

Ciberseguridad para PYMES

Modalidad:

e-learning con una duración 56 horas

Objetivos:

Desde el punto de vista del día a día de una Pyme o Micropyme, pretendemos abordar el concepto de Ciberseguridad haciendo hincapié en las ciberamenazas que se reciben en una empresa o comercio, y los diferentes sistemas de prevención y defensa existentes. Los 3 puntos fundamentales en los que se basa el itinerario formativo:

Reconocer conceptos básicos y características de ciberseguridad: Al finalizar el curso, los participantes comprenderán los fundamentos de la ciberseguridad, incluyendo conceptos clave y características.

Entender el cibercrimen y los ciberataques: Los participantes deben aprender sobre los diferentes tipos de ciberataques o ciberamenazas, cómo se llevan a cabo y cómo se pueden prevenir. Esto incluye el estudio de casos reales en la historia como ejemplos para comprender mejor las tácticas utilizadas por los ciberdelincuentes.

Promover la prevención y la reacción ante ciberataques: Conocer que tipos de ciberataques se reciben a diario en nuestro negocio o actividad tanto por correo electrónico, vía web, así como mediante las pasarelas de pago, Bizum, etc? ayuda a prevenir, detectar y responder adecuadamente a las ciberamenazas. Esto implica desarrollar habilidades para proteger sistemas y redes, así como para actuar de manera efectiva en caso de incidentes.

Contenidos:

1. Qué se entiende por ciberseguridad

1.1 Definición de ciberseguridad



- 1.2 Objetivos del curso
- 1.3 Evolución de la computación
- 1.4 Conclusión
- 1.5 Cuestionario: Qué se entiende por ciberseguridad

2. Ciberamenazas

- 2.1 Definición de ciberamenazas
- 2.2 Diferencias entre Amenaza Personal y Amenaza Generalizada
- 2.3 Conclusión
- 2.4 Cuestionario: Ciberamenazas

3. Concepto de vulnerabilidad en las Pymes

- 3.1 El concepto de vulnerabilidad en ciberseguridad
- 3.2 Tipos de vulnerabilidad
- 3.3 Implicaciones emocionales y psicológicas de la vulnerabilidad
- 3.4 Como identificar vulnerabilidades en las PYMES
- 3.5 Seguros para proteger su empresa
- 3.6 Cuestionario: Concepto de vulnerabilidad en las Pymes

4. Ciberamenazas comunes en el entorno de las PYMES

- 4.1 Introducción a ciberamenazas
- 4.2 Ciberamenazas
- 4.3 Phishing
- 4.4 Ransomware
- 4.5 Ataques DDos
- 4.6 Malware
- 4.7 APT
- 4.8 Cuestionario: Introducción a Ciberamenazas

5. Ciberamenazas II

- 5.1 Fugas de datos

- 5.2 Pasarelas de pago
- 5.3 Ataques a la cadena de suministros
- 5.4 Amenazas internas
- 5.5 Amenazas asociadas a la instalación de software
- 5.6 Memorias USB infectadas
- 5.7 Cuestionario: Ciberamenazas II

6. Ciberamenazas en el comercio electrónico

- 6.1 Amenazas en los sistemas de pago electrónico
- 6.2 Estafas en la compraventa
- 6.3 Estafas a través de Bizum
- 6.4 Cuestionario: Ciberamenazas en el comercio electrónico

7. Sistemas de protección para PYMES

- 7.1 Concienciación del personal
- 7.2 Reconocimiento de Webs no seguras
- 7.3 Peligros asociados a la descarga de aplicaciones gratuitas
- 7.4 Bloqueo de acceso mediante contraseñas
- 7.5 Actualización de Software
- 7.6 Las copias de seguridad
- 7.7 Firewall y antivirus para la protección de tu PYME
- 7.8 Controles de acceso
- 7.9 Seguridad en la nube
- 7.10 Política de uso de dispositivos personales BYOD
- 7.11 Monitorización y detección temprana
- 7.12 Plan de respuesta ante incidentes
- 7.13 Cuestionario: Sistemas de protección para PYMES

8. Formular una denuncia ante un ciberataque en España

- 8.1 Pasos en la formulación de la denuncia
- 8.2 Medidas adicionales a la denuncia
- 8.3 Cuestionario: Formular una denuncia ante un ciberataque

9. Instituto nacional de ciberseguridad de España INCIBE

9.1 Qué es el INCIBE

9.2 A quienes ayuda el INCIBE

9.3 Cómo trabaja el INCIBE

9.4 Por qué es importante el INCIBE

9.5 Cuestionario: Instituto nacional de ciberseguridad

10. IA y Ciberseguridad

10.1 Introducción a IA y ciberseguridad

10.2 Sinergias entre IA y ciberseguridad

10.3 Cómo la IA esta transformando la ciberseguridad para las PYMES

10.4 Desafíos y consideraciones para las PYMES al implementar IA en ciberseguridad

10.5 Implementación de sistemas basados en IA

10.6 Ejemplos de éxito en la adopción de IA para ciberseguridad

10.7 Elección de proveedores de soluciones de IA en ciberseguridad adecuados para PYMES

10.8 Conclusión

10.9 Cuestionario: IA y Ciberseguridad

10.10 Cuestionario: Cuestionario final