la gestión eficiente de recursos. -Gestión eficiente del almacenamiento para reducir el desperdicio de espacio. -Implementación de prácticas de reciclaje y disposición responsable de hardware. -Uso de herramientas de monitorización para identificar y reducir el consumo innecesario de recursos.

Habilidades de gestión, personales y sociales

- Pensamiento crítico para analizar los principios fundamentales de la seguridad informática para identificar y proteger los sistemas contra amenazas comunes.
- Capacidad analítica en la identificación de amenazas de seguridad.
- Actitud de vigilancia medioambiental, garantizando la eficiencia y ahorro energético de sistemas y entornos de trabajo.

MÓDULO DE FORMACIÓN 2: Gestión de la Seguridad y Cumplimiento Normativo

OBJETIVO

Gestionar la seguridad informática y asegurar el cumplimiento de normativas como RGPD y LOPDGDD.

DURACIÓN EN CUALQUIER MODALIDAD DE IMPARTICIÓN: 15 horas

Teleformación: Duración de las tutorías presenciales: 0 horas

RESULTADOS DE APRENDIZAJE

Conocimientos / Capacidades cognitivas y prácticas

- Conocimiento de la principal legislación sobre protección y seguridad.
    - Ley Orgánica de Protección de Datos y Garantía de Derechos Digitales (LOPDGDD)
    - Reglamento General de Protección de Datos (RGPD)
    - Normas ISO/IEC 27001 y familia ISO 27000
- Gestión de riesgos (metodologías como MAGERIT, OCTAVE, NIST)
- Elaboración de políticas y planes de seguridad
- Realización de auditorías de seguridad y cumplimiento.

Habilidades de gestión, personales y sociales

- Habilidades de planificación en el desarrollo de políticas y planes de seguridad adaptados a la estructura y necesidades de la empresa, garantizando una protección integral.
- Adaptación a las necesidades y políticas empresariales.
- Preocupación por el seguimiento y cumplimiento de políticas de protección de datos.
- Preocupación por el seguimiento y cumplimiento de políticas y regulaciones de seguridad.

MÓDULO DE FORMACIÓN 3:	Seguridad en Sistemas Operativos y Protección ante Malware

OBJETIVO

Configurar y proteger sistemas operativos para reducir riesgos, detectando y neutralizando amenazas de malware mediante herramientas de seguridad.

DURACIÓN EN CUALQUIER MODALIDAD DE IMPARTICIÓN: 40 horas

Teleformación: Duración de las tutorías presenciales: 0 horas

RESULTADOS DE APRENDIZAJE

Conocimientos / Capacidades cognitivas y prácticas

- Implementación de seguridad en Sistemas Operativos - Políticas en Windows 10/11 y Windows Server - Políticas en distribuciones Linux (Ubuntu/Debian, CentOS, etc.) - Políticas en macOS - Configuración de políticas y actualización de sistemas - Gestión de usuarios y permisos
- Protección ante Malware y Amenazas Avanzadas - Reconocimiento de tipos de malware - Ransomware y su impacto en las empresas - Malware móvil y en dispositivos IoT - Técnicas de detección y análisis de malware - Uso de programas antimalware y antivirus avanzados - Estrategias de protección y respuesta ante incidentes.

Habilidades de gestión, personales y sociales

- Atención a la seguridad de los sistemas.
- Prevención para detectar y responder eficazmente a ataques de malware mediante el uso de herramientas especializadas, protegiendo la infraestructura de la empresa.

MÓDULO DE FORMACIÓN 4: Seguridad Física y Herramientas de Gestión de Seguridad

OBJETIVO

Implementar medidas de seguridad física y utilizar Sistemas de Gestión de Eventos e Información de Seguridad (SIEM) para monitorizar, gestionar y responder a incidentes de seguridad.

DURACIÓN EN CUALQUIER MODALIDAD DE IMPARTICIÓN: 25 horas

Teleformación: Duración de las tutorías presenciales: 0 horas

RESULTADOS DE APRENDIZAJE

Conocimientos / Capacidades cognitivas y prácticas

- Gestión de la seguridad Física y del Entorno - Importancia de la seguridad física en entornos informáticos - Control de acceso físico a instalaciones - Protección contra desastres naturales y ambientales - Seguridad en centros de datos - Medidas contra robo, vandalismo y sabotaje
- Gestión de la seguridad en la Empresa y Gestión de SIEM - Exploración de herramientas SIEM (OSSIM/AlienVault, Splunk, IBM QRadar, etc.) - Monitoreo y correlación de eventos de seguridad - Planes de acción y respuesta ante incidentes - Fundamentos de ciberinteligencia y análisis de amenazas.

Habilidades de gestión, personales y sociales

- Adaptación a las necesidades y políticas empresariales.
- Preocupación por el seguimiento y cumplimiento de políticas de protección de datos.
- Preocupación por el seguimiento y cumplimiento de políticas y regulaciones de seguridad.
- Optimización de recursos.

MÓDULO DE FORMACIÓN 5: Seguridad Web y en Redes

OBJETIVO

Mitigar vulnerabilidades en aplicaciones web y redes, asegurando comunicaciones mediante la implementación de protocolos y configuraciones seguras.

DURACIÓN EN CUALQUIER MODALIDAD DE IMPARTICIÓN: 30 horas

Teleformación: Duración de las tutorías presenciales: 0 horas

RESULTADOS DE APRENDIZAJE

Conocimientos / Capacidades cognitivas y prácticas

- Gestión de la seguridad Web y Aplicaciones - Reconocimiento de vulnerabilidades en aplicaciones web (OWASP Top 10) - Identificación de ataques comunes (SQL Injection, XSS, CSRF, etc.) - Buenas prácticas en desarrollo seguro de software - Uso de certificados SSL/TLS y HTTPS - Herramientas para análisis y pruebas de penetración en aplicaciones web
- Gestión de la seguridad en Redes y Comunicaciones - Protocolos y arquitectura de redes seguras - Seguridad en redes inalámbricas (Wi-Fi 6 y 6E) - Configuración segura de routers y firewalls - Redes privadas virtuales (VPN) y acceso remoto seguro - Segmentación de redes y microsegmentación - Protección contra ataques DDoS.

Habilidades de gestión, personales y sociales

- Pensamiento preventivo para identificar y corregir vulnerabilidades en aplicaciones web antes de que sean explotadas mediante el uso de análisis de vulnerabilidades y pruebas de penetración. •Resolución de problemas: Implementar soluciones de seguridad avanzadas como VPN, firewalls, y segmentación de redes para prevenir y mitigar ataques como DDoS.

MÓDULO DE FORMACIÓN 6: **Actualización Continua y Tendencias en Ciberseguridad**

OBJETIVO

Mantenerse al día con las nuevas tecnologías y tendencias en ciberseguridad para proteger mejor los sistemas.

DURACIÓN EN CUALQUIER MODALIDAD DE IMPARTICIÓN: 10 horas

Teleformación: Duración de las tutorías presenciales: 0 horas

RESULTADOS DE APRENDIZAJE

Conocimientos / Capacidades cognitivas y prácticas

- Actualización de la Seguridad
    - Importancia de la actualización constante en seguridad informática
    - Recursos y herramientas para mantenerse actualizado (certificaciones, blogs, foros)
- Identificación de tendencias en ciberseguridad
    - Inteligencia artificial y machine learning en ciberseguridad
    - Ciberseguridad en entornos cloud y multi-nube
    - Seguridad en dispositivos IoT y sistemas industriales (ICS/SCADA)
    - Normativas y marcos emergentes (Zero Trust, SASE).

Habilidades de gestión, personales y sociales

- Análisis proactivo.
- Fomento del trabajo colaborativo.
- Fomento de la capacidad para analizar de manera crítica las implementaciones y resultados propios y del equipo de trabajo para poder mejorarlos, corregirlos o exponerlos.
- Evaluación constante del rendimiento.

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 explicite, 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.