Catálogo de Especialidades Formativas

PROGRAMA FORMATIVO

CIBERSEGURIDAD Y HACKING ÉTICO

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:	CIBERSEGURIDAD Y HACKING ÉTICO
Familia Profesional:	INFORMÁTICA Y COMUNICACIONES
Área Profesional:	SISTEMAS Y TELEMÁTICA
Código:	IFCT0203
Nivel de cualificación profesional:	3

Objetivo general

Adquirir conocimientos y habilidades prácticas en hacking ético para identificar, analizar y mitigar vulnerabilidades en sistemas informáticos y redes, mediante el uso de técnicas avanzadas de ciberseguridad y herramientas especializadas.

Relación de módulos de formación

Módulo 1	Arquitectura de Redes	20 horas
Módulo 2	Infraestructuras Linux y Windows	55 horas
Módulo 3	Métodos de investigación, recolección de datos y escaneo	50 horas
Módulo 4	Routers, puertas de enlace y seguridad WiFi	40 horas
Módulo 5	Análisis de vulnerabilidades y ciberataques	60 horas
Módulo 6	Password Cracking	20 horas
Módulo 7	Exploits y Malware	55 horas

Modalidades de impartición

Presencial
Teleformación

Duración de la formación

Duración total en cualquier modalidad de impartición	300 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: -Título de Bachiller o equivalente -Título de Técnico Superior (FP Grado superior) o equivalente -Haber superado la prueba de acceso a Ciclos Formativos de Grado Superior -Certificado de profesionalidad de nivel 3
Experiencia profesional	No se requiere
Otros	Cuando no se pueda acreditar la titulación requerida, se deberán demostrar conocimientos: -Básicos de ofimática y sistema

Otros	operativo.
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 conocmiento de ingeniería informática y de sistemas, ingeniería eléctrica, ingeniería electrónica, ingeniería de la telecomunicación, ingeniería industrial, matemáticas o estadística.
Experiencia profesional mínima requerida	La experiencia se acreditará en el ámbito de la especialidad (programación) y será de al menos 12 meses.
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 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 informática	45.0 m²	2.4 m² / participante

Espacio formativo	Equipamiento
Aula de informática	-Mesa y silla para el/la formador/a-Mesas y sillas para el alumnado-Material de aula-Pizarra-PC instalado en red con posibilidad de impresión de documentos, cañón con proyector e internet para el personal formador-PCs instalados en red e internet con posibilidad de impresión para el alumnadoTodos los ordenadores han de tener las siguientes características mínimas:- Procesador i5- Memoria RAM 8 GB - Disco duro 500 GB - Tarjeta de red 10/100/1000 Mbps - Tarjeta gráfica- Tarjeta de sonido - Periféricos: Teclado, Ratón y Monitor colorSoftware específico para el aprendizaje de cada acción formativa:-Sistema operativo (versión/es con soporte oficial)-Navegador

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).

MÓDULO DE FORMACIÓN 1: Arquitectura de Redes

OBJETIVO

Comprender los fundamentos de la arquitectura de redes para analizar la estructura y funcionamiento de las redes de comunicación, enfocándose en su seguridad y posibles vulnerabilidades, así como en la eficiencia energética.

DURACIÓN EN CUALQUIER MODALIDAD DE IMPARTICIÓN: 20 horas

Teleformación: Duración de las tutorías presenciales: 0 horas

RESULTADOS DE APRENDIZAJE

Conocimientos / Capacidades cognitivas y prácticas

- Conocimiento de los fundamentos de arquitectura de redes
- Identificación de topologías de red y modelos de referencia (OSI y TCP/IP)
- Manejo de dispositivos de red (routers, switches, firewalls)
- Control de la seguridad en la arquitectura de redes
- Implementación de medidas de sostenibilidad.
    - Optimización del consumo energético mediante la gestión eficiente de recursos.
    - Implementación de políticas de apagado y encendido automático de servidores.
    - Utilización de tecnologías de virtualización para consolidar servidores.
    - 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

- Capacidad de análisis crítico para evaluar la arquitectura de red para identificar posibles vulnerabilidades y mejorar su seguridad en un entorno empresarial.
- Toma de decisiones informadas en la elección de las topologías y dispositivos de red adecuados para garantizar la eficiencia y seguridad en las comunicaciones de la empresa.
- Atención a la sostenibilidad ambiental y a la eficiencia energética.

MÓDULO DE FORMACIÓN 2: Infraestructuras Linux y Windows

OBJETIVO

Adquirir habilidades en la administración de sistemas Linux y Windows para gestionar servidores y redes, identificando y mitigando posibles vulnerabilidades de seguridad.

DURACIÓN EN CUALQUIER MODALIDAD DE IMPARTICIÓN: 55 horas

Teleformación: Duración de las tutorías presenciales: 0 horas

RESULTADOS DE APRENDIZAJE

Conocimientos / Capacidades cognitivas y prácticas

- Instalación, configuración y uso de infraestructuras Linux - Instalación y configuración de sistemas Linux - Comandos básicos y administración de sistemas Linux - Seguridad en servidores Linux - Herramientas de análisis y monitoreo en Linux
- Instalación, configuración y uso de infraestructuras Windows - Instalación y configuración de sistemas Windows - Administración de sistemas Windows - Seguridad en servidores Windows - Uso de PowerShell para administración y automatización.

Habilidades de gestión, personales y sociales

- Capacidad de gestión de incidencias para resolver problemas relacionados con servidores Linux, asegurando la continuidad del servicio en la infraestructura empresarial.
- Trabajo bajo presión para mitigar vulnerabilidades de seguridad en servidores Linux ante posibles ataques, manteniendo la calma y priorizando las acciones necesarias.
- Capacidad de resolución de problemas para detectar y corregir vulnerabilidades en sistemas Windows, asegurando la estabilidad de la infraestructura tecnológica de la organización.
- Automatización y eficiencia en el uso de PowerShell para automatizar tareas rutinarias, optimizando el tiempo y los recursos de la empresa.

MÓDULO DE FORMACIÓN 3: **Métodos de investigación, recolección de datos y escaneo**

OBJETIVO

Aplicar métodos de investigación y técnicas de escaneo para identificar información relevante y vulnerabilidades en redes y sistemas, utilizando herramientas avanzadas de OSINT y escaneo.

DURACIÓN EN CUALQUIER MODALIDAD DE IMPARTICIÓN: 50 horas

Teleformación: Duración de las tutorías presenciales: 0 horas

RESULTADOS DE APRENDIZAJE

Conocimientos / Capacidades cognitivas y prácticas

- Conocimiento de métodos de investigación y recolección de Datos - Técnicas de reconocimiento y recolección de información - Uso de herramientas Open Source Intelligence (OSINT) - Análisis de información recolectada - Documentación de la investigación
- Utilización de técnicas y tecnologías de Escaneo - Herramientas de escaneo de redes (Nmap y Nessus) - Metodologías de escaneo y mapeo de redes - Análisis de resultados de escaneo - Identificación de servicios y sistemas operativos.

Habilidades de gestión, personales y sociales

- Atención al detalle para recoger y analizar datos relevantes sobre posibles amenazas, garantizando una investigación precisa y útil para la seguridad informática.
- Comunicación clara en la documentación de los hallazgos de la investigación de manera comprensible para que todos los miembros del equipo los comprendan • Trabajo colaborativo: Colaborar con otros equipos para compartir los resultados de escaneos y vulnerabilidades, contribuyendo a una respuesta conjunta ante posibles amenazas.
- Análisis proactivo para anticipar y detectar vulnerabilidades en sistemas antes de que se conviertan en una amenaza real para la empresa.

MÓDULO DE FORMACIÓN 4: Routers, puertas de enlace y seguridad WiFi

OBJETIVO

Configurar y asegurar routers, puertas de enlace y redes WiFi para proteger dispositivos y redes frente a accesos no autorizados y ataques.

DURACIÓN EN CUALQUIER MODALIDAD DE IMPARTICIÓN: 40 horas

Teleformación: Duración de las tutorías presenciales: 0 horas

RESULTADOS DE APRENDIZAJE

Conocimientos / Capacidades cognitivas y prácticas

- Configuración de Routers y Firewalls - Seguridad en dispositivos de red - Técnicas de ataque a routers - Mitigación de riesgos en configuraciones de red
- Control de técnicas de auditoría de redes inalámbricas - Seguridad en redes WiFi (WEP, WPA y WPA2) - Herramientas de análisis de seguridad en WiFi - Pruebas de penetración en redes inalámbricas.

Habilidades de gestión, personales y sociales

- Capacidad de gestión de la seguridad en la implementación de medidas de seguridad en routers y puertas de enlace para proteger la infraestructura de la organización frente a ciberataques.
- Prevención de riesgos para identificar y mitigar riesgos en la configuración de la red, garantizando una comunicación segura en la empresa.
- Mejora continua para la implementación de soluciones de seguridad en redes inalámbricas, basándose en los resultados de auditorías previas para reducir futuras vulnerabilidades.

MÓDULO DE FORMACIÓN 5: Análisis de vulnerabilidades y ciberataques

OBJETIVO

Realizar análisis de vulnerabilidades y comprender los diferentes tipos de ciberataques, desarrollando estrategias de mitigación y prevención.

DURACIÓN EN CUALQUIER MODALIDAD DE IMPARTICIÓN: 60 horas

Teleformación: Duración de las tutorías presenciales: 0 horas

RESULTADOS DE APRENDIZAJE

Conocimientos / Capacidades cognitivas y prácticas

- Análisis de Vulnerabilidades - Identificación y clasificación de vulnerabilidades - Herramientas de análisis de vulnerabilidades - Pruebas de penetración y su metodología - Generación de informes de vulnerabilidades
- Identificación de Ciberataques - Clasificación de ciberataques - Metodologías de ataque (phishing, DDoS, etc.) - Análisis de casos de ciberataques reales - Prevención y mitigación de ciberataques

Habilidades de gestión, personales y sociales

- Fomento de la capacidad analítica en el análisis exhaustivo de vulnerabilidades en redes y sistemas para priorizar las soluciones más críticas en el entorno laboral.
- Planificación estratégica en la elaboración de informes de vulnerabilidades que permitan a la organización tomar decisiones estratégicas para mejorar su ciberseguridad.
- Pensamiento preventivo: Desarrollar estrategias de prevención de ciberataques para proteger los datos y sistemas críticos de la organización.
- Capacidad de gestión de crisis, respondiendo de manera efectiva a un ciberataque, liderando la contención y mitigación de sus efectos en tiempo real.

MÓDULO DE FORMACIÓN 6: Password Cracking

OBJETIVO

Aprender y aplicar técnicas de cracking de contraseñas para evaluar la fortaleza de las credenciales de acceso, utilizando herramientas especializadas y medidas de protección.

DURACIÓN EN CUALQUIER MODALIDAD DE IMPARTICIÓN: 20 horas

Teleformación: Duración de las tutorías presenciales: 0 horas

RESULTADOS DE APRENDIZAJE

Conocimientos / Capacidades cognitivas y prácticas

- Aplicación de técnicas de cracking
    - Métodos y herramientas de cracking de contraseñas
    - Estrategias de defensa contra el cracking
- Cifrado y almacenamiento seguro de contraseñas
- Implementación de password cracking
- Evaluación de la fortaleza de las credenciales de acceso.

Habilidades de gestión, personales y sociales

- Capacidad de análisis para evaluar la robustez de las contraseñas corporativas y proponer soluciones para mejorar la seguridad de los accesos.
- Ética profesional, usando las técnicas de cracking de forma ética, asegurando que se utilicen exclusivamente para la mejora de la seguridad dentro de la organización.

MÓDULO DE FORMACIÓN 7: Exploits y Malware

OBJETIVO

Desarrollar y aplicar exploits, así como identificar, analizar y mitigar amenazas de malware en sistemas, reforzando la seguridad de los entornos de red.

DURACIÓN EN CUALQUIER MODALIDAD DE IMPARTICIÓN: 55 horas

Teleformación: Duración de las tutorías presenciales: 0 horas

RESULTADOS DE APRENDIZAJE

Conocimientos / Capacidades cognitivas y prácticas

- Implementación de Exploits - Concepto y tipos de exploits - Análisis de vulnerabilidades y desarrollo de exploits - Técnicas de explotación de sistemas - Mitigación de riesgos de exploits
- Seguridad frente a Malware - Tipos de malware (virus, troyanos, ransomware, etc.) - Métodos de propagación de malware - Análisis y desinfección de sistemas infectados - Prevención contra malware y buenas prácticas

Habilidades de gestión, personales y sociales

- Innovación tecnológica desarrollando exploits controlados para probar la seguridad de sistemas informáticos, evaluando nuevas maneras de reforzar la infraestructura tecnológica.
- Resolución de conflictos, proponiendo soluciones de mitigación ante exploits detectados, evitando que se conviertan en amenazas reales para los sistemas corporativos.
- Resiliencia para gestionar la detección y eliminación de malware en sistemas críticos, minimizando el impacto en las operaciones diarias de la organización.

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.