Catálogo de Especialidades Formativas

PROGRAMA FORMATIVO

DEFENSA EN CIBERSEGURIDAD

Marzo 2023

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:	DEFENSA EN CIBERSEGURIDAD
Familia Profesional:	INFORMÁTICA Y COMUNICACIONES
Área Profesional:	SISTEMAS Y TELEMÁTICA
Código:	IFCT0047
Nivel de cualificación profesional:	3

Objetivo general

Proporcionar los conocimientos y capacidades necesarios en el campo de la defensa en ciberseguridad para detectar ciberamenazas, y ser capaz de administrar las mismas (evaluar riesgos asociados a los incidentes de seguridad, saber aplicar medidas de contención, erradicar y dar respuesta).

Relación de módulos de formación

Módulo 1	CONCEPTOS PREVIOS DE CIBERSEGURIDAD	4 horas
Módulo 2	SOFT SKILLS	32 horas
Módulo 3	SISTEMAS Y REDES OPERATIVAS	80 horas
Módulo 4	COMPUTER NETWORK DEFENSE	100 horas
Módulo 5	SOFTWARE DE MONITORIZACIÓN DE CENTROS SOC	24 horas
Módulo 6	CAMPOS DE LA CIBERSEGURIDAD DISTINTOS DE LA DEFENSA.	8 horas
Módulo 7	SISTEMAS UNIX.	40 horas

Modalidad de impartición

Presencial

Duración de la formación

Duración total	288 horas

Requisitos de acceso del alumnado

Acreditaciones / titulaciones	Cumplir como mínimo alguno de los siguientes requisitos: Haber superado cualquier prueba oficial de acceso a la universidad
Experiencia profesional	No se requiere
Otros	En relación con la titulación cursadas por los alumnos es necesario que se corresponda con la familia profesional de Informática y comunicaciones.

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, en cualquier materia relacionada directamente con las Tecnologías de la Información. Diplomado, Ingeniero Técnico, Arquitecto Técnico o el Título de Grado correspondiente u otros títulos equivalentes, en cualquier materia relacionada directamente con las Tecnologías de la Información.
Experiencia profesional mínima requerida	Se requiere al menos dos años de experiencia laboral en el sector de la ciberseguridad, o en su defecto experiencia demostrable de al menos 4 años relacionada con la materia a impartir.
Competencia docente	Acreditar una experiencia docente en entidades públicas o privados, que sea superior a 50 horas, en cualquier materia relacionada con Tecnologías de la Información.

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.

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.

Ocupaciones y puestos de trabajo relacionados

27111019 ANALISTAS DE SISTEMAS, NIVEL MEDIO (JUNIOR)

27231014 ANALISTAS Y DESARROLLADORES DE REDES INFORMÁTICAS

27291012 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: CONCEPTOS PREVIOS DE CIBERSEGURIDAD

OBJETIVO

Conocer y comprender el funcionamiento de un Centro de Operaciones de Seguridad.

DURACIÓN TOTAL:

4 horas

RESULTADOS DE APRENDIZAJE

Conocimientos / Capacidades cognitivas y prácticas

- Identificación de los distintos ámbitos en los que se divide la ciberseguridad.
- Asociación de los distintos ámbitos de la ciberseguridad a las diferentes necesidades de potenciales clientes.
- Interpretación de las necesidades de los distintos ámbitos a incidentes reales nacionales e internacionales.
- Enumeración de los principales softwares especializados necesarios para una gestión adecuada de la ciberseguridad.

Habilidades de gestión, personales y sociales

- Sensibilización de la comprensión de fenómenos abstractos sobre ciberseguridad y capacidad para extrapolarlos a incidentes futuros.
- Capacidad para transmitir la información a un equipo multidiciplinar

MÓDULO DE FORMACIÓN 2: SOFT SKILLS

OBJETIVO

Adquirir la capacidad de hablar en público y redactar informes de manera adecuada en el sector de la ciberseguridad.

DURACIÓN TOTAL: 32 horas

RESULTADOS DE APRENDIZAJE

Conocimientos / Capacidades cognitivas y prácticas

- Habilidades de comunicación oral:
  - Superación del miedo escénico frente a auditorios o reuniones.
- Síntesis expositiva.
  - Transmisión de la idea fundamental y las accesorias.
- Redacción de informes:
  - Síntesis expositiva escrita.
- Fundamentación de las recomendaciones recogidas en el informe.

Habilidades de gestión, personales y sociales

- Gestión emocional frente a público.
- Aplicación de la capacidad de síntesis expositiva.

MÓDULO DE FORMACIÓN 3: SISTEMAS Y REDES OPERATIVAS

OBJETIVO

Identificar los principales elementos que componen las redes y los sistemas operativos como base para gestionar posteriormente la seguridad de los mismos en un directorio activo.

DURACIÓN TOTAL: 80 horas

RESULTADOS DE APRENDIZAJE

Conocimientos / Capacidades cognitivas y prácticas

- Sistemas operativos:
  - Definición de los conceptos sobre sistemas operativos y redes relacionados con la ciberseguridad.
  - Gestión sistemas operativos de manera orientada a su securización.
  - Conocimiento de la estructura de los diferentes sistemas operativos.
  - Identificación de los procesos e hilos presentes en los sistemas operativos.
  - Gestión de la memoria teniendo presente la seguridad de la misma.
  - Gestión de los archivos presentes en un sistema operativo de manera segura.
  - Aseguramiento de las entradas y salidas de información.
- Redes:

- Comprensión del concepto, funcionamiento y estructura de una red.
- Aplicación del conocimiento adquirido de los sistemas operativos en una red concreta.
- Implementación de las medidas de seguridad en una red dada.

• Directorio activo:
- Definición del concepto de directorio activo.
- Mantenimiento de la securización de lo sistemas y las redes durante el empleo de información organizada dentro de un directorio activo.
- Conocimiento de los distintos elementos de un directorio activo.
- Implementación de las medidas de seguridad necesarias en un directorio activo de manera que permitan las medidas de seguridad de los sistemas y redes.

Habilidades de gestión, personales y sociales

- Comprensión de la naturaleza y funcionamiento de las redes y sistemas desde la perspectiva de la ciberseguridad.
- Capacidad para transmitir los requerimientos necesarios para securizar sistemas y redes.

MÓDULO DE FORMACIÓN 4: COMPUTER NETWORK DEFENSE

OBJETIVO

Adquirir las habilidades necesarias sobre detección de amenazas y análisis de dispositivos tras un ciberincidente como capacidades defensivas.

DURACIÓN TOTAL:

100 horas

RESULTADOS DE APRENDIZAJE

Conocimientos / Capacidades cognitivas y prácticas

• Análisis de amenazas:
- Comprensión de la actividad y roles que componen un Centro de Operaciones de Seguridad.
- Diferenciación de las principales situaciones gestionadas en un Centro de Operaciones de Seguridad
- Selección de las herramientas y metodologías de análisis adecuadas para la respuesta ante un incidente.

• Análisis de dispositivos:
- Evaluación del funcionamiento de los sistemas y redes objeto de securización para una correcta elección de procedimientos a implementar para su defensa.
- Ajuste de la actividad seleccionada a los límites de una adecuada normativa.
- Gestión de un incidente de distintos niveles de criticidad.
- Comprensión de un análisis forense.
- Identificación de las principales metodologías de análisis de malware y reversing.
- Familiarización con los distintos tipos de malware.
- Comprensión y manipulación de IDS, HIDS y dispositivos en red.

- Comprensión y manipulación de software propietario específico de ciberseguridad

Habilidades de gestión, personales y sociales

- Capacidad de discriminación de las técnicas adecuadas a cada tipología concreta de incidente.
- Comunicación fluida y eficaz con otros miembros del Centro de operaciones de Seguridad.

MÓDULO DE FORMACIÓN 5: SOFTWARE DE MONITORIZACIÓN DE CENTROS SOC

OBJETIVO

Familiarizarse con los softwares específicos de seguridad para aplicar el aprendizaje previo en los ámbitos defensivo y ofensivo.

DURACIÓN TOTAL:

24 horas

RESULTADOS DE APRENDIZAJE

Conocimientos / Capacidades cognitivas y prácticas

- Software propietario defensivo:
  - Familiarización con la naturaleza de software propietario avanzado de gestión de incidentes de ciberseguridad.
  - Empleo de las funcionalidades del software propietario a los conceptos aprendidos en materia de defensa.
  - Análisis de la información obtenido sobre un ciberincidente dado mediante el empleo de las funciones específicas del software propietario.
- Software propietario y su relación con el ataque:
  - Empleo de las funcionalidades del software propietario en materia de defensa para la elaboración de planes de ataque ético.
  - Análisis de la información obtenido sobre un ciberincidente dado mediante el empleo de las funciones específicas del software propietario como base para la elaboración de un ciberataque ético.

Habilidades de gestión, personales y sociales

- Ética en el empleo y confidencialidad del software propietario.
- Capacidad de aprendizaje continúo relacionada con el desarrollo de software específico.

MÓDULO DE FORMACIÓN 6:	CAMPOS DE LA CIBERSEGURIDAD DISTINTOS DE LA DEFENSA.

OBJETIVO

Obtener una perspectiva general del sector de la ciberseguridad introduciendo al alumnado en los campos de la programación, la geopolítica, el análisis forense de móviles, a la seguridad ofensiva y el Gobierno, Riesgo y Cumplimiento.

DURACIÓN TOTAL: 8 horas

RESULTADOS DE APRENDIZAJE

Conocimientos / Capacidades cognitivas y prácticas

- Programación:
  - Comprensión y ejecución de expresiones regulares en programación para su empleo en el ámbito de la ciberseguridad.
- Geopolítica:
  - Conocimiento de la disciplina geopolítica y de su relación y aplicación en el sector de la ciberseguridad.
- Forense de móviles:
  - Descripción y conocimiento de un análisis de un dispositivo móvil como medio de obtención de información sobre ciberseguridad.
- Gobierno, Riesgo y Cumplimiento:
  - Acercamiento a los Marcos normativos, gobernanza y análisis de riesgos en ciberseguridad.
- Seguridad ofensiva:
  - Introducción a las auditorías ofensivas ética en ciberseguridad.

Habilidades de gestión, personales y sociales

- Extrapolación de conceptos a ámbitos dispares pero relacionados en ciberseguridad.
- Creatividad analítica.

MÓDULO DE FORMACIÓN 7: SISTEMAS UNIX.

OBJETIVO

Ejecutar comandos y órdenes específicas en sistemas UNIX relacionadas con el posterior desempeño en ciberseguridad.

DURACIÓN TOTAL: 40 horas

RESULTADOS DE APRENDIZAJE

Conocimientos / Capacidades cognitivas y prácticas

- Comandos y órdenes:
  - Definición de los conceptos básicos empleados en sistemas UNIX
  - Gestión de sistemas UNIX de manera orientada a su securización.
  - Conocimiento de la estructura de los sistemas UNIX.
- Identificación de los procesos presentes en UNIX.
  - Gestión de la memoria desde un sistema UNIX teniendo presente la seguridad de la misma.
  - Gestión de los archivos en UNIX de manera segura.
  - Aseguramiento de las entradas y salidas de información.
  - Composición de instrucciones en el lenguaje propio de sistemas UNIX.
  - Normalización de fuentes
  - Correlación de eventos,

Habilidades de gestión, personales y sociales

- Puesta en práctica de la capacidad de resolución de problemas
- Adquisición de actitudes positivas hacia el razonamiento lógico-matemático

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.