Catálogo de Especialidades Formativas

PROGRAMA FORMATIVO

CIBERSEGURIDAD Y CIBERINTELIGENCIA

Noviembre 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:	CIBERSEGURIDAD Y CIBERINTELIGENCIA
Familia Profesional:	INFORMÁTICA Y COMUNICACIONES
Área Profesional:	SISTEMAS Y TELEMÁTICA
Código:	IFCT0018
Nivel de cualificación profesional:	4

Objetivo general

Adquirir conocimientos altamente especializados sobre ciberseguridad y ciberinteligencia.

Relación de módulos de formación

Módulo 1	COMPUTER NETWORK DEFENSE	140 horas
Módulo 2	VIGILANCIA DIGITAL Y CIBERINTELIGENCIA	60 horas
Módulo 3	OFFENSIVE CYBER CAPABILITIES	100 horas
Módulo 4	SEGURIDAD INDUSTRIAL	80 horas
Módulo 5	CIBERSEGURIDAD EN UN CONTEXTO EMPRESARIAL	40 horas

Modalidad de impartición

Mixta

Duración de la formación

Duración total 420 horas

Mixta Duración total de la formación presencial: 344 horas

Requisitos de acceso del alumnado

Acreditaciones / titulaciones	Cumplir como mínimo alguno de los siguientes requisitos: Título de Grado o equivalente
Experiencia profesional	No se requiere
Otros	Título de Grado o equivalente en el ámbito de Telecomunicaciones, Informática, Ingeniería industrial, Biomedicina y Matemáticas.
Modalidad mixta	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.

Prescripciones de formadores y tutores

Acreditación requerida	Cumplir como mínimo alguno de los siguientes requisitos: • Licenciado, ingeniero, Arquitecto o Título de grado preferiblemente en las ingenierías de Informática, Telecomunicaciones o Industrial.
Experiencia profesional mínima requerida	• Si se cuenta con la titulación requerida se acreditará un mínimo 2 años de experiencia profesional en el ámbito al que se dirige la formación. • Si no se cuenta con la titulación requerida se deberá acreditar una experiencia profesional de al menos cuatro años en el ámbito al que se dirige la formación.
Competencia docente	• Certificado de profesionalidad de docencia de la Formación profesional para el empleo o equivalente o tener formación en metodología didáctica para adultos (mínimo 300 horas) • Acreditar experiencia docente superior a 300 horas
Modalidad mixta	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

• Acreditar mediante documentación la titulación/es o certificación/es académicas y la experiencia profesional.

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.
Otras especificaciones
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: • Aula virtual propia basada en el LMS Moodle. • Equipos portátiles y periféricos. • Plataforma de telecomunicaciones.

Si la especialidad se imparte en **modalidad mixta**, para realizar la parte presencial de la formación, se utilizarán los espacios formativos y equipamientos necesarios indicados anteriormente.

Para impartir la formación en **modalidad mixta**, 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

  - 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)

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: COMPUTER NETWORK DEFENSE

OBJETIVO

Aplicar los conceptos, herramientas y metodologías utilizados en el área de Defensa de una empresa del sector, profundizando en los distintos equipos que la componen: SOC, Threat Hunting, Forense y Lab52.

DURACIÓN TOTAL: 140 horas

Mixta: Duración de la formación presencial: 112 horas

RESULTADOS DEL APRENDIZAJE

Conocimientos / Capacidades cognitivas y prácticas

- Conocimientos relativos al funcionamiento de un SOC.
- SOC
- Interpretación de los casos de uso más comunes en la gestión de incidentes de seguridad.
- Gestión de incidente, grupos de intervención rápida.
- Selección de las herramientas y metodologías de análisis más adecuadas para la respuesta a incidentes.
- Forense.
- Identificación de las principales metodologías de análisis de malware y reversing.
- Introducción al malware.
- Honeynets.
- Establecimiento de los mecanismos para securizar una red.
- IDS, HIDS, dispositivos de red.
- Correlación.
- Comprensión y utilización de la suite de productos propios.
- Correlación.

Habilidades de gestión, personales y sociales

- Capacidad de trabajo en equipo
- Valoración de la importancia de tener autoconfianza e iniciativa.

Resultados que tienen que adquirirse en presencial

Deberán realizarse de forma presencial las siguientes actividades:

- Conocimientos relativos al funcionamiento de un SOC.
- SOC
- Interpretación de los casos de uso más comunes en la gestión de incidentes de seguridad.
- Gestión de incidente, grupos de intervención rápida.
- Selección de las herramientas y metodologías de análisis más adecuadas para la respuesta a incidentes.
- Forense.
- Identificación de las principales metodologías de análisis de malware y reversing.
- Introducción al malware.
- Honeynets.

- Establecimiento de los mecanismos para securizar una red

MÓDULO DE FORMACIÓN 2: VIGILANCIA DIGITAL Y CIBERINTELIGENCIA

OBJETIVO

Desarrollar proyectos de auditoría en el ámbito de inteligencia y geopolítica, aplicando los conceptos y metodologías utilizados en el área de Vigilancia Digital Industrial.

DURACIÓN TOTAL: 60 horas

Mixta: Duración de la formación presencial: 48 horas

RESULTADOS DEL APRENDIZAJE

Conocimientos / Capacidades cognitivas y prácticas

- Comprensión de los distintos proyectos y servicios que se ofrecen desde Vigilancia Digital y Lab52.
- Comprensión del concepto de Inteligencia, sus tipos y el ciclo de Inteligencia.
- Comprensión de la necesidad de la aplicación de la Inteligencia, geopolítica y social media en el ámbito de la ciberseguridad.
- Conocimiento de los diferentes conflictos geopolíticos globales más significativos.
- Conocimiento y comprensión de las disciplinas de OSINT, SOCMINT y HUMINT.
- Conocimiento de las herramientas y búsquedas más adecuadas para cada tipo de investigación.
- Clarificación de los mitos de la Darkweb.
- Generación de un informe de Information Gathering básico.
- Conocer los ataques más comunes de los delincuentes en fuentes abiertas y social media.

Habilidades de gestión, personales y sociales

- Valoración de la importancia de la capacitad organizativa en del desarrollo del trabajo
- Importancia en el establecimiento de objetivos y prioridades en el desarrollo del proyecto

Resultados que tienen que adquirirse en presencial

Deberán realizarse de forma presencial las siguientes actividades:

- Comprensión del concepto de Inteligencia, sus tipos y el ciclo de Inteligencia.
- Comprensión de la necesidad de la aplicación de la Inteligencia, geopolítica y social media en el ámbito de la ciberseguridad.
- Conocimiento de los diferentes conflictos geopolíticos globales más significativos.
- Conocimiento y comprensión de las disciplinas de OSINT, SOCMINT y HUMINT.

MÓDULO DE FORMACIÓN 3: OFFENSIVE CYBER CAPABILITIES

OBJETIVO

Desarrollar proyectos de hacking ético en distintos ámbitos, aplicando conceptos y metodologías utilizados en el área de Ataque.

DURACIÓN TOTAL:

100 horas

Mixta: Duración de la formación presencial: 80 horas

RESULTADOS DEL APRENDIZAJE

Conocimientos / Capacidades cognitivas y prácticas

- Conocimiento de la estructura y objetivos de los distintos tipos de servicios de hacking ético.
- Servicios de ataque.
- Determinación de las distintas fases a la hora de abordar un proyecto prestado por el equipo de OCC.
- Metodologías de ataque.
- Adquisición de agilidad en la elección y uso de herramientas de hacking.
- Hacking Ético interno y externo.
- Evaluación desde un punto de vista objetivo el nivel de riesgo de una aplicación, sistema, plataforma o infraestructura.
- Hacking Ético interno y externo.
- Auditoría web.
- Auditoría Wi-Fi.
- Ingeniería social.
- Auditoría de aplicaciones móviles.
- Selección de las TTPs adecuadas a cada fase de un proceso de intrusión dado un escenario de partida.
- Hacking Ético interno y externo.
- Auditoría web.
- Auditoría Wi-Fi.
- Ingeniería social.
- Auditoría de aplicaciones móviles.
- Identificar, desarrollar y poner en práctica los procedimientos técnicos que lleven al auditor hasta los objetivos de un proyecto.
- Hacking Ético interno y externo.
- Auditoría web.
- Auditoría Wi-Fi.
- Ingeniería social.
- Auditoría de aplicaciones móviles.
- Interpretación y expresión técnica y desde un punto de vista ejecutivo de los resultados de un análisis de vulnerabilidades.
- Hacking Ético interno y externo.
- Auditoría web.

Habilidades de gestión, personales y sociales

Capacidad de toma de decisiones a la hora de implementar servicios de hacking ético.

Resultados que tienen que adquirirse en presencial

Deberán realizarse de forma presencial las siguientes actividades:

- Conocimiento de la estructura y objetivos de los distintos tipos de servicios de hacking ético.
- Servicios de ataque.
- Determinación de las distintas fases a la hora de abordar un proyecto prestado por el equipo de OCC.
- Metodologías de ataque.
- Adquisición de agilidad en la elección y uso de herramientas de hacking.
- Hacking Ético interno y externo.
- Evaluación desde un punto de vista objetivo el nivel de riesgo de una aplicación, sistema, plataforma o infraestructura.
- Hacking Ético interno y externo.
- Auditoría web.
- Auditoría Wi-Fi.
- Ingeniería social.
- Auditoría de aplicaciones móviles.
- Selección de las TTPs adecuadas a cada fase de un proceso de intrusión dado un escenario de partida.
- Hacking Ético interno y externo.
- Auditoría web.
- Auditoría Wi-Fi.
- Ingeniería social.
- Auditoría de aplicaciones móviles.
- Identificar, desarrollar y poner en práctica los procedimientos técnicos que lleven al auditor hasta los objetivos de un proyecto.

MÓDULO DE FORMACIÓN 4: SEGURIDAD INDUSTRIAL

OBJETIVO

Desarrollar proyectos de auditoría, aplicando conceptos y metodologías utilizados en el área de Seguridad industrial.

DURACIÓN TOTAL: 80 horas

Mixta: Duración de la formación presencial: 64 horas

RESULTADOS DEL APRENDIZAJE

Conocimientos / Capacidades cognitivas y prácticas

- Conceptos básicos de los Sistemas de Control Industrial (ICS) y el marco normativo correspondiente.
- Reconocimiento de las bases sobre las que se asienta el Internet de las Cosas.
- Realización de un Taller de Control Industrial.
- Principales técnicas y tácticas respecto al ataque y la defensa de los ICS.
- Realización de un análisis fundamental de una red industrial.
- Conocimiento de los procesos industriales básicos presentes en la mayoría de las organizaciones.
- Conocimiento del funcionamiento del sector eléctrico español.

Habilidades de gestión, personales y sociales

Asimilación de las metodologías de defensas utilizadas en el área de la seguridad industrial

Resultados que tienen que adquirirse en presencial

Deberán realizarse de forma presencial las siguientes actividades:

- Conceptos básicos de los Sistemas de Control Industrial (ICS) y el marco normativo correspondiente.
- Reconocimiento de las bases sobre las que se asienta el Internet de las Cosas.
- Realización de un Taller de Control Industrial.

MÓDULO DE FORMACIÓN 5: CIBERSEGURIDAD EN UN CONTEXTO EMPRESARIAL

OBJETIVO

Aplicar los conocimientos y las competencias en ciberseguridad en un contexto empresarial.

DURACIÓN TOTAL: 40 horas

Mixta: Duración de la formación presencial: 40 horas

RESULTADOS DEL APRENDIZAJE

Conocimientos / Capacidades cognitivas y prácticas

. Integración de las competencias sobre ciberseguridad, en un contexto empresarial.
• Ejecución de proyectos de investigación, desarrollo e innovación, con garantía de la seguridad para las personas y bienes, la calidad final de los productos y su homologación.
• Comprensión y aplicación de conocimientos ciberseguridad a problemas reales.
• Diseño y desarrollo de sistemas, aplicaciones y servicios informáticos específicos del ámbito de la ciberseguridad.
• Utilización y desarrollo de metodologías, métodos, técnicas y programas de uso específico del ámbito de la ciberseguridad, ajustados a normas y estándares de la misma.
• Integración de tecnologías y sistemas propios de una empresa en diferentes contextos de y frente a diferentes problemas de ciberseguridad.

Habilidades de gestión, personales y sociales

Demostración de interés por la integración de diferentes técnicas y metodologías para la aplicación la ciberseguridad en un contexto empresarial.

Resultados que tienen que adquirirse en presencial

Deberán realizarse de forma presencial las siguientes actividades:

• Integración de las competencias sobre ciberseguridad, en un contexto empresarial.
• Ejecución de proyectos de investigación, desarrollo e innovación, con garantía de la seguridad para las personas y bienes, la calidad final de los productos y su homologación.
• Comprensión y aplicación de conocimientos ciberseguridad a problemas reales.
• Diseño y desarrollo de sistemas, aplicaciones y servicios informáticos específicos del ámbito de la ciberseguridad.
• Utilización y desarrollo de metodologías, métodos, técnicas y programas de uso específico del ámbito de la ciberseguridad, ajustados a normas y estándares de la misma.
• Integración de tecnologías y sistemas propios de una empresa en diferentes

contextos de y frente a diferentes problemas de ciberseguridad.

ORIENTACIONES METODOLÓGICAS

• Metodología Resultado-Aprendizaje, incluyendo los propios resultados de aprendizaje de cada módulo, las asignaturas.
• Buenas prácticas para fomentar la interacción y el aprendizaje en clase.
• Instrucciones técnicas de acceso a recursos, plataformas, y herramientas de una empresa real.

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.

En resumen, cada módulo de esta acción formativa dispone de un método de evaluación adaptado a las propias necesidades, y definido en base a la metodología de resultado-aprendizaje. Por tanto, son los responsables últimos de cada módulo los que, junto con el equipo de coordinación, definen las diferentes acciones a llevar a cabo para medir y evaluar de manera holística a los alumnos.