Tecnológico de Monterrey | Educación Continua

DIPLOMADO DE ALTA ESPECIALIDAD

Estructura Funcional de Ciberseguridad en las Organizaciones

Objetivo

Desarrollarás las habilidades y competencias de ciberseguridad que te permitan llevar a cabo la gestión efectiva de riesgos del negocio vinculados a riesgos de tecnologías de información.

Beneficios del programa:

- Fortalecerás tus habilidades y capacidades de gestión y respuesta ante amenazas cibernéticas..
- Desarrollarás un conocimiento técnico y visión estratégica, serás capaz de integrar las decisiones de ciberseguridad a los intereses del negocio, administrando los riesgos de información y reduciendo su impacto en el mismo.

• Dirigido a:

> Director o miembro consolidado de un equipo de TI en una empresa, con ingeniería o licenciatura en TICs, con 3 años de experiencia.

Contenido del programa

El Diplomado de Alta Especialidad en Estructura Funcional de Ciberseguridad en las Organizaciones consta de **cuatro módulos**, que suman **96 horas** de aprendizaje en total. Cada módulo tiene 24 horas (12 horas presenciales y 12 horas de trabajo en línea).

Módulo 1. Rol y Estructuras Organizacionales del CISO (*chief information security officer*)

(12 horas presenciales + 12 horas en línea)

Objetivo:

1. Describir el papel de un CISO dentro de la empresa.

1.1. Detallar cómo funcionan las áreas específicas como el cumplimiento de la seguridad, la gobernanza y las operaciones, y cómo se relacionan entre sí.

2. Explicar el proceso de gobierno de la seguridad de TI.

2.1. Diseñar diferentes estructuras organizacionales, y por qué podría haber diferentes enfoques para diferentes organizaciones.

2.2. Describir cómo los desafíos de cumplimiento en diferentes entre diferentes industrias y países.

1. Definición.
2. Evolución del rol y las responsabilidades del CISO
3. Diferentes modelos de organización (pequeñas, medianas, grandes empresas)
4. Diferentes modelos para diferentes industrias
5. Diferentes modelos para diferentes regiones del mundo
6. Modelos para posicionar al CISO

Módulo 2. Estructura del Equipo de Trabajo del CISO

(12 horas presenciales + 12 horas en línea)

Objetivo:

3. Comprender los elementos necesarios para poder definir y establecer el equipo de trabajo del CISO.

3.1. Describir los puntos de referencia con los marcos de referencia de seguridad.

3.2. Discutir el potencial de los roles de ciberseguridad.

3.3. Desarrollar un catálogo de servicios de seguridad de TI.

3.4. Discutir la importancia de la privacidad dentro del programa.

1. Relación de un programa de ciberseguridad y los marcos de referencia
2. Roles de ciberseguridad
3. Dimensionamiento y diseño de equipos de trabajo
4. Uso del catálogo de servicios de seguridad de TI
5. Privacidad de datos

Módulo 3. Gestión de Riesgos de Ciberseguridad en el Negocio

(12 horas presenciales + 12 horas en línea)

Objetivo:

1. Identificar los riesgos y su impacto en las actividades el negocio.

4.1. Describir los diferentes motivos y enfoques para externalizar algunas o todas las operaciones de seguridad de TI.

5. Implementar gestión de riesgos de ciberseguridad en el negocio.

5.1. Discutir diferentes enfoques para la protección, detección, identificación de incidentes, respuesta y recuperación.

5.2. Describir cómo vincular los riesgos de TI con los riesgos del negocio.

1. Fundamentos de la gestión de riesgos empresariales
2. Gobernanza de riesgos de seguridad de TI
3. Relación del riesgo de TI con el riesgo del negocio
4. Riesgo de terceros
5. Conformidad de marcos de referencia
6. Desarrollo de un programa basado en riesgos empresariales

Módulo 4. Planeación e Implementación del Programa de Seguridad de TI

(12 horas presenciales + 12 horas en línea)

Objetivo:

6. Desarrollar un presupuesto de seguridad de TI.

6.1. Desarrollar un plan de capacitación y concientización para educar a los usuarios finales.

6.2. Analizar los puntos de referencia para el presupuesto de seguridad de TI.

6.3. Describir las diferentes áreas presupuestarias.

1. Estructura de gobierno y gestión
2. Educación y entrenamiento de la fuerza laboral
3. Puntos de referencia para el presupuesto de seguridad de TI
4. Diferentes áreas presupuestarias como personal, hardware, licencias, servicios, capacitación, asociaciones, etc.
5. Presupuesto operativo versus gasto de capital