Programa de Formación:

Ciberseguridad para Empresas

Duración:

25 horas

Formato:

Curso online sincrónico con sesiones en vivo, materiales de apoyo y ejercicios prácticos. Incluye estudios de caso, simulaciones y análisis de riesgos en entornos empresariales.

Estructura del Programa

Módulo 1: Fundamentos de Ciberseguridad y Marco Normativo

(4 horas)

Objetivos:

- Comprender los conceptos fundamentales de la ciberseguridad y su importancia en las empresas.
- Identificar las principales amenazas y vulnerabilidades en entornos empresariales.
- Conocer el marco legal y las normativas de seguridad aplicables a distintos sectores.

Contenidos:

- Introducción a la ciberseguridad: definición y alcance.
- Principales amenazas cibernéticas en empresas: malware, phishing, ransomware, ataques de denegación de servicio (DDoS).

- Principios de seguridad de la información: confidencialidad, integridad y disponibilidad (CIA).
- Normativas y estándares de seguridad:
    - ISO 27001 y sistemas de gestión de seguridad de la información (SGSI).
    - Reglamento General de Protección de Datos (GDPR).
    - Leyes locales de protección de datos y ciberseguridad.

Actividades:

- Análisis de casos reales de ciberataques y su impacto en empresas.
- Discusión sobre regulaciones y cumplimiento normativo en distintos sectores.

Módulo 2: Gestión de Riesgos y Seguridad en la Empresa

(5 horas)

Objetivos:

- Identificar y evaluar los riesgos de ciberseguridad en una organización.
- Aplicar metodologías para la gestión de riesgos y medidas preventivas.
- Desarrollar estrategias para la protección de la información empresarial.

Contenidos:

- Metodologías de gestión de riesgos en ciberseguridad (ISO 31000, NIST Cybersecurity Framework).
- Evaluación de vulnerabilidades en infraestructura y sistemas de la empresa.
- Medidas de seguridad en redes corporativas y entornos cloud.
- Políticas de seguridad de la información y concienciación en el personal.
- Desarrollo de un plan de respuesta a incidentes de ciberseguridad.

Actividades:

- Taller práctico de identificación y evaluación de riesgos en un entorno empresarial simulado.
- Diseño de una política de seguridad para una empresa ficticia.

Módulo 3: Protección de Redes, Sistemas y Datos

(6 horas)

Objetivos:

- Implementar medidas de protección en redes, dispositivos y aplicaciones empresariales.
- Aplicar estrategias de seguridad para la gestión de accesos y datos sensibles.
- Evaluar la efectividad de herramientas de monitoreo y detección de amenazas.

Contenidos:

- Seguridad en redes corporativas: segmentación, firewalls, VPN y detección de intrusos.
- Protección de servidores y sistemas operativos (Windows, Linux).
- Seguridad en entornos cloud y buenas prácticas para la gestión de datos.
- Control de acceso y autenticación segura (MFA, gestión de credenciales).
- Herramientas de monitoreo y respuesta ante amenazas (SIEM, IDS/IPS).

Actividades:

- Configuración básica de firewall y reglas de seguridad en un entorno de prueba.
- Simulación de un intento de acceso no autorizado y análisis de respuesta.

Módulo 4: Ciberseguridad para Usuarios y Concienciación Empresarial (5 horas)

Objetivos:

- Sensibilizar a los empleados sobre la importancia de la seguridad digital.
- Identificar los principales errores humanos que generan brechas de seguridad.

- Implementar programas de formación en ciberseguridad dentro de la empresa.

Contenidos:

- Ingeniería social y manipulación psicológica en ataques cibernéticos.
- Buenas prácticas en el uso de correos electrónicos y navegación segura.
- Gestión segura de contraseñas y autenticación en múltiples factores.
- Estrategias de formación y concienciación para empleados y directivos.

Actividades:

- Simulación de ataques de phishing y análisis de respuestas de los usuarios.
- Desarrollo de una campaña de concienciación en seguridad para empleados.

Módulo 5: Simulación de Incidentes y Estrategias de Respuesta

(5 horas)

Objetivos:

- Aplicar los conocimientos adquiridos en la gestión de un incidente de seguridad.
- Desarrollar un plan de respuesta y mitigación de ciberataques en la empresa.
- Evaluar la efectividad de los protocolos implementados.

Contenidos:

- Planificación y ejecución de simulaciones de ciberataques.
- Respuesta ante incidentes: comunicación, análisis y mitigación.
- Elaboración de informes post-incidente y medidas de mejora.

Actividades:

- Taller práctico: simulación de un ataque de ransomware en una empresa ficticia.
- Análisis de impacto y diseño de un plan de respuesta para minimizar daños.

Evaluación del Curso

- Pruebas de conocimiento en cada módulo con preguntas interactivas.
- Proyecto final donde los participantes diseñarán una estrategia de ciberseguridad para su empresa.
- Retroalimentación del instructor sobre el desempeño en ejercicios prácticos y simulaciones.

Herramientas y Recursos Digitales

- Plataformas para Clases en Vivo: Zoom, Microsoft Teams, Google Meet.
- Software Especializado:
    - Firewalls y herramientas de monitoreo de redes.
    - Simuladores de ataques de phishing y análisis de vulnerabilidades.
    - Herramientas de gestión de riesgos y cumplimiento normativo.
- Recursos Complementarios:
    - Documentación técnica y guías de mejores prácticas.
      Acceso a webinars y foros de discusión sobre ciberseguridad empresarial.
    - Casos de estudio y reportes de incidentes reales.

Este programa está diseñado para empresas de cualquier tamaño que deseen fortalecer su seguridad informática, reducir riesgos de ciberataques y fomentar una cultura organizacional de ciberseguridad.