

CURSO ONLINE • TODA LA PLANTILLA • ESPAÑOL E INGLÉS

Formación en ciberseguridad

Curso para reconocer las amenazas más habituales (phishing, fraude del CEO, ransomware), conocer las herramientas y normas básicas de protección y adoptar buenas prácticas en el día a día. Con casos reales, casos prácticos de pymes y los pasos a seguir ante un incidente explicados de forma sencilla.

DURACIÓN

2 horas

a tu ritmo

MODALIDAD

100 % online

ordenador o móvil

IDIOMAS

Español e inglés

mismo contenido

FUNDAE

Bonificable

con tu crédito de formación

POR QUÉ ES IMPORTANTE

El artículo 32 del **RGPD** exige a toda empresa aplicar **medidas técnicas y organizativas apropiadas** para proteger los datos, y la concienciación del personal es una de ellas. La **Directiva NIS2** va más allá para las **entidades esenciales e importantes**: obliga a formar a sus órganos de dirección y fomenta la formación periódica de la plantilla. En España, su ley de transposición sigue en tramitación.

OBJETIVOS

Lo que aprenderá tu equipo

- ✓ Entender los conceptos clave de la ciberseguridad y los riesgos del día a día.
- ✓ Reconocer el phishing, el fraude del CEO, el ransomware y la ingeniería social.
- ✓ Conocer las herramientas esenciales: antivirus, cifrado, MFA y VPN.
- ✓ Aplicar buenas prácticas en contraseñas, copias, correo y teletrabajo.
- ✓ Saber cómo actuar y a quién avisar ante un incidente o una brecha de datos.

CÓMO FUNCIONA

Sencillo para la empresa y el alumno

- 01 La empresa da de alta a cada persona y sigue su progreso desde su panel.
- 02 El alumno hace el curso a su ritmo: su avance se guarda solo.
- 03 Cada módulo termina con un test de repaso.
- 04 Un tutor resuelve las dudas en el foro del curso en 48 horas laborables.
- 05 Al aprobar el examen final, el alumno descarga su diploma.

Programa académico

MÓDULO 01

30 MIN

Introducción a la ciberseguridad

- Conceptos clave y tríada CIA: confidencialidad, integridad y disponibilidad
- Amenazas, actores y factor humano: el caso WannaCry y Telefónica (2017)
- Normativa clave: RGPD y LOPDGDD, Esquema Nacional de Seguridad, NIS2 e ISO 27001
- Cómo comunicar una brecha de datos y a quién: notificación a la AEPD en 72 horas
- Ciberhigiene: contraseñas, USB desconocidos y trabajo desde una wifi pública

Test de 10 preguntas · 80 % para superarlo

MÓDULO 02

30 MIN

Amenazas y ataques informáticos

- Panorama actual de amenazas e impacto real de los ciberataques en las empresas
- Tipos de malware y técnicas de ataque: ransomware, DDoS y otras
- Ingeniería social: phishing, fraude del CEO y falso soporte técnico
- Qué hacer en los primeros 15 minutos si sospechas que has caído
- Casos reales: Hospital Clínic de Barcelona (2023), SEPE (2021) y sus lecciones

Test de 10 preguntas · 80 % para superarlo

MÓDULO 03

30 MIN

Herramientas y tecnologías de ciberseguridad

- Tipos de herramientas: antivirus, EDR y XDR, firewalls y su función
- El cifrado en tu día a día y cómo activar MFA y passkeys
- VPN corporativa: beneficios, limitaciones y por qué evitar las gratuitas
- Herramientas avanzadas (CASB, SOAR), defensa en capas y modelo Zero Trust
- Recursos gratuitos de INCIBE (línea 017) y cultura de seguridad sostenible

Test de 10 preguntas · 80 % para superarlo

MÓDULO 04

30 MIN

Buenas prácticas y estrategias de defensa

- Defensa en profundidad y contraseñas: frases de contraseña y gestores
- Copias de seguridad con la regla 3-2-1 aplicada a una pyme, y actualizaciones
- Correo electrónico: cómo analizar un mensaje sospechoso y responder al phishing
- Navegación segura, teletrabajo y qué hacer si pierdes el móvil o el portátil
- Respuesta a incidentes: un caso de ransomware en una pyme y gestión de crisis

Test de 10 preguntas · 80 % para superarlo

EVALUACIÓN

Tests por módulo

10 preguntas por módulo. Se necesita un 80 % para avanzar.

EXAMEN FINAL

20 preguntas · 45 min

80 % para aprobar y 3 intentos. Se abre tras completar el curso y 90 minutos de formación.

ACREDITACIÓN

Diploma descargable

Registro del progreso y de los resultados de cada alumno.

FORMACIÓN BONIFICABLE

Bonificable a través de FUNDAE

Tu empresa puede recuperar el coste del curso con su **crédito de formación**, descontándolo de las cotizaciones a la Seguridad Social. Todas las empresas con personas trabajadoras en el Régimen General disponen de este crédito cada año, con un mínimo de 420 €.

- ✓ Formación en modalidad de teleformación.
- ✓ La plataforma registra conexiones, tiempo de formación y resultados de cada alumno.
- ✓ Tutor asignado y foro de dudas, como exige la teleformación bonificada.
- ✓ Diploma para cada alumno que supera el curso.

IDIOMAS

En español y en inglés

El curso está disponible en **español** y en **inglés**, con el mismo contenido, los mismos tests y el mismo examen final. Ideal para plantillas internacionales que trabajan en España: la versión inglesa explica la normativa aplicable en España en inglés.

A QUIÉN VA DIRIGIDO

A toda la plantilla

- ✓ Empresas de cualquier tamaño y sector que manejan información y datos personales.
- ✓ Pymes que quieren reducir el riesgo de fraudes, ransomware y brechas de datos.
- ✓ Especialmente útil para administración, contabilidad, dirección y teletrabajo.

METODOLOGÍA

Práctico y fácil de seguir

- ✓ Casos prácticos de situaciones reales en la oficina.
- ✓ Ciberataques reales en España explicados de forma sencilla.
- ✓ Contenido interactivo con preguntas de repaso en cada apartado.
- ✓ Tiempo mínimo por pantalla para asegurar una lectura real.

PANEL PARA LA EMPRESA

Control total de la formación

- ✓ Alta de alumnos en minutos con nombre y email.
- ✓ Progreso en tiempo real: minutos, tests y examen de cada persona.
- ✓ Informes descargables para acreditar la formación.
- ✓ Licencias ampliables cuando las necesites.

Cumplir nunca fue tan fácil

Forma a tu plantilla, protege la información de tu empresa y bonifícalo con FUNDAE.

[cumpleo.com →](https://cumpleo.com)