Catálogo de Especialidades Formativas

PROGRAMA FORMATIVO

CIBERSEGURIDAD AVANZADA

Marzo 2024

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:	CIBERSEGURIDAD AVANZADA
Código:	CTRD0031
Nivel de cualificación profesional:	3
Especialidad de carácter intersectorial:	Digitales / Ofimática / TICs

Objetivo general

Aplicar habilidades avanzadas de ciberseguridad en actividades del ámbito profesional y personal, en el entorno digital

Relación de módulos de formación

Módulo 1	Análisis de amenazas cibernéticas avanzadas.	20 horas
Módulo 2	Respuesta a incidentes cibernéticos.	30 horas
Módulo 3	Arquitecturas de seguridad avanzadas.	20 horas
Módulo 4	Ingeniería social y concienciación de la seguridad.	20 horas
Módulo 5	Ética y legalidad en ciberseguridad.	20 horas

Modalidades de impartición

Presencial
Teleformación

Duración de la formación

Duración total en cualquier modalidad de impartición	110 horas
Teleformación	Duración total de las tutorías presenciales: 22 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 -Haber superado cualquier prueba oficial de acceso a la universidad -Certificado de profesionalidad de nivel 3 -Título de Grado o equivalente -Título de Postgrado (Máster) o equivalente
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 virtual en la que se apoya la acción formativa.

Prescripciones de formadores y tutores

Acreditación requerida	Cumplir como mínimo alguno de los siguientes requisitos: • Licenciado, Ingeniero, Arquitecto o el Título de Grado correspondiente u otros títulos equivalentes. • Diplomado, Ingeniero Técnico, Arquitecto Técnico o el Título de Grado correspondiente u otros títulos equivalentes.
Experiencia profesional mínima requerida	Experiencia práctica en ciberseguridad.
Competencia docente	• Experiencia docente acreditable de al menos 60 horas en modalidad presencial o e-learning en los últimos dos años impartiendo formación relacionada con competencias digitales. • Certificado de Profesionalidad de Docencia de la Formación Profesional para la Ocupación. • Máster Universitario de Formador de Formadores u otras acreditaciones oficiales equivalentes.
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 m²	2.4 m² / 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/as. • Software específico para el aprendizaje de la acción formativa

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.
Otras especificaciones
- Pizarra virtual interactiva. - PC instalado en red con posibilidad de impresión de documentos, cañón con proyección e Internet para el formador. - Herramientas de comunicación y audio. - Software específico para el aprendizaje de cada acción formativa: • Paquete integrado de ofimática. • Visor de documentos en formato pdf. • Plataforma de videoconferencia (Zoom). - Conexión a Internet: banda ancha con cable o inalámbrica (3G o 4G/LTE). - Altavoces y un micrófono: integrados o con complemento USB o Bluetooth inalámbricos. - Cámara web o cámara web HD: integrada o con complemento USB o bien una cámara HD o videocámara HD con tarjeta de captura de vídeo. - Navegadores: iOS/iPadOS: Safari5+, Chrome y Android: Webkit (predeterminado), Chrome. - Cualquier procesador de 1 GHz de un núcleo o superior (que no sea Intel).

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 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

- 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 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

- 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.

Requisitos oficiales de las entidades o centros de formación

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

Centro Móvil

Es posible impartir esta especialidad en centro móvil.

DESARROLLO MODULAR

MÓDULO DE FORMACIÓN 1: Análisis de amenazas cibernéticas avanzadas.

OBJETIVO

Conocer, identificar, analizar y comprender las causas, el origen y las amenazas cibernéticas más avanzadas en el contexto del uso de herramientas de software y hardware conectado y no conectado a internet.

DURACIÓN EN CUALQUIER MODALIDAD DE IMPARTICIÓN: 20 horas

Teleformación: Duración de las tutorías presenciales: 11 horas

RESULTADOS DE APRENDIZAJE

Conocimientos / Capacidades cognitivas y prácticas

• Conocimiento de los tipos de amenazas cibernéticas avanzadas, sus características y objetivos.
• Análisis de las técnicas de ataque avanzadas utilizadas por los ciberdelincuentes.
• Uso de herramientas y técnicas de análisis de amenazas para identificar y comprender las amenazas cibernéticas avanzadas.

Habilidades de gestión, personales y sociales

• Implementación de medidas de seguridad para proteger los sistemas, redes y datos de una organización.
• Concienciación acerca de los riesgos que conlleva el uso de dispositivos digitales conectados a la red.

Resultados que tienen que adquirirse en presencial

Deberán realizarse de forma presencial las siguientes actividades:

• Ante un supuesto práctico, desarrollo de competencias analíticas para identificar y comprender las amenazas cibernéticas.
• Identificación y evaluación de los riesgos cibernéticos a los que están expuestos los sistemas, redes y datos de una organización.
• Desarrollo de planes de seguridad para proteger los sistemas, redes y datos de una organización.

MÓDULO DE FORMACIÓN 2: Respuesta a incidentes cibernéticos.

OBJETIVO

Adquirir los conocimientos y habilidades necesarios para identificar y comprender los incidentes cibernéticos, implementar las medidas de respuesta a incidentes adecuadas, llevar a cabo las tareas de respuesta a incidentes de forma eficaz y documentar los incidentes cibernéticos.

DURACIÓN EN CUALQUIER MODALIDAD DE IMPARTICIÓN: 30 horas

Teleformación: Duración de las tutorías presenciales: 11 horas

RESULTADOS DE APRENDIZAJE

Conocimientos / Capacidades cognitivas y prácticas

• Aplicación de medidas de seguridad avanzadas para proteger los sistemas operativos.
• Comprensión del ciclo de vida de un incidente cibernético.
• Aplicación de los procedimientos de respuesta a incidentes.
• Identificación de las herramientas y técnicas de respuesta a incidentes.
• Aplicación de las herramientas y técnicas de respuesta a incidentes.
• Explicación de los conceptos básicos de la seguridad de los datos.
• Desarrollo de habilidades de la comunicación y gestión de incidentes.
• Creación de documentación de incidentes.

Habilidades de gestión, personales y sociales

• Concienciación de los riesgos que conlleva el uso de dispositivos digitales conectados a la red.
• Comprensión de la naturaleza de las amenazas cibernéticas, las técnicas utilizadas por los ciberdelincuentes y las consecuencias potenciales de un ataque.
• Valoración de la importancia de la formación continua para el conocimiento de las últimas tendencias en ciberseguridad.
• Sensibilización en el trabajo eficaz con otros profesionales de la ciberseguridad para resolver problemas complejos.

Resultados que tienen que adquirirse en presencial

Deberán realizarse de forma presencial las siguientes actividades:

• Concienciación de los riesgos que conlleva el uso de dispositivos digitales conectados a la red.
• Comprensión de la naturaleza de las amenazas cibernéticas, las técnicas utilizadas por los ciberdelincuentes y las consecuencias potenciales de un ataque.
• Valoración de la importancia de la formación continua para el conocimiento de las últimas tendencias en ciberseguridad.
• Sensibilización en el trabajo eficaz con otros profesionales de la ciberseguridad para resolver problemas complejos.

MÓDULO DE FORMACIÓN 3: Arquitecturas de seguridad avanzadas.

OBJETIVO

Conocer los principios y conceptos básicos para diseñar, implementar y gestionar, las arquitecturas de seguridad avanzadas en el contexto de una organización.

DURACIÓN EN CUALQUIER MODALIDAD DE IMPARTICIÓN: 20 horas

Teleformación: Duración de las tutorías presenciales: 0 horas

RESULTADOS DE APRENDIZAJE

Conocimientos / Capacidades cognitivas y prácticas

- Explicación de los conceptos y principios básicos de las arquitecturas de seguridad avanzadas.
- Análisis de los requisitos de seguridad de una organización.
- Diseño de arquitecturas de seguridad avanzadas.
- Implementación de arquitecturas de seguridad avanzadas.

Habilidades de gestión, personales y sociales

- Desarrollo de actitudes y habilidades específicas, como la adaptabilidad, la creatividad, la agilidad y la innovación, actitudes y habilidades necesarias para adaptarse a los cambios constantes que se producen en el entorno laboral, así como para generar nuevas ideas y soluciones.
- Destreza en el diseño e implementación de arquitecturas de seguridad avanzadas y su despliegue a través de la organización y los equipos, tomando conciencia de la importancia de la comunicación efectiva.
- Iniciativa para trabajar de forma eficaz en entornos de diseño e implementación de arquitecturas de seguridad avanzadas en equipo para lograr un trabajo colaborativo eficiente.

MÓDULO DE FORMACIÓN 4: Ingeniería social y concienciación de la seguridad.

OBJETIVO

Conocer y comprender los conceptos básicos de la ingeniería social, así como identificar sus técnicas más comunes, y aplicar los métodos de prevención asociados.

DURACIÓN EN CUALQUIER MODALIDAD DE IMPARTICIÓN: 20 horas

Teleformación: Duración de las tutorías presenciales: 0 horas

RESULTADOS DE APRENDIZAJE

Conocimientos / Capacidades cognitivas y prácticas

- Definición de ingeniería social y cómo funciona.
- Identificación de las técnicas de ingeniería social más comunes
- Evaluación y análisis de las técnicas de ingeniería social: suplantación de identidad, pretexto, cebo y presión.
- Explicación de los métodos de prevención de ingeniería social.
- Aplicación de medidas de protección de ataques de ingeniería social.
- Aplicación de métodos de prevención de ingeniería social.

Habilidades de gestión, personales y sociales

- Liderazgo y motivación para la adopción de prácticas de seguridad en equipo.
- Iniciativa para la toma de decisiones informadas sobre cómo proteger la información y los sistemas desde la empatía con las víctimas.
- Efectividad para comunicar los riesgos de la ingeniería social.
- Desarrollo de la resiliencia necesaria para recuperar el sistema de un ataque de ingeniería social.
- Destreza en la gestión de proyectos de seguridad.

MÓDULO DE FORMACIÓN 5: Ética y legalidad en ciberseguridad.

OBJETIVO

Adquirir los conocimientos y habilidades necesarios para actuar de forma ética y legal en el ámbito de la ciberseguridad.

DURACIÓN EN CUALQUIER MODALIDAD DE IMPARTICIÓN: 20 horas

Teleformación: Duración de las tutorías presenciales: 0 horas

RESULTADOS DE APRENDIZAJE

Conocimientos / Capacidades cognitivas y prácticas

- Descripción de los principios éticos de la ciberseguridad.
- Conocimiento de la legislación aplicable a la ciberseguridad.
- Aplicación de los principios éticos y la legislación a la práctica de la ciberseguridad.

Habilidades de gestión, personales y sociales

- Liderazgo para promover que los demás adopten prácticas de seguridad éticas y legales en equipo.
- Iniciativa para la toma de decisiones informadas sobre cómo cumplir con la legalidad, proteger la información y los sistemas desde la empatía con las víctimas con una perspectiva moral.
- Efectividad para comunicar los riesgos de la ingeniería social.
- Desarrollo de la resiliencia necesaria para recuperar el sistema de un ataque de ingeniería social.
- Destreza en la gestión de proyectos de seguridad.

ORIENTACIONES METODOLÓGICAS

Todo el programa se basa en la realización de ejercicios prácticos para una mejor asimilación de conceptos. En cada unidad se han incluido casos prácticos a llevar a cabo, así como el estudio de casos de éxito reales.

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.