Catálogo de Especialidades Formativas

PROGRAMA FORMATIVO

Ciberseguridad. Riesgos y amenazas en la red

Marzo 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. RIESGOS Y AMENAZAS EN LA RED
Familia Profesional:	INFORMÁTICA Y COMUNICACIONES
Área profesional:	SISTEMAS Y TELEMÁTICA
Código:	IFCT121
Nivel de cualificación profesional:	3

Objetivo general

Concienciar a los usuarios de los posibles riesgos que pueden afectarle a nivel individual y de empresa, así como facilitarles una serie de “buenas prácticas” que puedan aplicar no sólo en su espacio de trabajo sino también en su vida personal.

Relación de módulos de formación

Módulo 1 Ciberseguridad. Riesgos y amenazas en la red 10 horas

Modalidades de impartición

Teleformación

Duración de la formación

Duración total 10 horas

Teleformación Duración total de las tutorías presenciales: 0 horas

Requisitos de acceso del alumnado

Acreditaciones / titulaciones	No se requieren acreditaciones/titulaciones. No obstante, se han de poseer las habilidades de comunicación lingüística suficientes que permitan cursar con aprovechamiento la formación.
Experiencia profesional	Experiencia en el sector mínima de 6 meses.
Modalidad de teleformación	Además de lo indicado anteriormente, los participantes han de tener las destrezas suficientes para ser usuarios de la plataforma virtual en la que se apoya la acción formativa.

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. - Diplomado, Ingeniero Técnico, Arquitecto Técnico o el Título de Grado correspondiente u otros títulos equivalentes. - Técnico o Técnico Superior de F.P. - Certificados de profesionalidad de nivel 2 o 3.

Experiencia profesional mínima requerida	Se requiere una experiencia mínima en el sector de al menos 2 años.
Competencia docente	Se requiere un mínimo de 300 horas de experiencia como docente o estar en posesión del Certificado de Profesionalidad de Docencia de la Formación Profesional para el empleo o equivalente.
Otros	Esta acción formativa será diseñada y desarrollada por un/a formador/a experto/a en la materia con experiencia y formación pedagógica.
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.

Requisitos mínimos de espacios, instalaciones y equipamientos

Para impartir la formación en **modalidad 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/as 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/as 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/as 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/a pueda interaccionar a través del navegador con el tutor-formador, el sistema y con los demás alumnos/as. 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/as, 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/a 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

Ocupaciones relacionadas con el ámbito profesional de la informática y las comunicaciones.

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: CIBERSEGURIDAD. RIESGOS Y AMENAZAS EN LA RED

OBJETIVO

Concienciar a los usuarios de los posibles riesgos que pueden afectarle a nivel individual y de empresa, así como facilitarles una serie de "buenas prácticas" que puedan aplicar no sólo en su espacio de trabajo sino también en su vida personal.

DURACIÓN: 10 horas

Teleformación Duración de las tutorías presenciales: 0 horas

RESULTADOS DE APRENDIZAJE

Conocimientos/ Capacidades cognitivas y prácticas

- Conocimientos avanzados sobre nuestra identidad digital.
  - Capacidad de identificación personal en el ámbito digital.
  - Conocimiento sobre la protección de nuestra identidad digital.
  - Conocimiento sobre los derechos asociados a la identidad digital.
  - Conocimiento avanzado de los aspectos de navegación segura por internet.
  - Capacidad de identificación y uso de protocolos seguros en internet.
  - Conocimiento avanzado sobre el proceso de reporte y comunicación de ciberincidentes.
- Conocimiento de las ciberamenazas y aplicación de técnicas de defensa.
  - Conocimiento de los incidentes de seguridad (robo, filtrado y secuestro de información) y sus características.
  - Capacidad para la implementación de las estrategias de protección contra los ciberataques.
  - Capacidades para aplicar técnicas de defensa en el ciber-entorno.
  - Capacidad para minimizar los daños causados por los posibles ciberincedentes.
- Conocimiento avanzado de los lenguajes de programación en ciberseguridad.
  - Conocimiento del leguaje común de los ciberriesgos.
  - Conocimiento de los principales lenguajes de programación orientados a la ciberseguridad.
  - Conocer los lenguajes que utilizan los hackers.
- Detección, análisis y anticipación a los riesgos de seguridad.
  - Conocimiento sobre las vulnerabilidades y riesgos de seguridad informática.
  - Detección, análisis y anticipación a los riesgos de seguridad.
  - Conocimiento sobre los comportamientos que ponen en riesgo nuestra seguridad en entornos digitales.
  - Capacidad de detección incipiente de los riesgos y minimización de los efectos de los daños producidos en la seguridad digital.
- Implementación de buenas prácticas en entorno digital.
  - Capacidad de búsqueda y localización de información sobre buenas prácticas en las entidades oficiales de gestión de la ciberseguridad (CCN-CERT o INCIBE).
  - Capacidad de implementar buenas prácticas en el entorno digital a través del conocimiento de los principales mecanismos de protección (gestión segura de contraseñas, gestión y control de los sistemas de antivirus, control de accesos y aplicaciones críticas, etc.).
  - Capacidad de identificación y clasificación de la información que se maneja en entorno digital y aplicación de las medidas necesarias para su protección que se plasmará en distintas políticas de seguridad informática.

Habilidades de gestión, personales y sociales

- Habilidad para la implementación de procesos y protocolos para la protección de los archivos y evitar poner en riesgo los datos por cualquier tipo de amenaza.
- Habilidad para el análisis y evaluación de los riesgos y peligros que afectan a una organización con identificación de los activos de información, definición de las amenazas a las que pueden estar expuestos, detectar vulnerabilidades definiendo sus riesgos y consecuencias.
- Habilidad para implementación y gestión de políticas de protección ante los peligros de la red mediante el uso de herramientas de seguridad y métodos para evitar estas amenazas.
- Habilidad para prevenir los riesgos de nuestra privacidad digital utilizando métodos de encriptación de la información de internet, autentificación multifactor, contando con programas informáticos que proporcione seguridad al sistema.
- Habilidad para el análisis de datos y estadísticas sobre las motivaciones que hay detrás de los ciberataques.
- Capacidad para mejorar la seguridad informática tras el análisis de las motivaciones de los ciberataques y los incidentes que estos provocan, extrayendo aprendizajes para afrontar con éxito los ciberataques

ORIENTACIONES METODOLÓGICAS

- La metodología está basada en casos prácticos y autoevaluciones.

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.
- Autoevaluación mediante pruebas objetivas que permiten a cada participante comprobar de forma autónoma si ha alcanzado los objetivos propuestos, lo que aumenta su motivación, con la realización de casos prácticos de aplicación de contenido en cada uno de los módulos del curso.