CIBERSEGURIDAD EN LA EMPRESA

Código: 60166 **Duración:** 56h

Objetivos:

Objetivo General.
Capacitar a los participantes en ciberseguridad empresarial y normativas europeas y españolas para que puedan proteger activos digitales y manejar incidentes de seguridad, fomentando una cultura de seguridad en sus empresas.

Objetivos específicos.

1. Comprender los conceptos fundamentales de la ciberseguridad, incluyendo los riesgos asociados y las medidas de protección necesarias.
2. Familiarizarse con las tecnologías y herramientas de ciberseguridad, como antivirus, firewalls, encriptación y análisis forense, para implementar soluciones efectivas.
3. Dominar la creación de políticas de ciberseguridad, la gestión de incidentes y la evaluación de riesgos en el entorno empresarial.
4. Cumplir con las regulaciones y estándares de ciberseguridad en España y la Unión Europea, incluida la Directiva NIS2, garantizando el cumplimiento normativo en las organizaciones.
5. Estar preparado para abordar incidentes de seguridad, gestionar la notificación de estos eventos y contribuir a la promoción de una cultura de seguridad en el lugar de trabajo.

Contenidos:

UNIDAD 1. INTRODUCCIÓN A LA CIBERSEGURIDAD.

1.1. ¿Qué es la ciberseguridad?

1.1.1. La necesidad de la ciberseguridad.

1.1.2. Conceptos básicos.

1.2. Riesgos en materia de ciberseguridad.

1.2.1. Factores que propician los riesgos.

1.2.2. ¿De quién hay que protegerse?

1.3. Creación de una cultura de seguridad en la empresa.

1.3.1. Roles y responsabilidades en la seguridad de la información.

UNIDAD 2. TECNOLOGÍAS Y HERRAMIENTAS DE CIBERSEGURIDAD.

2.1. Antivirus y software de seguridad.

2.2. Firewalls y sistemas de detección de intrusiones (IDS).

2.3. Autenticación y gestión de contraseñas.

2.4. Encriptación y seguridad de datos.

2.4.1. La encriptación de datos y el RGPD.

2.5. Herramientas de análisis de seguridad y forenses.

2.5.1. Selección de herramienta de análisis forense digital.

UNIDAD 3. CIBERSEGURIDAD EMPRESARIAL Y MARCO NORMATIVO.

3.1. El desarrollo de políticas de ciberseguridad.

3.2. Planificación y respuesta ante incidentes de seguridad.

3.3. Evaluación de riesgos y gestión de la seguridad de información.

3.4. Cumplimiento de regulaciones y estándares de ciberseguridad.

3.5. Marco normativo en ciberseguridad.

3.5.1. La ciberseguridad en la UE.

3.5.2. Ciberseguridad en España.

3.5.3. Repercusiones del no cumplimiento de la legislación en España.

3.5.4. Ley Orgánica 10/1995, de 23 de noviembre, del Código Penal.

3.5.5. Ley Orgánica 5/2000, de 12 de enero, reguladora de la responsabilidad penal de los menores.

UNIDAD 4. ANTECEDENTES A LA DIRECTIVA NIS2.

4.1. Importancia de la ciberseguridad en la UE.

4.1.1. Análisis de las regulaciones en la UE

4.2. La directiva NIS1.

4.2.1. El Real Decreto-ley 12/2018 sobre seguridad de las redes y sistemas de información.

4.2.2. Real Decreto 43/2021.

4.3. La evolución de la Directiva NIS.

4.3.1. La influencia del COVID-19.

4.3.2. Los cambios clave de la Directiva NIS2.

UNIDAD 5. LA DIRECTIVA NIS2.

5.1. Objetivos de la NIS2.

5.2.Ámbito de aplicación.

5.2.1. Clasificación de los sectores: críticos y de alta criticidad.

5.2.2. Clasificación de Entidades: esenciales e importantes.

5.3. Instituciones asociadas a la Directiva NIS2.

5.4. Impacto de la Directiva.

5.4.1. Gestión de riesgos.

5.4.2. Mecanismos de intercambio de información.

5.5. Plazo de la notificación de incidentes.

5.6. Funciones y competencias de las autoridades competentes.

5.7. Régimen sancionador.

5.8. Próximos pasos.

UNIDAD 6. OTRAS REGULACIONES A NIVEL EUROPEO EN MATERIA DE SEGURIDAD.

6.1. Estrategia de Ciberseguridad Europea.

6.2. El Reglamento DORA.

6.3. La Directiva CER.

6.3.1. Mejores prácticas y pasos recomendados.

6.4. El Reglamento sobre Ciberseguridad y sus esquemas de certificación.

6.4.1. Relación con la Directiva NIS.

6.5. El futuro reglamento para la Ciberresiliencia.