Ciberseguridad: buenas prácticas.

Esta formación propone una introducción a la ciberseguridad en la empresa, donde se verán cuáles son las principales amenazas a las que hacen frente las empresas hoy en día, cómo deberían gestionar este riesgo independientemente de su tamaño y qué procesos y mecanismos de seguridad. deben implementarse para minimizar las probabilidades de sufrir un incidente de ciberseguridad.

La formación se centrará en los conceptos clave y proporcionarán ejemplos prácticos para mejorar la comprensión de los participantes. Además también se proporcionará material adicional, tales como recursos online y lecturas recomendadas, para que los estudiantes puedan profundizar en los temas tratados.

Hay que tener en cuenta que la ciberseguridad es un campo en constante evolución, por lo que es esencial fomentar la conciencia y el interés continuo de los participantes en la materia, animándolos a seguir aprendiendo y actualizándose sobre las últimas tendencias y las mejores prácticas en ciberseguridad.

Impartición: Jueves día 02/11/2023
Duración: 3 horas, de 09:00h a 12:00h
Modalidad: Aula Virtual (plataforma Zoom)
Formulario inscripción

Objetivos:

- Entender por qué la ciberseguridad en la empresa es un proceso continuo en el tiempo.
- Definir unas pautas de actuación en caso de situación de ciberataques.
- Identificar los principales riesgos y amenazas de ciberseguridad por la empresa.
- Conocer algunos aspectos básicos de políticas de seguridad de la información.
- Definición de buenas prácticas de seguridad informática.
- Fomentar la conciencia de la ciberseguridad en los participantes de la formación.
- Los alumnos estarán capacitados para aplicar las medidas de seguridad aprendidas tanto a nivel personal como profesional.

Programa:

1. Fundamentos de la ciberseguridad.
   - ¿Qué es la ciberseguridad?

- Vulnerabilidades y amenazas.
- Procedimientos y mecanismos de seguridad.

2. Amenazas y ataques cibernéticos
   - Tipo de ataques: malware, phishing, ransomware.
   - Ataques por denegación de servicio: casos y medidas básicas para prevenir y proteger
3. Protección de datos
   - Protección de datos personales y sensibles.
   - Buenas prácticas en seguridad de los datos y uso de contraseñas seguras.
   - Uso seguro de dispositivos y redes wi-fi.
   - Seguridad online y redes sociales.
4. Gestión de la ciberseguridad.
   - Estrategia de ciberseguridad.
   - Gestión del riesgo.
   - Políticas de ciberseguridad.
   - Normativas, estándares y regulaciones.