CIBERSEGURIDAD PARA PROFESIONALES

Si quieres estar al día en temas de ciberseguridad, ¡este es tu curso! Fórmate en las áreas de gestión, organización, tecnología y sistemas.

BeJob

CIBERSEGURIDAD PARA PROFESIONALES

¡CONVIÉRTETE EN UN PROFESIONAL DE LA CIBERSEGURIDAD!

DURACIÓN: 30 HORAS

OBJETIVOS

- Realizar una aproximación a la importancia de la ciberseguridad en la empresa y conocer sus fundamentos.
- Analizar los riesgos reales y potenciales de Cibercrimen para cualquier tipo de organización.
- Entender el Reglamento General de Protección de Datos o GDPR y reconocer la figura del DPO, así como sus competencias y funciones.
- Aportar una visión desde la gestión empresarial y protección de datos.
- Realizar un análisis básico de la vulnerabilidad de la organización desde el punto de vista técnico y legal para garantizar la protección de la información.
- Conocer las medidas técnicas y organizativas necesarias para la protección de los activos utilizados para el tratamiento de datos personales.

TIPOLOGÍA

DURACIÓN: 30 horas

FORMATO: Online

«Dos de cada cinco gobiernos y compañías ampliarán sus equipos de seguridad en internet en más de un 15% dentro del próximo año, lo que llevará a la creación de 350.000 empleos en ciberseguridad en todo el continente en 2022».

ENCUESTA REALIZADA POR CENTRO PARA LA CIBERSEGURIDAD Y EDUCACIÓN (ISC)

CIBERSEGURIDAD PARA PROFESIONALES

CONTENIDOS

UNIDAD 1. CONTEXTO DE LA PROTECCIÓN DE DATOS Y LA CIBERSEGURIDAD

En este módulo se plantean los principales conceptos sobre ciberseguridad, se analiza la evolución del sector y se observa la aplicabilidad en diferentes aspectos tanto empresariales como domésticos.

UNIDAD 2. LEGISLACIÓN

GDPR, Infraestructuras crí ticas..., análisis de riesgos, económicos, análisis reputacional... Se analizarán, desde un punto de vista no técnico, los principales aspectos legales que todo profesional debe conocer para asegurarse el cumplimiento de las nuevas normãivas.

UNIDAD 3. ANÁLISIS DE LA SITUACIÓN: PRINCIPALES AMENAZAS Y SECTORES INVOLUCRADOS

Principales amenazas (DDoS, Ransonware...), organizaciones cibercriminales, etc.
Se planteará una visión general de la situación actual y se analizan algunos de los casos reales más comunes con el objẽivo de contextualizar el curso.

UNIDAD 4. HACKING ÉTICO

Técnicas, escáneres, vulnerabilidades, exploits, ataques de fuerza bruta, ingeniería inversa... Test de penetración, ingeniería social, análisis forense. En este módulo se analizan las diferentes técnicas de trabajo y servicios de los hackers éticos.

UNIDAD 5. HERRAMIENTAS DE DEFENSA. DISPOSITIVOS Y TÉCNICAS AVANZADAS

Dispositivos y herramientas: Firewalls, sandboxing, antivirus, antimalware, IDS, SIEM, DLP, IAM. Técnicas avanzadas: Machine Learning. Servicios de protección de datos SOC servicios en la nube.
Se explica, de manera muy divulgativa y sencilla el funcionamiento de diferentes herramientas y tecnologías para la ciberseguridad.

UNIDAD 6. LOS DATOS COMO ACTIVO VALIOSO

Técnicas de protección. Prevención de fugas de información. Los datos son el fundamento de la economía digital y cada vez más se trabaja de manera colaborativa con terceros, por tanto se necesita un enfoque muy específico a la hora de prevenir ataques, fugas de información, falseamiento, etc.

UNIDAD 7. AMENAZAS Y OPORTUNIDADES

Internet de las cosas, digitalización, nuevos dispositivos...
En este último módulo, los alumnos podrán conocer los retos que se presentan en ciberseguridad derivados de la aparición y consolidación de nuevas herramientas y dispositivos.

CIBERSEGURIDAD PARA PROFESIONALES

PROGRAMA

UNIDAD 1. CONTEXTO DE LA PROTECCIÓN DE DATOS Y LA CIBERSEGURIDAD

- Evolución, importancia e impacto de la ciberseguridad
- Conceptos
- Caso práctico. Wannacry

UNIDAD 2. LEGISLACIÓN

- Legislación europea: GDPR y Privacy Shield
- GDPR I: Ámbito objetivo y subjetido. Principios y derechos del interesado
- GDPR II: Responsables y encargados del tratamiento
- GDPR III: Autoridades de control y Comité Europeo de Protección de Datos
- GDPR IV: Recursos, responsabilidades y sanciones
- Armonización Internacional: transferencia de datos y Privacy Shield
- El DPO: responsabilidades y funciones

UNIDAD 3. ANÁLISIS DE LA SITUACIÓN: PRINCIPALES AMENAZAS Y SECTORES INVOLUCRADOS

- Gobiernos
- Sector Privado
- Organizaciones criminales
- Ciudadanos
- Inteligencia colectiva
- Análisis de riesgos
- Asegurar el riesgo

UNIDAD 4. HACKING ÉTICO

- Concepto
- Técnica I: Análisis de vulnerabilidades
- Técnica II: Ingeniería social
- Técnica III: Test de penetración y análisis forense
- Cómo opera un hacker ético

UNIDAD 5. HERRAMIENTAS DE DEFENSA. DISPOSITIVOS Y TÉCNICAS AVANZADAS

- Protección perimetral
- Protección del endpoint
- Sistemas avanzados de detección
- Servicios de protección SOC

UNIDAD 6. LOS DATOS COMO ACTIVO VALIOSO

- Importancia de los datos en la empresa
- La privacidad
- Protección de la fuga de datos

UNIDAD 7. AMENAZAS Y OPORTUNIDADES

- Nuevos retos: IoT y entornos de producción

APÚNTATE EN

WWW.BEJOB.COM

BeJob