Catálogo de Especialidades Formativas

PROGRAMA FORMATIVO

Test de intrusión

Mayo 2022

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:	TEST DE INTRUSIÓN
Familia Profesional:	INFORMÁTICA Y COMUNICACIONES
Área Profesional:	SISTEMAS Y TELEMÁTICA
Código:	IFCT125
Nivel de cualificación profesional:	4

Objetivo general

Manejar tanto los procedimientos como las herramientas y técnicas para atacar los sistemas informáticos, identificando si las aplicaciones tienen alguna vulnerabilidad y si ésta es explotable en las condiciones del entorno de trabajo, con las medidas de protección disponibles.

Relación de módulos de formación

Módulo 1	Test de intrusión y tipología de herramientas	8 horas
Módulo 2	Metodologías de Test de intrusión	20 horas
Módulo 3	Herramientas para la ejecución de test de intrusión	18 horas
Módulo 4	Resultados e informes	6 horas
Módulo 5	Planificación y ejecución de un test de intrusión.	8 horas

Modalidades de impartición

Presencial

Teleformación

Duración de la formación

Duración total en cualquier modalidad de impartición	60 horas
Teleformación	Duración total de las tutorías presenciales: 8 horas

Requisitos de acceso del alumnado

Acreditaciones/ titulaciones	Cumplir como mínimo alguno de los siguientes requisitos: - Título de Grado o equivalente - Título de Postgrado (Máster) o equivalente - Título de Técnico Superior (FP Grado Superior) o equivalente de la familia profesional Informática y Comunicaciones - Certificado de profesionalidad de nivel 3 de la familia profesional Informática y Comunicaciones
Experiencia profesional	En caso de no disponer de certificación, acreditación o titulación se requerirá experiencia profesional mínima de 2 años en tareas relacionadas con la gestión de redes o sistemas informáticos.

Otros	Se recomienda, que el alumnado posea conocimientos básicos de: - Programación de aplicaciones informáticas - Técnicas de comprobación de funcionalidad de procesos y funciones informáticas - Procesos de autenticación y autorización de acceso para usuarios y servicios. - Redacción de resúmenes de datos. Cuando el alumnado no disponga de la acreditación o titulación requerida demostrará los conocimientos y competencias suficientes mediante una prueba competencial práctica de nivel consistente en escribir un pequeño programa informático y planificar los pasos a seguir para validar su correcto funcionamiento; conocer las técnicas de autenticación de usuarios y entre servidores, y los mecanismos de acreditación y otorgación de derechos de acceso; Redacción de un pequeño informe de resultados, resumiendo unos datos.
Modalidad de teleformación	Además de lo indicado anteriormente, el alumnado debe 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

Para acreditar los conocimientos adquiridos bastará con aportar el justificante de haber finalizado los estudios, o el resguardo de haberlo solicitado, o el expediente académico de los estudios realizados.

En caso de requerir la justificación de la experiencia laboral, el alumnado deberá aportar un certificado de la empresa, indicando las tareas a las que se ha dedicado y el porcentaje de la jornada laboral dedicado a las tareas relacionadas con la formación que nos ocupa.

Prescripciones de formadores y tutores

Acreditación requerida	Cumplir como mínimo alguno de los siguientes requisitos: - Licenciado, Ingeniero, máster en alguna especialidad TIC relacionada con esta formación, o el Título de Grado correspondiente u otros títulos equivalentes. - Diplomado, Ingeniero Técnico, o el Título de Grado correspondiente u otros títulos equivalentes. - Técnico Superior de la familia profesional de Informática y Comunicaciones.
Experiencia profesional mínima requerida	Se requerirán 2 años de experiencia en tareas relacionadas con los temas abordados en esta formación.
Competencia docente	Experiencia docente o investigadora acreditable en el ámbito de la ciberseguridad, de al menos 60 horas en modalidad presencial
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 m^2 para 15 participantes	Incremento Superficie/ participante (Máximo 30 participantes)
Aula de gestión	45 m^2	2,4 m^2/ participantes

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, cañón con proyección e Internet para el formador - PC's instalados en red e Internet para los alumnos. - Software específico para el aprendizaje de cada acción formativa: • Sistema operativo Windows y Linux (Kali) • Herramienta de análisis de código fuente • Herramientas de test de vulnerabilidades

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

En el caso de que aumente el número de alumnos, hasta un máximo de 30, la superficie de las aulas se incrementará proporcionalmente (según se indica en la tabla en lo relativo a m^2/ alumno) 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 del alumnado.

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

Si se utiliza el aula virtual han de cumplirse las siguientes indicaciones:

• **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.

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 alumnado 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.

Otras especificaciones

Tecnología y equipos	- La plataforma de teleformación incluirá una herramienta que permita la conexión síncrona de docentes y alumnos, con sistema incorporado de audio, video y posibilidad de compartir archivos, la propia pantalla u otras aplicaciones tanto por el docente como por el alumnado, con registro de los tiempos de conectividad.

Ocupaciones y puestos de trabajo relacionados

- 27191013 Auditores-asesores informáticos
- 2711 Analistas de sistemas
- 2723 Analistas de redes informáticas
- 27231014 Analistas y desarrolladores de redes informáticas
- 2722 Administradores de sistemas y redes
- 3811 Técnicos en operaciones de sistemas informáticos
- 3812 Técnicos en asistencia al usuario de tecnologías de la información
- 3813 Técnicos en redes
- 27111046 Ingenieros técnicos en informática de sistemas
- 27191022 Ingenieros técnicos en informática, en general
- 2729 Especialistas en bases de datos y en redes informáticas no clasificados bajo otros epígrafes

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: TEST DE INTRUSIÓN Y TIPOLOGÍA DE HERRAMIENTAS

OBJETIVO

Seleccionar las diferentes estrategias y funcionamiento de las herramientas disponibles en la ejecución de un test (prueba) de intrusión.

DURACIÓN EN CUALQUIER MODALIDAD DE IMPARTICIÓN: **8** horas

Teleformación: Duración de las tutorías presenciales: 0 horas

RESULTADOS DE APRENDIZAJE

Conocimientos/ Capacidades cognitivas y prácticas

- Distinción entre test de intrusión y auditoría
  - Objetivos
  - Elementos diferenciadores
- Clasificación de la tipología según la información que dispongamos
  - Caja blanca
  - Caja negra
  - Caja gris
- Clasificación de la tipología en función de los servicios a testear:
  - Pen test de red
  - Pen test de redes inalámbricas
  - Pen test de sistemas
  - Pen test de aplicaciones web
  - Pen test de ingeniería social

Habilidades de gestión, personales y sociales

- Rigor en la delimitación del entorno operativo en el que se encuentran las herramientas de ciberseguridad que se quieren forzar.
- Capacidad para la organización, y en caso necesario, disgregación, de los equipos de test del entorno informático.

MÓDULO DE FORMACIÓN 2: METODOLOGÍAS DE TEST DE INTRUSIÓN

OBJETIVO

Comparar las técnicas y recomendaciones prácticas, de organizaciones internacionales relevantes, para la realización de test de intrusión.

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 las fases de un test de intrusión
  - Planificación del test
  - Análisis del test
  - Informes con los resultados del test
- Definición de Conceptos
  - Alcance del test
  - Vector de ataque
- Clasificación OSSTMM (Open Source Security Testing Methodology Manual)
  - Seguridad física
  - Seguridad de los procesos
  - Seguridad en las tecnologías de Internet
  - Seguridad en las comunicaciones
  - Seguridad inalámbrica
  - Seguridad de la información
  - RAV (Risk assessment value)
- Clasificación OWASP (Open Web Applications Security Project)
  - Pruebas de gestión de la configuración y la implementación
  - Pruebas de gestión de identidad
  - Prueba de autenticación
  - Prueba de autorización
  - Prueba de gestión de sesiones
  - Prueba de validación de entrada
  - Prueba de manejo de errores
  - Prueba de criptografía débil
  - Pruebas de lógica empresarial
  - Pruebas del lado del cliente
  - Pruebas de API
- Diferenciación entre OSSTMM y OWASP

Habilidades de gestión, personales y sociales

- Asimilación de los objetivos de las diferentes pruebas a realizar para comprobar la efectividad de los patrones de ataque comunes.
- Constancia en la valoración de las características de los mecanismos de protección y las características de las pruebas a realizar para constatar la resiliencia de los sistemas a cada tipo de ataque.

MÓDULO DE FORMACIÓN 3: HERRAMIENTAS PARA LA EJECUCIÓN DE TEST DE INTRUSIÓN

OBJETIVO

Seleccionar las herramientas y procedimientos de explotación de vulnerabilidades en las aplicaciones y plataformas de programas, tanto para la preparación de test de intrusión (penetración), como para la detección de la eficiencia de los mecanismos de protección existentes.

DURACIÓN EN CUALQUIER MODALIDAD DE IMPARTICIÓN: 18 horas

Teleformación: Duración de las tutorías presenciales: 0 horas

RESULTADOS DE APRENDIZAJE

Conocimientos/ Capacidades cognitivas y prácticas

- Clasificación de herramientas genéricas
  - Burp Suite
  - OpenVas
  - Nessus
  - Metasploi
  - Kali Linux
- Clasificación de herramientas de red
  - Nmap
  - Aircrack-ng
  - Wireshark
  - Zmap
  - Ettercap
- Clasificación de herramientas de robo de contraseñas
  - Hydra
  - John de Ripper
  - Hashcat

Habilidades de gestión, personales y sociales

- Capacidad para la aplicación de las herramientas de detección y explotación de vulnerabilidades, certificando en su caso la resiliencia del sistema a métodos de ataque comunes.
- Respeto por el cumplimiento de las condiciones de servicio establecidas en los contratos de test de penetración acordados con las organizaciones solicitantes del servicio.

MÓDULO DE FORMACIÓN 4: RESULTADOS E INFORMES

OBJETIVO

Elaborar informes en función de los análisis realizados, especificando los resultados y recomendaciones obtenidos.

DURACIÓN EN CUALQUIER MODALIDAD DE IMPARTICIÓN: 6 horas

Teleformación: Duración de las tutorías presenciales: 0 horas

RESULTADOS DE APRENDIZAJE

Conocimientos/ Capacidades cognitivas y prácticas

- Descripción de herramientas de ayuda a la documentación
  - Dradis
  - Faraday
- Elaboración de informes
  - Evaluación y análisis de los resultados
  - Especificación de test realizados
  - Resultados técnicos

- Recomendaciones

- Definición de políticas de conservación de los registros:
  - Granularidad y perdurabilidad de los datos registrados en función de fuentes y relevancia
  - Requerimientos normativos y contractuales

Habilidades de gestión, personales y sociales

- Implicación en la preservación de la confidencialidad de los resultados de evaluación de vulnerabilidades encontradas.
- Rigor en la documentación de los procedimientos de test y análisis de vulnerabilidades realizados en informes detallados y resúmenes ejecutivos.
- Hábito de planificación de actividades de recogida y clasificación de datos recopilados durante los test de intrusión.

MÓDULO DE FORMACIÓN 5: PLANIFICACIÓN Y EJECUCIÓN DE UN TEST DE INTRUSIÓN

OBJETIVO

Aplicar técnicas y herramientas en la planificación y elaboración de un test de intrusión real.

DURACIÓN EN CUALQUIER MODALIDAD DE IMPARTICIÓN: 8 horas

Teleformación: Duración de las tutorías presenciales: 8 horas

RESULTADOS DE APRENDIZAJE

Conocimientos/ Capacidades cognitivas y prácticas

- Selección de la metodología más adecuada para realizar un test de intrusión.
  - Definir el alcance
  - Determinar vectores de ataque
  - Planificación para llevarla a cabo.
- Selección del tipo de test de intrusión para determinar la explotabilidad de las vulnerabilidades.
  - Determinar el test en función del alcance
  - Ejecución del test seleccionado
  - Obtención de resultados
- Elaboración del informe de test de intrusión.
  - Recopilación y ordenación de la información
  - Redacción del informe

Habilidades de gestión, personales y sociales

- Colaboración con otros miembros del equipo de trabajo en la ejecución y validación de tests.
- Rigor en la redacción de informes de resultados.

Resultados que obligatoriamente tienen que adquirirse en presencial

- Selección de la metodología más adecuada para realizar un test de intrusión.
  - Definir el alcance
  - Determinar vectores de ataque
  - Planificación para llevarla a cabo.
- Selección del tipo de test de intrusión para determinar la explotabilidad de las vulnerabilidades.
  - Determinar el test en función del alcance
  - Ejecución del test seleccionado
  - Obtención de resultados
- Elaboración del informe de test de intrusión.
  - Recopilación y ordenación de la información
  - Redacción del informe.

ORIENTACIONES METODOLÓGICAS

La impartición de la docencia se llevará a cabo complementando:

- Introducción de conceptos teóricos y metodológicos
- Estudio de casos en los que se hayan aplicado éstos
- Realización de ejercicios prácticos para demostrar las capacidades adquiridas.

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. En las evaluaciones programadas se pueden agrupar conocimientos de diversos módulos.
- Se realizará 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 alumnos.
- La puntuación final alcanzada se expresará en términos de Apto/ No Apto.