Catálogo de Especialidades Formativas

PROGRAMA FORMATIVO

Implantación y gestión de la 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:	IMPLANTACIÓN Y GESTIÓN DE LA CIBERSEGURIDAD
Familia Profesional:	INFORMÁTICA Y COMUNICACIONES
Área Profesional:	SISTEMAS Y TELEMÁTICA
código:	IFCT123
Nivel de cualificación profesional:	4

Objetivo general

Gestionar las herramientas y procedimientos de protección de los sistemas de información contra ciber-ataques o accesos no autorizados.

Relación de módulos de formación

Módulo 1	Protección y detección de ataques.	25 horas
Módulo 2	Herramientas básicas de prevención	18 horas
Módulo 3	Control de acceso de usuarios y aplicaciones	18 horas
Módulo 4	Herramientas de gestión de procesos de recuperación	20 horas
Módulo 5	Planes de instalación y operación de sistemas de gestión de la ciberseguridad	10 horas

Modalidades de impartición

Presencial

Teleformación

Duración de la formación

Duración total en cualquier modalidad de impartición		91 horas
	Teleformación	Duración total de las tutorías presenciales: 10 horas

Requisitos de acceso del alumnado

Acreditaciones / titulaciones	Cumplir como mínimo alguno de los requisitos siguientes: - Título de Grado o equivalente - Título de Postgrado (Master) 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: - Estructura de paquetes de los Protocolos de comunicación en redes de ordenadores 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 identificar los diferentes campos de algunos paquetes de datos en protocolos de comunicación en redes de ordenadores.
Modalidad de teleformación	Además de lo indicado anteriormente, el alumnado debe 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 será suficiente 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 requisitos siguientes: - 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 mínima de 30 horas, o experiencia mínima de 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

Los formadores deben 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/ 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 - PC's 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 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 con respecto a m^2/ Alumno) y el equipamiento estará de acuerdo con este aumento.

No debe interpretarse que los diversos espacios formativos identificados deban diferenciarse necesariamente mediante cerramientos.

Las instalaciones y equipamientos deberán cumplir la normativa industrial e higiénico sanitaria correspondiente y responderán a medidas de accesibilidad y seguridad del alumnado.

En 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 debe 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 de 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 alojamiento mínimo igual al total del alumnado de estas acciones, considerando que el número máximo de alumnos por tutor es de 80 y un número de usuarios concurrentes del 40% de este alumnado.

  b) Disponer de la capacidad de transferencia necesaria para que no se produzca efecto retraso 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 en el 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 al menos 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 debe cumplir con los requisitos que establece 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 esta plataforma debe identificar la localización física del servidor y el cumplimiento 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 sea aplicable al Reglamento (UE) 2016/679 del Parlamento Europeo y de 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 visores compatibles. Si se requiere la instalación adicional de algún apoyo para funcionalidades avanzadas, la plataforma debe facilitar el acceso a la misma sin coste.

- Disponibilidad del servicio web de seguimiento (operativo y en funcionamiento) de las acciones formativas impartidas, de acuerdo con el 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 dé 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, deben estar disponibles para el alumnado desde el inicio hasta la finalización de la acción formativa, manteniendo un horario de funcionamiento de la 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 para este 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 debe 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 estas herramientas debe 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 posibilitan el almacenamiento y la gestión de archivos (visualizar archivos, organizados en carpetas -directorios- y subcarpetas, copiar, pegar, eliminar, comprimir, descargar o cargar archivos), la publicación organizada y selectiva de los contenidos de estos 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, 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 el contenido cumpla estos requisitos:

- Como mínimo, ser el establecido en el mencionado 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, por lo 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 (autoavaluables 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, vídeo, 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 glosarios que identifiquen y definan los términos o vocablos básicos, relevantes o claves para la comprensión de los aprendizajes.
- Evaluar su adquisición durante ya la finalización de la acción formativa a través de actividades de evaluación (ejercicios, preguntas, trabajos, problemas, casos, pruebas, etc.), que permiten medir el rendimiento o el ejercicio 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

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: PROTECCIÓN Y DETECCIÓN DE ATAQUES

OBJETIVO

Aplicar medidas de protección a los equipos informáticos conectados a una red corporativa.

DURACIÓN EN CUALQUIER MODALIDAD DE IMPARTICIÓN: 25 horas

Teleformación: Duración de las tutorías presenciales: 0 horas

RESULTADOS DE APRENDIZAJE

Conocimientos / Capacidades cognitivas y prácticas

- Gestión de incidentes de ciberseguridad: Centro de Operaciones de Seguridad - SOC
  - El peligro
  - Defensores en la guerra contra el delito cibernético
- Inspección detallada de los ataques a través de la red
  - Herramientas de supervisión del tráfico de red
  - Vulnerabilidades y ataques al protocolo
  - Vulnerabilidades y ataques a los servicios
- Aplicación de medidas de protección de ataques
  - Métodos de intrusiones en sistemas
  - Métodos de infecciones de aplicaciones
  - Herramientas para el descubrimiento de nuevos patrones de ataque
  - Métodos de detección basados en firma
  - Métodos de detección heurísticos
  - Métodos de detección de comportamiento anormal

Habilidades de gestión, personales y sociales

- Asimilación de las funciones y objetivos del centro de operaciones de seguridad en la prevención de ataques de ciberseguridad en las redes.
- Consulta de las fuentes de información sobre los ataques conocidos y las recomendaciones de detección y mitigación de estos.
- Rigor en la selección, recomendación y automatización de las tareas de instalación, configuración y actualización de las herramientas de detección y prevención de ataques.
- Valoración de las características y limitaciones de cada tipo de herramienta de protección y detección
- Organización de los equipos de supervisión y detección de ataques.

MÓDULO DE FORMACIÓN 2: HERRAMIENTAS BÁSICAS DE PREVENCIÓN

OBJETIVO

Configurar las herramientas básicas de protección de un sistema informático.

DURACIÓN EN CUALQUIER MODALIDAD DE IMPARTICIÓN: 18 horas

Teleformación: Duración de las tutorías presenciales: 0 horas

RESULTADOS DE APRENDIZAJE

Conocimientos / Capacidades cognitivas y prácticas

- Análisis de los Cortafuegos
  - Principios de funcionamiento
  - Tipos de cortafuegos: tradicionales, UTM (Unified Threat Management) y NGFW (Next Generation Firewall)
  - Políticas de filtrado
  - Gestión y configuración de firewalls
- Aplicación de sistemas de protección contra virus y malware
  - APT: Amenazas persistentes avanzadas
  - Concepto de EPP (Endpoint protecction platform)
  - Concepto de EDR (Endpoint Detection and Response)
  - Gestión y configuración de sistemas EDR
  - Estrategias de configuración de sistemas de protección en los endpoints.
  - Ejemplos de sistemas EDR y EPP

Habilidades de gestión, personales y sociales

- Sensibilización para seleccionar los cortafuegos más adecuados en la detección de los tipos y patrones de ataque conocidos, tanto a nivel de red, como de aplicación.
- Valoración de aplicación de políticas de filtrado.
- Rigor en la selección de los sistemas de protección contra virus y programas maliciosos (Malware) más adecuadas para las características del tráfico y documentos gestionados en la organización, en función de sus características funcionales y operativas.
- Coordinación en la gestión y configuración de los sistemas de protección y detección de programas maliciosos.

MÓDULO DE FORMACIÓN 3: CONTROL DE ACCESO DE USUARIOS Y APLICACIONES

OBJETIVO

Planificar los mecanismos de autenticación y autorización de usuarios más adecuados para evitar la suplantación de identidad y/o accesos no autorizados, desde su diseño hasta su mantenimiento.

DURACIÓN EN CUALQUIER MODALIDAD DE IMPARTICIÓN: 18 horas

Teleformación: Duración de las tutorías presenciales: 0 horas

RESULTADOS DE APRENDIZAJE

Conocimientos / Capacidades cognitivas y prácticas

- Configuración de mecanismos de control de acceso y autenticación
  - Métodos de identificación de los usuarios (contraseñas, biometría, etc.). ID digital y firma-e. Riesgos y beneficios de la ID digital

- Sistemas de gestión de los derechos de acceso de usuario: ACL, RBAC, PBAC
- Sistemas de autenticación vs. autorización
- Sistemas de federación de Identidades: SSO
- Artefactos de acreditación de derechos de acceso (SAML)
- Procedimientos de otros y bajas de usuarios y privilegios.

- Análisis de propuestas prácticas de control de acceso a aplicaciones
  - Autenticación y autorización en servicios WEB.
  - OAuth, OAuth2 y tokens.

Habilidades de gestión, personales y sociales

- Evaluación desde riesgos asociados a potenciales suplantadores de identidad.
- Canalización de las necesidades de los usuarios de conocimiento y gestión de los datos sensibles vinculadas a los procesos de negocio de la corporación.
- Rigor en la selección, planificación e implantación de los mecanismos de autenticación más adecuadas para cada aplicación y colectivo de usuarios.
- Responsabilidad en la redacción y mantenimiento de los procedimientos de gestión de identidad dentro de la corporación.

MÓDULO DE FORMACIÓN 4: HERRAMIENTAS DE GESTIÓN DE PROCESOS DE RECUPERACIÓN

OBJETIVO

Planificar los procedimientos de recuperación de datos y servicios de las corporaciones, así como las herramientas más básicas para conseguirlo de forma eficiente y efectiva, incluyendo su validación.

DURACIÓN EN CUALQUIER MODALIDAD DE IMPARTICIÓN: 20 horas

Teleformación: Duración de las tutorías presenciales: 0 horas

RESULTADOS DE APRENDIZAJE

Conocimientos / Capacidades cognitivas y prácticas

- Planificación de la recuperación y restauración de servicios después de un incidente
  - Definición e implantación de los planes de recuperación, según el tipo de incidente e impacto
  - Definición e implantación de los planes de restauración de los procesos de negocio.
  - Planificación y ejecución de ejercicios de recuperación y restauración
- Gestión de las copias de seguridad
  - Tipo de copias de seguridad, según la frecuencia y la ubicación de las copias
  - Herramientas de automatización de procesos de copia
  - Procedimientos y pruebas de recuperación de copias
  - Protección de las copias de seguridad
  - Políticas de copias de seguridad
- Aplicación de herramientas de configuración y mantenimiento remotos
  - Herramientas de acceso remoto a dispositivos de sobremesa y portátiles.
  - Herramientas de acceso remoto a dispositivos móviles
  - Capacidades de instalación, control y configuración remotas.

Habilidades de gestión, personales y sociales

- Negociación en la identificación de los procesos de negocio críticos y de los componentes de los sistemas informáticos necesarios para su funcionamiento.
- Responsabilidad en el dimensionado de los recursos necesarios para la recuperación de los procesos de negocio de la corporación, y planificación de su puesta en marcha en caso de incidente grave.
- Rigor en la configuración, planificación, mantenimiento y validación de los procedimientos de recuperación de datos.
- Colaboración en la puesta en marcha de herramientas de mantenimiento remoto de dispositivos y formación del personal en su utilización responsable.

MÓDULO DE FORMACIÓN 5: PLANES DE INSTALACIÓN Y OPERACIÓN DE SISTEMAS DE GESTIÓN DE LA CIBERSEGURIDAD

OBJETIVO

Aplicar las herramientas y procesos necesarios para gestionar la seguridad de los sistemas de información.

DURACIÓN EN CUALQUIER MODALIDAD DE IMPARTICIÓN: 10 horas

Teleformación: Duración de las tutorías presenciales: 10 horas

RESULTADOS DE APRENDIZAJE

Conocimientos / Capacidades cognitivas y prácticas

- Detección de anomalías en el tráfico de una red corporativa
  - Configuración de una herramienta de supervisión del tráfico en la red
  - Configuración de una herramienta de detección de anomalías en la red
- Detección de indicadores de ataque o incidente
  - Reconocimiento de patrones de ataque
  - Detección de intrusiones e infecciones en las redes y sistemas corporativos
- Automatización de procedimientos
  - Instalación y configuración de las herramientas de protección contra incidentes.
  - Supervisión de funcionamiento y optimización de eficiencia
- Recuperación después de un incidente de seguridad informática
  - Planificación de los procedimientos y designación de responsabilidades
  - Puesta en práctica y validación de los procedimientos

Habilidades de gestión, personales y sociales

- Colaboración con otros miembros de la organización en la definición, planificación y validación de los procedimientos de recuperación y restauración de servicios y procesos de negocio.
- Rigor en la redacción de informes de resultados.

Resultados que obligatoriamente deben adquirirse en presencial

- Detección de anomalías en el tráfico de una red corporativa
  - Configuración de una herramienta de supervisión del tráfico en la red
  - Configuración de una herramienta de detección de anomalías en la red
- Detección de indicadores de ataque o incidente
  - Reconocimiento de patrones de ataque
  - Detección de intrusiones e infecciones en las redes y sistemas corporativos
- Automatización de procedimientos
  - Instalación y configuración de las herramientas de protección contra incidentes.
  - Supervisión de funcionamiento y optimización de eficiencia
- Recuperación después de un incidente de seguridad informática
  - Planificación de los procedimientos y designación de responsabilidades
  - Puesta en práctica y validación de los procedimientos

ORIENTACIONES METODOLÓGICAS

La impartición de la docencia se llevará a cabo complementando:

- Introducción de conceptos teóricos y metodológicos
- Estudio de casos en que se hayan aplicado estos
- 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 fin del curso. En las evaluaciones programadas se pueden agrupar conocimientos de varios 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 diferentes resultados de aprendizaje, y que garanticen la fiabilidad y validez de la misma.
- Cada instrumento de evaluación se acompañará del correspondiente sistema de corrección y puntuación en el que se explicite, de forma clara e inequívoca, los criterios de medición para evaluar los resultados alcanzados por los alumnos.
- La puntuación final alcanzada se expresará en términos de Apto / No Apto.