Catálogo de Especialidades Formativas

PROGRAMA FORMATIVO

DESARROLLO DE SISTEMAS DE LA CIBERSEGURIDAD

Agosto 2023

GOBIERNO DE ESPAÑA MINISTERIO DE TRABAJO Y ECONOMÍA SOCIAL SEPE

SISTEMA NACIONAL DE EMPLEO

IDENTIFICACIÓN DE LA ESPECIALIDAD Y PARÁMETROS DEL CONTEXTO FORMATIVO

Denominación de la especialidad:	DESARROLLO DE SISTEMAS DE LA CIBERSEGURIDAD
Familia Profesional:	INFORMÁTICA Y COMUNICACIONES
Área Profesional:	SISTEMAS Y TELEMÁTICA
Código:	IFCT0048
Nivel de cualificación profesional:	2

Objetivo general

Desarrollar políticas y sistemas de Ciberseguridad como personal de soporte para la gestión de proyectos

Relación de módulos de formación

Módulo 1	Introducción a la ciberseguridad y arquitectura de redes	35 horas
Módulo 2	Hacking ético y ataque	75 horas
Módulo 3	Post-Explotación y Password Cracking	35 horas
Módulo 4	Hacking Wifi y Malware	30 horas
Módulo 5	Auditorías web, Hacking infraestructuras y forense	50 horas
Módulo 6	Programación en Python y Seguridad	30 horas

Modalidades de impartición

Presencial
Teleformación

Duración de la formación

Duración total en cualquier modalidad de impartición	255 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 -Haber superado cualquier prueba oficial de acceso a la universidad

Experiencia profesional	No se requiere
Otros	Cuando el aspirante no disponga del nivel académico mínimo o de la experiencia profesional, demostrará conocimientos y competencias suficientes para participar en el curso con aprovechamiento mediante una prueba de acceso.
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: • Licenciatura, ingeniería, arquitectura o el título de grado correspondiente u otros títulos equivalentes. • Diplomatura, ingeniería técnica, arquitectura técnica o el título de grado correspondiente u otros títulos equivalentes. • Técnico/a superior de informática de la familia profesional de informática y comunicaciones. • Certificados de profesionalidad de nivel 3 de la familia profesional de informática y comunicaciones.
Experiencia profesional mínima requerida	En caso de que no se cumpla con los requisitos descritos anteriormente, se pedirá una experiencia laboral mínima acreditable de 2 años en el sector de la programación y/o consultoría tecnológica
Competencia docente	Cumplir como mínimo alguno de los siguientes requisitos: • Será necesario tener formación metodológica o experiencia docente. • 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 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. - Software específico para el aprendizaje de cada acción formativa: o Lenguajes de programación: Python. o Entorno de hacking ético: Herramientas de redes (Whois, Trceroute, ...), OWASP, Google Dorks, Hydra, Hashcat, Ophcrack, Airgeddon, otros entornos. o Gestión de OS: Windows, Linux.

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

  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.

Ocupaciones y puestos de trabajo relacionados

- 27211018 ADMINISTRADORES DE SISTEMAS DE REDES
- 27231014 ANALISTAS Y DESARROLLADORES DE REDES INFORMÁTICAS
- 27211027 ADMINISTRADORES DE BASES DE DATOS

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 y arquitectura de redes**

OBJETIVO

Analizar los requerimientos técnicos y los conceptos básicos de la seguridad, la privacidad y las amenazas en el entorno de las redes.

DURACIÓN EN CUALQUIER MODALIDAD DE IMPARTICIÓN: 35 horas

Teleformación: Duración de las tutorías presenciales: 0 horas

RESULTADOS DE APRENDIZAJE

Conocimientos / Capacidades cognitivas y prácticas

- **Introducción de los elementos de la ciberseguridad**
  - La seguridad en Internet
  - Redes LAN – WAN
  - Internet
  - Privacidad – Anonimato
  - Seguridad Wifi
  - Amenazas
  - Contraseñas seguras
  - Correo seguro
  - Backup / Recuperación / Borrado
  - Antivirus
- **Análisis del entorno de la arquitectura de redes**
  - Introducción a las redes
  - Modelo OSI
  - Creación de laboratorios
  - NAT vs Bridge en virtual
  - GNS3.
  - Creación de redes locales

Habilidades de gestión, personales y sociales

- Asimilación de los componentes de la seguridad en las redes
- Disposición para crear contraseñas y entornos seguros

MÓDULO DE FORMACIÓN 2: Hacking ético y ataque

OBJETIVO

Aplicar las operaciones para la creación de laboratorios virtuales mediante herramientas de redes.

DURACIÓN EN CUALQUIER MODALIDAD DE IMPARTICIÓN: 75 horas

Teleformación: Duración de las tutorías presenciales: 0 horas

RESULTADOS DE APRENDIZAJE

Conocimientos / Capacidades cognitivas y prácticas

- **Definición del Hacking Ético**
  - Utilización de las diferentes distribuciones específicas
  - Resumen de herramientas para la recolección de información. Herramientas de red (Whois, Traceroute, ping ...), herramientas de Kali, Google Dorks, plugins de Firefox útiles y técnicas OSINT
- **Identificación de puertos y vulnerabilidades**
  - Análisis de servicios y puertos (NMAP y evasión de Firewalls)
- **Síntesis de vulnerabilidades**
  - Identificación de diferentes escáneres de vulnerabilidades (Acunetix, Nessus, Nikto, Cmsmap, Wpscan, Zap y Burp Suite Pro)
  - Clasificación de las vulnerabilidades
- **Simulación de un ataque**
  - Análisis de la situación, búsqueda de exploits (metasploit y pivoting)
  - Representación de un ataque manual y automatizado, ataque directo e inverso.

Habilidades de gestión, personales y sociales

- Asimilación de las fases para la creación de laboratorios virtuales con NAT y Bridge
- Hábito en el uso de la herramienta GNS3 para la creación de redes locales

MÓDULO DE FORMACIÓN 3: Post-Explotación y Password Cracking

OBJETIVO

Ejecutar técnicas específicas para el hacking, el análisis de vulnerabilidades y la post-explotación de información.

DURACIÓN EN CUALQUIER MODALIDAD DE IMPARTICIÓN: 35 horas

Teleformación: Duración de las tutorías presenciales: 0 horas

RESULTADOS DE APRENDIZAJE

Conocimientos / Capacidades cognitivas y prácticas

- **Identificación de los ámbitos de la Post-Explotación**
  - Extracción de información sensible y útil, y escalada de privilegios.
  - Tipos de ataque y escalada posterior (directos, inversos e ingeniería social)
- **Análisis de la sección del Password Cracking**
  - Ataques online y offline
  - Herramientas de recuperación (Hashcat, Hydra, Ophcrack, Metasploit i John)

Habilidades de gestión, personales y sociales

- Asimilación de técnicas de cracking de contraseñas en entorno online y offline
- Rigor en la adquisición de herramientas específicas para la post-explotación de información

MÓDULO DE FORMACIÓN 4: Hacking Wifi y Malware

OBJETIVO

Aplicar las técnicas de hacking de redes Wifi y evasión de sistemas de seguridad.

DURACIÓN EN CUALQUIER MODALIDAD DE IMPARTICIÓN: 30 horas

Teleformación: Duración de las tutorías presenciales: 0 horas

RESULTADOS DE APRENDIZAJE

Conocimientos / Capacidades cognitivas y prácticas

- **Asimilación de los principales aspectos del Hacking Wifi**
  - Material necesario
  - Uso de Airgeddon
- **Identificación de los principales tipos de Malware**
  - Configuración y creación de troyano
  - Métodos de infección y evasión de antivirus

Habilidades de gestión, personales y sociales

- Implicación en el uso de herramientas de hacking de redes mediante Airgeddon.
- Canalización de técnicas para la configuración de métodos de infección y evasión de antivirus.

MÓDULO DE FORMACIÓN 5: Auditorías web, Hacking infraestructuras y forense

OBJETIVO

Analizar aspectos técnicos relacionados con la taxonomía de los ataques cibernéticos.

DURACIÓN EN CUALQUIER MODALIDAD DE IMPARTICIÓN: 50 horas

Teleformación: Duración de las tutorías presenciales: 0 horas

RESULTADOS DE APRENDIZAJE

Conocimientos / Capacidades cognitivas y prácticas

- **Interpretación del ámbito de las Auditorias Web**
  - Taxonomía de un ataque
  - Ejemplos de vulnerabilidades y ataques (inyección SQL y de código, LFI, RFI i Xss)
- **Representación de las diferentes infraestructuras de Hacking**
  - Redes
  - Escalada de privilegios y Shell Scripting
- **Describir los aspectos de la informática forense clasificándola**
  - Análisis forense a móviles y de datos
  - Identificación de la evidencia digital y elaboración del informe

Habilidades de gestión, personales y sociales

- Coordinación de las diferentes taxonomías de ataque, vulnerabilidades y ataques con inyección SQL, XSS, LFI y código RFI
- Asimilación de técnicas para hacking de redes y sistemas operativos
- Reflexión de conceptos sobre informática forense, evidencia digital y análisis de datos
- Rigor técnico para el desarrollo de informes forense

MÓDULO DE FORMACIÓN 6: Programación en Python y Seguridad

OBJETIVO

Analizar los requerimientos técnicos y el diseño necesario para el desarrollo de programación con Python.

DURACIÓN EN CUALQUIER MODALIDAD DE IMPARTICIÓN: 30 horas

Teleformación: Duración de las tutorías presenciales: 0 horas

RESULTADOS DE APRENDIZAJE

Conocimientos / Capacidades cognitivas y prácticas

- **Aplicación del ámbito de la Programación en Python dentro del entorno de la ciberseguridad**
- Instalación de Python en Windows, Linux y librerías externas y entorno IDE
- Introducción a la programación dentro de Python (estructuras de control, funciones, módulos, objetos, análisis de datos y recolección de información y escáner en red)
- **Distinción de los diferentes elementos de la seguridad**
- Instalación de Firewall y monitorización (configuración básica y creación de reglas)
- Instalación de UTM (configuración y análisis UTM)

Habilidades de gestión, personales y sociales

- Asimilación de procesos de desarrollo de software Python para el análisis y la recolección de información
- Disposición para instalar y configurar firewalls y UTMs
- Coordinación para la monitorización de redes e instalación de sistemas IDS

- 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.

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.

- La puntuación final alcanzada se expresará en términos de Apto/ No Apto.