CIBERSEGURIDAD

Área: Informática
Modalidad: Presencial
Duración: 6 h
Precio: 78.00€

Curso Bonificable
Contactar
Recomendar
Matricularme

OBJETIVOS

Profundizar sobre los principales elementos de identificación, protección, detección, respuesta y recuperación ante una amenaza en ciberseguridad y alinear los recursos que ofrecen las tecnologías de la información con los objetivos del negocio o institucionales.

Conocer cómo proteger los datos sensibles frente a las amenazas que pueden materializarse por parte de nuestros adversarios.

Tener conocimiento de las principales herramientas, metodologías y servicios más adecuados para la gestión de proyectos de seguridad de la información.

CONTENIDOS

1.Introducción
1.1.4ª Revolución Industrial
IoT
5G
Cyber-Seguridad
Blockchain
Inteligencia Artificial
Ordenadores Cuánticos
2.¿Por qué es importante la Cyber-Seguridad?
2.1.Plan Director de Seguridad
Requisitos
Análisis del negocio y procesos de la empresa.
Identificación de las áreas sensibles o existencia de posibles vulnerabilidades (“Risk questionnaire”)
Procedimientos para la confirmación de las vulnerabilidades (“Penetration test”)
Establecimiento de estratégias de análisis y subsanación de las vulnerabilidades (“Risk Assessment”)
Implementación de políticas de mantenimiento y seguimiento de futuras evoluciones de seguridad (“Maintenance & Surveillance”)
Resultados
Política de Cyber-Seguridad para Alta Dirección
Política de Cyber-Seguridad para el Departamento de Seguridad (CISO)
Política de Cyber-Seguridad para los Trabajadores de la Organización
Política de Cyber-Seguridad a seguir por Terceros que colaboren con la Organización (Proveedores y Clientes)
Las 6 Fases del PDS
Conocer la situación actual
Conocer la estrategia de la organización
Definir proyectos e iniciativas
Procedimientos para la confirmación de las vulnerabilidades (“Penetration test”)

Establecimiento de estratégias de análisis y subsanación de las vulnerabilidades (“Risk Assessment”)
Implementación de políticas de mantenimiento y seguimiento de futuras evoluciones de seguridad (“Maintenance & Surveillance”)
Resultados
Política de Cyber-Seguridad para Alta Dirección
Política de Cyber-Seguridad para el Departamento de Seguridad (CISO)
Política de Cyber-Seguridad para los Trabajadores de la Organización
Política de Cyber-Seguridad a seguir por Terceros que colaboren con la Organización (Proveedores y Clientes)
Las 6 Fases del PDS
Conocer la situación actual
Conocer la estrategia de la organización
Definir proyectos e iniciativas
Clasificación y priorización
Aprobación por la dirección
Implantación del PDS
3.Ejemplos Prácticos
3.1.Enfoque técnico sobre:
APT detectar y mitigar
ZDA (Zero Day Attack) protección
Plataforma de aislamiento de Amenazas
Malware
Phishing
Real-Time Información forénsica
Ransomware (prevención)
DDOS simulación
Seguridad de Bases de Datos