Ciberseguridad para pymes - protege tu negocio sin miedo (GD-04)

Este programa formativo te permitirá adquirir los conocimientos necesarios para proteger tu negocio y poder dar respuesta ante las posibles amenazas de seguridad. Además de implementar buenas prácticas que ayuden a tu empresa a emprender acciones preventivas para poder debilitar o minimizar el riesgo de los ciberataques.
Este proyecto está financiado por la Unión Europea (fondos del programa Next Generation EU) liderado por la Secretaría de Estado de Digitalización e Inteligencia Artificial (SEDIA) del Ministerio para la Transformación Digital y de la Función Pública, en colaboración con la Fundación EOI F.S.P., cuyo objetivo es la formación en gestión digital para pymes con el fin de mejorar su productividad y sus posibilidades de crecimiento e internacionalización.

Financiado por la Unión Europea NextGenerationEU

MODALIDADES

Este curso está disponible en modalidad Live Training (Virtual EN DIRECTO)

REQUISITOS

- Ser trabajador/a de una pyme española (con número de empleados de 1 a 249)
- Pueden participar en el curso hasta 5 empleados por empresa (CIF)

OBJETIVO

- Es un programa totalmente gratuito que te va a permitir:
- Mejorar la seguridad de tu negocio.
- Estar al tanto de las amenazas emergentes y tendencias en ciberataque.

- Te va a preparar, para saber dar respuesta a los incidentes de seguridad, aportándote las claves para proteger de forma preventiva tu empresa.
- Además, conocerás la normativa y legislación aplicable.

CONTENIDO

Módulo 1: Introducción a la Ciberseguridad

1.1 ¿Qué es la ciberseguridad? Definición e importancia en el mundo actual.
1.2 Amenazas cibernéticas comunes:
1.2.1 Malware (virus, ransomware, troyanos)
1.2.2 Phishing y ataques de ingeniería social. Ejemplo de campaña real.
1.2.3 Ataques DDoS
1.2.4 Hacking
1.3 Consecuencias de los ciberataques: Pérdidas económicas, daño a la reputación, interrupción de operaciones

Módulo 2: Conceptos Básicos de seguridad informática

2.1 Hardware y software: Componentes básicos de un sistema informático.
2.2 Redes: Funcionamiento básico de las redes, tipos de redes (LAN, WAN).
2.3 Sistemas operativos: Diferencias entre sistemas operativos (Windows, Linux, macOS).
2.4 Seguridad de la información: Conceptos de confidencialidad, integridad y disponibilidad.

Módulo 3: Buenas prácticas de seguridad

3.1 Contraseñas seguras: Creación y gestión de contraseñas fuertes.
3.2 Seguridad en dispositivos móviles: Protección de smartphones y tablets.
3.4 Respaldos de datos: Importancia de realizar copias de seguridad regularmente.
3.3 Navegación segura en internet: Identificación de sitios web fraudulentos.
3.5 Seguridad en el correo electrónico: Cómo evitar caer en ataques de phishing.

Módulo 4. Amenazas Emergentes y Tendencias

4.1 IoT y seguridad: Vulnerabilidades de los dispositivos IoT.
4.2 Cloud computing y seguridad: Riesgos asociados a la computación en la nube.
4.3 Criptografía: Conceptos básicos de cifrado y descifrado.
4.4 Inteligencia artificial y ciberseguridad: Cómo la IA se utiliza tanto para atacar como para defender.

Módulo 5: Incidentes de seguidad y respuesta

5.1 Detección de incidentes: Señales de alerta y herramientas de detección.
5.2 Análisis de incidentes: Investigación de un incidente de seguridad.
5.3 Respuesta a incidentes: Plan de respuesta a incidentes, contención y recuperación.
5.4 Comunicación en caso de incidentes: Cómo comunicar un incidente a los interesados.

Módulo 6: Normativa y Legislación

6.1 Marco legal de la ciberseguridad: Leyes y regulaciones aplicables.
6.2 RGPD: Reglamento General de Protección de Datos.
6.3 Otros estándares: ISO 27001, NIST Cybersecurity Framework.

DURACIÓN

50 horas en directo + 100 horas de formación complementaría.

¿CÓMO OBTENER LA TITULACIÓN?

- Asistir a un mínimo del 75% de horas de duración de las 50 horas de formación live training, con un porcentaje máximo de 25% de faltas horas justificadas
- Realizar el examen final online a la finalización de cada uno de los 6 módulos del curso
- Entrega del Trabajo final sobre la resolución de casos prácticos

OBSERVACIONES

A mayores, contarás con el apoyo de nuestros docentes expertos para poder poner en práctica los conocimientos. Y durante 2 meses tendrás acceso a la biblioteca virtual de campus AENOR con documentación y normas de referencia,. lo que permitirá complementar tu formación con hasta 100 horas más para realizar un caso práctico que aborde todo el temario