Catálogo de Especialidades Formativas

PROGRAMA FORMATIVO

Gestión de la ciberseguridad en PYMES. Comercio electrónico seguro

Noviembre 2020

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:	GESTIÓN DE LA CIBERSEGURIDAD EN PYMES. COMERCIO ELECTRÓNICO SEGURO
Familia Profesional:	COMERCIO Y MARKETING
Área Profesional:	MARKETING Y RELACIONES PÚBLICAS
Código:	COMM03
Nivel de cualificación profesional:	3

Objetivo general

Aplicar los aspectos fundamentales en los que se basa la ciberseguridad para detectar posibles ciberataques e implementar en las pequeñas y medianas empresas, mecanismos de defensa que protejan la información y los recursos que manejan dicha información, así como los aspectos que permiten garantizar la continuidad del negocio en una empresa mediante el desarrollo de políticas de seguridad, la aplicación de recursos humanos, técnicos y de procedimiento para proteger la información sensible y el aseguramiento de la disponibilidad de los dispositivos que manejan la información.

Relación de módulos de formación

Módulo 1	Introducción a la ciberseguridad	20 horas
Módulo 2	Aplicación de la ciberseguridad en las PYMES	30 horas

Modalidades de impartición

Presencial

Teleformación

Duración de la formación

Duración total en cualquier modalidad de impartición	50 horas
Teleformación	Duración total de las tutorías presenciales: 0 horas

Requisitos de acceso del alumnado

Acreditaciones/ titulaciones	Cumplir como mínimo alguno de los siguientes requisitos: - Título de Técnico Superior (FP Grado Superior) o equivalente - Haber superado la prueba de acceso a Ciclos Formativos de Grado Superior - Haber superado cualquier prueba oficial de acceso a la universidad - Certificado de profesionalidad de nivel 3 - Título de Grado o equivalente - Título de Postgrado (Máster) o equivalente
Experiencia profesional	No se requiere
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.

Justificación de los requisitos del alumnado

Se justificarán documentalmente las acreditaciones correspondientes a títulos y/o certificados

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 - Título de Postgrado (Máster) o equivalente
Experiencia profesional mínima requerida	Se requiere un mínimo de tres años de experiencia profesional en el área de conocimiento relacionado con lo establecido en el programa formativo.
Competencia docente	Se requiere un mínimo de dos años de experiencia como docente, o estar en posesión del Certificado de Profesionalidad de Docencia de la Formación Profesional para el Empleo o equivalente.
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

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 - PCs-portátiles instalados en red e Internet - Software específico para el aprendizaje de cada acción formativa: o Servidor virtual o entorno de aprendizaje virtual para simular aplicaciones prácticas de ciberseguridad.

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 m^2/ 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.

Además, en el caso 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 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 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 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.

Aula virtual

Tecnología y equipos	Plataforma de aprendizaje 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 los participantes, con registro de los tiempos de conectividad.

Ocupaciones y puestos de trabajo relacionados

- 13211026 Directores de departamento de servicios informáticos, en general
- 24111029 Físicos
- 24151021 Matemáticos
- 27111028 Analistas de sistemas, nivel superior
- 27121021 Analistas de aplicaciones, nivel superior
- 27231014 Diseñadores de red
- 27111037 Ingenieros informáticos
- 27221011 Técnicos superiores de mantenimiento y reparación de equipos informáticos
- 27121012 Analistas de aplicaciones, nivel medio
- 27111019 Analistas de sistemas, nivel medio
- 27121030 Analistas-programadores, nivel medio
- 27191022 Ingenieros técnicos en informática, en general
- 27111046 técnicos en informática de sistemas
- 27121049 Ingenieros técnicos en informática de gestión

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: INTRODUCCION A LA CIBERSEGURIDAD

OBJETIVO

Identificar todos los aspectos fundamentales en los que se basa la ciberseguridad para detectar posibles ciberataques e implementar en las pequeñas y medianas empresas, mecanismos de defensa que protejan la información y los recursos que manejan dicha información.

DURACIÓN EN CUALQUIER MODALIDAD DE IMPARTICIÓN: 20 horas

Teleformación Duración de las tutorías presenciales: 0 horas

RESULTADOS DE APRENDIZAJE

Conocimientos/ Capacidades cognitivas y prácticas

- Identificación de los conceptos básicos de ciberseguridad y su relación con la seguridad
  - Definición y alcance de la ciberseguridad
  - Áreas de actuación de la ciberseguridad
  - Ubicación de la ciberseguridad
  - Dimensiones de la seguridad y garantías que ofrece
  - Implementación de las dimensiones
  - Protección de la información
- Relación entre las amenazas y las vulnerabilidades reconociendo sus efectos en los sistemas
  - Ingeniería social
  - Vulnerabilidades en la autenticación
  - Malware y botnets
  - Seguridad en el perímetro de las redes
  - Riesgos de seguridad
  - Incidentes de seguridad
- Identificación de los mecanismos de defensa a implementar en las redes privadas
  - Defensa en profundidad y la DMZ
  - Antimalware
  - Contraseñas
  - Control de acceso
  - Controles para definir una red segura
  - Sistemas de detección de ataques
  - Recuperación de los sistemas ante un ciberataque
- Utilidad de la correlación de eventos en la prevención e investigación de incidentes
  - Eventos y tipos
  - Eventos de los sistemas de seguridad
  - Criticidad de los eventos
  - Tratamiento de los eventos para su automatización
  - Soluciones de automatización. El SIEM
- Identificación de las medidas de seguridad en las redes inalámbricas y dispositivos móviles
  - La conexión inalámbrica y las redes
  - Configuración de seguridad de las WLAN
  - Medidas de seguridad en el router
  - Amenazas en los terminales móviles
- Caracterización de los mecanismos de protección de la información
  - Fuga de la información
  - Gestión de la fuga de información
  - Métodos de copia de seguridad
  - Restauración de los datos

- Reconocimiento de los sistemas biométricos y aplicaciones
  - Técnicas biométricas
  - Aplicaciones de la biometría
  - Gestión de riesgos en biometría
- Identificación de los servicios que se implementan en la nube
  - Cloud computing
  - Seguridad en la nube
  - Servicios de seguridad en la nube
- Caracterización de los diferentes tipos de ciberataques
  - Categorías de los ciberataques
  - Ataques para obtener información
  - Ataques a nivel de red
  - Ataques de monitorización
  - Ataques de autenticación
  - Ataques de denegación de servicio

Habilidades de gestión, personales y sociales

- Concienciación sobre la importancia de identificar correctamente y con rapidez los ciberataques a los que pueda estar sometida una PYME para minimizar o anular sus efectos.
- Actitud responsable en la implementación adecuada de arquitecturas y soluciones en las redes privadas de las PYMES, de forma que estén protegidas ante ataques de intrusión externa y/o sabotajes internos.
- Fomento de una actitud responsable en la implementación de los controles de seguridad en los recursos de red de la PYMES para asegurar la disponibilidad de los servicios que alojan y analizando las consecuencias de una implementación errónea.

MÓDULO DE FORMACIÓN 2: APLICACIÓN DE LA CIBERSEGURIDAD EN LAS PYMES

OBJETIVO

Identificar los aspectos que permiten describir cómo la ciberseguridad permite garantizar la continuidad del negocio en una empresa mediante el desarrollo de políticas de seguridad, la aplicación de recursos humanos, técnicos y de procedimiento para proteger la información sensible y el aseguramiento de la disponibilidad de los dispositivos que manejan la información.

DURACIÓN EN CUALQUIER MODALIDAD DE IMPARATICIÓN: 30 horas

Teleformación Duración de las tutorías presenciales: 0 horas

RESULTADOS DE APRENDIZAJE

Conocimientos/ Capacidades cognitivas y prácticas

- Introducción de la ciberseguridad en la empresa
  - Seguridad en la empresa
  - Causas de los ataques en la empresa
  - Revisión de ciberseguridad en la empresa
  - Pilares de una estrategia de ciberseguridad
  - Roles en ciberseguridad
  - Controles de seguridad a establecer en una organización
- Identificación del usuario como elemento de ciberseguridad en la empresa
  - Rol del usuario en el puesto de trabajo
  - Protección del puesto de trabajo
  - Acceso remoto y teletrabajo
  - Escritorio virtual

- Detección de necesidades de protección y seguridad en las empresas
  - Clasificación de la información empresarial
  - Medidas de protección de la información
  - Almacenamiento seguro de la información
  - Eliminación de los datos. Borrado seguro
  - Conservación de la información
  - Almacenamiento extraíble
- Desarrollo de planes y políticas de seguridad en una empresa
  - Plan director de seguridad
  - Políticas de seguridad dirigidas a los componentes de la empresa
  - Normas y procedimientos técnicos
- Utilidad de los planes de continuidad de negocio en la empresa
  - Análisis y gestión de riesgos
  - Plan de continuidad de negocio
  - Plan de contingencia
  - Auditorías de seguridad
- Necesidad de un plan de recuperación de desastres en la empresa
  - En plan de recuperación de desastres
  - Guía de desarrollo de un plan de recuperación de desastres
- Introducción a la seguridad en el comercio electrónico
  - Identidad digital y reputación empresarial
  - Cliente online y su protección
  - Redes sociales y la empresa
  - Fraude online
  - Protección de la web
- Aplicación de medidas de ciberseguridad en redes inalámbricas y dispositivos móviles
  - Formas de ataque y métodos de seguridad en las redes inalámbricas
  - Sistemas de gestión de dispositivos móviles de la empresa
  - Estrategia BYOD
- Caracterización de la tecnología IoT en la empresa
  - IoT en la empresa en la actualidad y en el futuro.
  - Riesgos de seguridad
  - Recomendaciones de seguridad

Habilidades de gestión, personales y sociales

- Fomento de la ciberseguridad como elemento positivo en el desarrollo de negocio de una empresa.
- Impulso a la aplicación de las mejores prácticas de ciberdefensa, destacando la importancia de su utilización en el entorno empresarial.
- Reconocimiento de la necesidad de disponer de políticas de seguridad y planes de continuidad del negocio en una empresa.
- Actitud responsable en la aplicación de medidas para mantener la disponibilidad de los recursos empresariales y asegurar la continuidad del negocio.

ORIENTACIONES METODOLÓGICAS

El enfoque didáctico debe combinar la asimilación del marco conceptual de la disciplina, su aplicabilidad en casos de éxito y ejercicios participativos individuales y grupales, haciendo del programa una experiencia dinámica, práctica y rica en experiencias.

Para alcanzar los resultados de aprendizaje que recogen en el módulo 1 se propone completarlos con la realización del siguiente proyecto.

- Proyecto1. Determinar los mecanismos de protección a implementar en el perímetro de una red privada de una pyme de e-commerce.

Para alcanzar los resultados de aprendizaje que recogen en el módulo 2 se propondrá un caso práctico para ayudar a alcanzar los conocimientos en materia de seguridad de la información.

- Proyecto 2. Establecer las medidas organizativas, técnicas y de procedimiento que permitan utilizar de forma segura una estrategia BYOD en una pyme.

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.