Catálogo de Especialidades Formativas

PROGRAMA FORMATIVO

Respuesta a incidentes de ciberseguridad

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:	RESPUESTA A INCIDENTES DE CIBERSEGURIDAD
Familia Profesional:	INFORMÁTICA Y COMUNICACIONES
Área Profesional:	SISTEMAS Y TELEMÁTICA
Código:	IFCT124
Nivel de cualificación profesional:	4

Objetivo general

Identificar las características de los ataques informáticos, programar herramientas de detección, y reaccionar para detener el ataque (contener) y recuperar el funcionamiento de los procesos de negocio.

Relación de módulos de formación

Módulo 1	Gestión de respuesta a incidentes	10 horas
Módulo 2	Recogida de datos y gestión de alarmas	40 horas
Módulo 3	Recomendaciones de buenas prácticas y marco regulador	24 horas
Módulo 4	Desarrollo de una respuesta a un incidente de ciberseguridad	12 horas

Modalidades de impartición

Presencial

Teleformación

Duración de la formación

Duración total en cualquier modalidad de impartición		86 horas
	Teleformación	Duración total de las tutorías presenciales: 12 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 acreditación/titulación se requerirá una 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: - Búsqueda avanzada de información en Internet i redes sociales - Programación de herramientas de Filtrado y homogeneización del formato de datos - Generación de ficheros de comandos de sistema operativo para automatizar y programar procesos 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 el manejo de herramientas de búsqueda en navegadores y webs de servicios de OSINT; programación de herramienta de extracción de datos de un fichero log y ejercicios de comandos para el lanzamiento de ejecución de aplicaciones a nivel práctico (básico).
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.

Justificación de las Prescripciones de formadoras y tutoras

Los formadores deberán acreditar su titulación y aportar alguna justificación de docencia impartida en la modalidad elegida.

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 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. - Software específico para el aprendizaje de cada acción formativa: • Sistema operativo Windows • Plataforma para la ejecución de sistemas y aplicaciones virtualizadas • Herramienta de SIEM

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 secuenciados pedagógicamente de tal manera que permiten su comprensión y retención.

- No ser meramente informativos, promoviendo su aplicación práctica a través de actividades de aprendizaje auto-evaluables 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)

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: GESTIÓN DE RESPUESTA A INCIDENTES

OBJETIVO

Identificar las diferentes estrategias, modelos de actuación y formas de implantación en la respuesta a incidentes, en función de las características del ataque, coordinando las actuaciones del equipo de respuesta asignado.

DURACIÓN EN CUALQUIER MODALIDAD DE IMPARTICIÓN: 10 horas

Teleformación: Duración de las tutorías presenciales: 0 horas

RESULTADOS DE APRENDIZAJE

Conocimientos/ Capacidades cognitivas y prácticas

- Descripción de un equipo de respuesta a incidentes
  - Estructura organizativa
  - Distribución de funciones y operación
- Organización de un equipo de respuesta a incidentes
  - Creación de procedimientos, políticas y planes para respuesta a incidentes
- Identificación de servicios
  - Servicios Reactivos
  - Servicios proactivos
  - Gestión de la ciberseguridad
- Relación de las fases en la respuesta a incidentes
  - Detección del incidente
  - Análisis de datos e identificación del incidente
  - Contención y erradicación del incidente
  - Recuperación del incidente
  - Notificación del incidente por regulación
- Localización y contacto de los equipos de coordinación y respuesta a Incidentes de ciberseguridad: CSIRTs
  - Agencia de Ciberseguridad de Cataluña: modelos de interrelación y servicio
  - Foros internacionales: FIRST, TERENA, Trusted Introducer
  - Agentes nacionales: INCIBE, CCN-CERT, CNPIC
  - Asociación nacional de equipos de respuesta a incidentes: CSIRT.ES

Habilidades de gestión, personales y sociales

- Asimilación de las funciones y objetivos de los organismos nacionales e internacionales de coordinación y soporte a los equipos de respuesta a incidentes.
- Intercambio de ideas mediante las herramientas de colaboración ofrecidas por cada uno de ellos y alcance de la colaboración esperada de éstos, tanto para miembros de sus organizaciones, como para equipos de respuesta no vinculados.
- Valoración de las fuentes de información sobre los ataques conocidos y las recomendaciones de detección y mitigación de éstos.
- Rigor en la selección, recomendación y automatización de las reacciones de respuesta a cada tipo de incidente detectado

- Implicación en la supervisión, evaluación, documentación y comunicación de la respuesta de los técnicos encargados de llevar a cabo las acciones reactivas recomendadas
- Prescripción del uso de las herramientas colaborativas para optimizar los recursos empleados en la respuesta a incidentes
- Evaluación del riesgo y la política de protección de datos y sistemas corporativos a las estrategias de respuesta a incidentes recomendadas por organismos nacionales e internacionales

MÓDULO DE FORMACIÓN 2: RECOGIDA DE DATOS Y GESTIÓN DE ALARMAS

OBJETIVO

Categorizar las fuentes de información de los datos implicados en incidentes de ciberseguridad.

DURACIÓN EN CUALQUIER MODALIDAD DE IMPARTICIÓN: 40 horas

Teleformación: Duración de las tutorías presenciales: 0 horas

RESULTADOS DE APRENDIZAJE

Conocimientos/ Capacidades cognitivas y prácticas

- Recopilación de datos significativos
  - Identificación de las fuentes de datos internas de un centro de operaciones de seguridad, mediante herramientas de monitorización de red y sistemas informáticos.
  - Identificación de fuentes de datos externas: Análisis de inteligencia del ataque (investigación, Threat Intelligence) e Inteligencia en fuentes abiertas (OSINT)
  - Recogida de evidencias digitales: búsquedas ciegas, preservación de la confidencialidad de los datos, preservación de la cadena de custodia y gestión de copias de seguridad.
- Análisis de datos de intrusiones
  - Evaluación del impacto potencial de la intrusión y determinación del nivel de alerta correspondiente
  - Detección de intrusiones (IDS)
  - Protección contra intrusiones (IPS)
  - Gestión de datos
  - Análisis forense: Conocer las buenas prácticas de recogida de evidencias digitales, para mantener su validez en caso de realizarse una denuncia por los daños sufridos.
- Correlación de datos y generación de alarmas
  - Gestión de logs de los diferentes sistemas y servicios
  - Sistemas de gestión de eventos de seguridad (SIEM)
  - Homogeneización de los datos. Filtrado y normalización de las fuentes.
  - Tratamiento de las alarmas: automatización de respuestas y Comunicación del escenario del incidente
  - Otras herramientas: Orquestación y automatización (SOAR), Visualización de datos y Generación automática de informes

Habilidades de gestión, personales y sociales

- Colaboración con los miembros de los equipos de recogida y análisis de datos, así como con expertos externos
- Designación de roles y responsabilidades a los miembros de los equipos de trabajo, asignación de tareas y distribución de turnos.
- Valoración de la utilidad de los datos recopilados y del impacto de los ataques en los procesos de negocio y los activos de la organización.
- Compromiso con la identificación y evaluación de fuentes de datos, tanto externas como internas, abiertas u ocultas en programas, memoria u otros sistemas de almacenamiento externo o en la nube.
- Rigor en la discriminación de datos verídicos de falsos
- Responsabilidad en la protección de los activos digitalizados y datos sensibles de la corporación.

MÓDULO DE FORMACIÓN 3: RECOMENDACIONES DE BUENAS PRÁCTICAS Y MARCO REGULADOR

OBJETIVO

Aplicar la normativa, herramientas y estándares correspondientes, en la detección y respuesta a incidentes de ciberseguridad.

DURACIÓN EN CUALQUIER MODALIDAD DE IMPARTICIÓN: 24 horas

Teleformación: Duración de las tutorías presenciales: 0 horas

RESULTADOS DE APRENDIZAJE

Conocimientos/ Capacidades cognitivas y prácticas

- Interpretación, selección y aplicación de las herramientas y los estándares internacionales y nacionales de detección y respuesta a incidentes de ciberseguridad
  - MITRE ATT&CK
  - SIGMA (Security Management Services)
  - SIEM (OSSIM)
  - IDS (SNORT)
  - RTIR
  - OTRS
  - LUCIA
- Clasificación de normativas de protección de datos personales
  - RGPD de la UE (Reglamento General de Protección de Datos Europeo)
  - LOPD-GDD (Ley orgánica de protección de datos y garantía de derechos digitales española)
- Adecuación al Esquema Nacional de Seguridad
  - Metodología de análisis y gestión de riesgos (MAGERIT)
  - Herramientas de análisis, evaluación y gestión de riesgos (PILAR)
- Aplicación de la Directiva NIS
  - Proveedores de servicios esenciales
  - Impacto en las empresas suministradoras

- Definición de los principios de la ética profesional:
  - En la respuesta a incidentes
  - En la captura y custodia de evidencias

Habilidades de gestión, personales y sociales

- Responsabilidad en la protección de los activos digitalizados y datos sensibles de la corporación.
- Sensibilización por los requisitos legales aplicables a los procesos de negocio de la corporación.

MÓDULO DE FORMACIÓN 4: DESARROLLO DE UNA RESPUESTA A UN INCIDENTE DE CIBERSEGURIDAD

OBJETIVO

Aplicar herramientas y técnicas de análisis y gestión de la respuesta a un incidente de ciberseguridad.

DURACIÓN EN CUALQUIER MODALIDAD DE IMPARTICIÓN: 12 horas

Teleformación: Duración de las tutorías presenciales: 12 horas

RESULTADOS DE APRENDIZAJE

Conocimientos/ Capacidades cognitivas y prácticas

- Extracción de información:
  - De una fuente de datos de tráfico en una red corporativa
  - De fuentes OSINT
- Automatización de los procesos de detección de intrusiones:
  - Integración de fuentes de datos en una herramienta SIEM.
  - Selección de los parámetros para la detección y generación de alarmas relevantes.
- Gestión de la respuesta a un incidente de seguridad informática.
  - Identificación de fuentes de cooperación para optimización de la respuesta a un incidente de ciberseguridad
  - Planificación de actuaciones y procedimientos
  - Resolución de un ciber-incidente

Habilidades de gestión, personales y sociales

- Colaboración con otros miembros del equipo de trabajo.
- Eficiencia en la utilización de herramientas habituales en los centros de operaciones de seguridad y equipos de respuesta a incidentes
- Rigor en la redacción de informes de resultados
- Constancia en la programación de actividades de recogida y clasificación de datos.

Resultados que obligatoriamente tienen que adquirirse en presencial

- Extracción de información:
  - De una fuente de datos de tráfico en una red corporativa
  - De fuentes OSINT
- Automatización de los procesos de detección de intrusiones:
  - Integración de fuentes de datos en una herramienta SIEM.
  - Selección de los parámetros para la detección y generación de alarmas relevantes.
- Gestión de la respuesta a un incidente de seguridad informática.
  - Identificación de fuentes de cooperación para optimización de la respuesta a un incidente de ciberseguridad
  - Planificación de actuaciones y procedimientos
  - Resolución de un ciber-incidente

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.