FORMACIÓN E-LEARNING

Curso Online de

CISO (Chief Information Security Officer)

→ Para gestionar e implementar controles que garanticen la seguridad de los sistemas de información ante los delitos cibernéticos.

CURSO BONIFICABLE

Iniciativas Empresariales
estrategias de formación

MANAGER BUSINESS SCHOOL

Tel. 902 021 206 - attcliente@iniciativasempresariales.com
www.iniciativasempresariales.com

BARCELONA - BILBAO - MADRID - SEVILLA - VALENCIA - ZARAGOZA

Presentación

La evolución de la tecnología y su importancia en los procesos de negocio de cualquier organización la ha convertido en el centro de operaciones de las empresas actuales.
El rol del director de informática también ha cambiado, ahora es considerada una posición estratégica dentro de la empresa. Una de las responsabilidades que debe tomar es la de mantener la seguridad de los activos de nuestra empresa, un dato perdido, un informe confidencial que es capturado por un atacante, un servidor de comercio electrónico con una pérdida de rendimiento debido a un ataque informático, puede dejar a nuestra empresa en una posición débil frente a la competencia e incluso provocar una pérdida de negocio que ponga en peligro su continuidad.

En este curso vamos a profundizar en el conocimiento de la gestión de la seguridad de nuestra organización. Entenderemos quién es el CISO de una organización, qué funciones tiene y qué responsabilidades deberá asumir. Aprenderemos desde cómo gestionar la seguridad a través de todos los procesos de negocio hasta cómo podemos definir la seguridad física de nuestras instalaciones y su entorno.

Estudiaremos conceptos importantes en el día a día:

- Cómo gestionar los accesos a los activos.
- Qué es la criptografía y cómo ha evolucionado.
- Cómo defendernos de los ataques al control de acceso.
- Cómo diseñar una arquitectura de seguridad.

Todo ello nos permitirá tener al final una amplia visión del dominio de la seguridad corporativa.

La Educación On-line

Los cursos e-learning de Iniciativas Empresariales le permitirán:

- **La posibilidad de escoger el momento y lugar más adecuado.**
- **Interactuar con otros estudiantes enriqueciendo la diversidad de visiones y opiniones y su aplicación en situaciones reales.**
- **Trabajar con más y diversos recursos que ofrece el entorno on-line.**
- **Aumentar sus capacidades y competencias en el puesto de trabajo en base al estudio de los casos reales planteados en este curso.**

Tel. 902 021 206 - attcliente@iniciativasempresariales.com - www.iniciativasempresariales.com

Método de Enseñanza

El curso se realiza on-line a través de la plataforma *e-learning* de Iniciativas Empresariales que permite, si así lo desea, descargarse los módulos didácticos junto con los ejercicios prácticos de forma que pueda servirle posteriormente como un efectivo manual de consulta.
A cada alumno se le asignará un tutor que le apoyará y dará seguimiento durante el curso, así como un consultor especializado que atenderá y resolverá todas las consultas que pueda tener sobre el material docente.
El curso incluye:

Aula Virtual | Tutor personal | Flexibilidad de horarios | Pruebas de Autoevaluación

Contenido y Duración del Curso

El curso tiene una duración de 80 horas y el material didáctico consta de:

Manual de Estudio
Corresponde a todas las materias que se imparten a lo largo de los 9 módulos de formación práctica de que consta el curso CISO (Chief Information Security Officer).

Material Complementario
Incluye ejemplos, casos reales, tablas de soporte, etc. sobre la materia con el objetivo de ejemplificar y ofrecer recursos para la resolución de las problemáticas específicas en la gestión de la seguridad de nuestra empresa.

Ejercicios de Seguimiento
Corresponden a ejercicios donde se plantean y solucionan determinados casos referentes a la gestión de la seguridad de nuestra empresa.

Pruebas de Autoevaluación
Para la comprobación práctica de los conocimientos que Ud. va adquiriendo.

Curso Bonificable

Tel. 902 021 206 - attcliente@iniciativasempresariales.com - www.iniciativasempresariales.com

Este curso le permitirá saber y conocer:

- La importancia de la función del CISO. Cómo definir cuál es su rol en la organización y en el departamento de TI y cuáles son las responsabilidades que debe asumir.
- Cuál es el principal objetivo de la Seguridad de la Información.
- Cómo planificar, organizar y controlar la política de seguridad de la información de nuestra empresa.
- Cómo podemos proteger nuestros accesos. Qué modelos tenemos, cómo autenticarse de forma más segura y qué ataques podemos recibir.
- Cuál es el grado de vulnerabilidad de nuestra red.
- Qué entendemos por criptografía y cómo ha ido evolucionando.
- Qué problemas pueden ocasionar las tecnologías Wireless.
- Cómo gestionar los incidentes en las operaciones del día a día y cómo conseguir su continuidad.
- De qué métodos disponemos para proteger nuestro entorno físico y su perímetro, cómo debemos implantarlos.
- Cómo seleccionar las estrategias de recuperación de datos más adecuadas para nuestra empresa.
- Qué controles de prevención y evaluación de riesgos podemos realizar para conocer su alcance.
- Cuál es la normativa legal vigente en seguridad de la información.
- Cómo hacer frente a un delito informático y evitar así que pueda dañar la competitividad de nuestra empresa.
- Cómo se evalúan los riesgos de los sistemas en todos los niveles de acceso.
- Cómo crear y gestionar una política de seguridad TI con sus correspondientes controles físicos, administrativos y técnicos.
- Cómo realizar un plan de prevención de desastre informático y continuidad de negocio.

Para prevenir, hacer frente y solucionar ataques a su sistema informático.

Dirigido a:

Directores y Responsables de Departamentos de TI, Administradores de Sistemas y Redes, Auditores y Consultores de Seguridad de la Información, Responsables de Seguridad TI, Técnicos e Ingenieros de Informática y Telecomunicaciones y, en general, a todas las personas que estén involucradas en la seguridad informática de la empresa.

Tel. 902 021 206 - attcliente@iniciativasempresariales.com - www.iniciativasempresariales.com

Contenido del curso

→ MÓDULO 1. Gobierno de la seguridad de la información y gestión de riesgos

10 horas

La gestión de la seguridad de la información de nuestra empresa protege los activos de la organización mediante la implementación de controles de diferentes tipos. Un fallo en la protección de la información de nuestros activos puede llevarnos a pérdidas, destrucción o alteraciones inesperadas de su valor y, en consecuencia, el resultado puede ser una pérdida de productividad, reputación o pérdidas financieras.

1.1. Conceptos y principios:
1.1.1. Aplicación del gobierno de la seguridad de la información.
1.1.2. The CIA Traid: Confidencialidad, Integridad y Disponibilidad.
1.1.3. Otros conceptos de seguridad.

1.2. Clasificación de los datos:
1.2.1. Controles de clasificación.

1.3. Roles y responsabilidades.

1.4. Gestión del ciclo de vida de la información.

1.5. Políticas, estándares, guías y procedimientos:
1.5.1. Política de seguridad.
1.5.2. Estándares.
1.5.3. Puntos de referencia.
1.5.4. Guías.
1.5.5. Procedimientos.
1.5.6. Implementación.

1.6. Marco de referencia ISO27000.

1.7. Gestión de riesgos:
1.7.1. Política de gestión de riesgo en la información.
1.7.2. Evaluación y análisis de riesgos.
1.7.3. Identificar vulnerabilidades y amenazas.
1.7.4. Ejemplo de metodología de valoración de riesgos.
1.7.5. Aproximación al análisis de riesgos.

Tel. 902 021 206 - attcliente@iniciativasempresariales.com - www.iniciativasempresariales.com

Contenido del curso

→ MÓDULO 2. Control de acceso

10 horas

El control de acceso es el proceso de autorizar usuarios, programas u otros sistemas para observar, modificar o tener la posesión de un recurso de nuestro negocio. Nos protege de amenazas y mitigan las vulnerabilidades reduciendo la exposición a actividades no autorizadas.

2.1. Principios de seguridad:
2.1.1. Concepto de defensa en profundidad.

2.2. Identificación, autenticación, autorización:
2.2.1. Identificación y autenticación.
2.2.2. Gestión de identidades.
2.2.3. Biometría.
2.2.4. Contraseñas.
2.2.5. One-Time Password.
2.2.6. Autorización.

2.3. Tipos de control de acceso.

2.4. Técnicas de control de acceso.

2.5. Auditoría.

2.6. Monitorización:
2.6.1. Detección de intrusiones (IDS).
2.6.2. Sistema de prevención de intrusiones (IPS).

2.7. Ataques al control de acceso.

→ MÓDULO 3. Diseño y arquitectura de seguridad

8 horas

Crear y mantener una buena arquitectura de seguridad es una tarea difícil. El rol del arquitecto de seguridad es trasladar los requerimientos del negocio a soluciones que proporcionen seguridad a nuestros activos. Un diseño complicado de un sistema implicará que el arquitecto tenga la capacidad de entender todos los activos con el fin de protegerlos y cumplir las prioridades del equipo directivo.

3.1. Arquitectura del PC y el sistema operativo:
3.1.1. Procesadores.
3.1.2. Memoria y almacenamiento.

Tel. 902 021 206 - attcliente@iniciativasempresariales.com - www.iniciativasempresariales.com

Contenido del curso

3.1.3. Periféricos y otros dispositivos de entrada / salida.
3.1.4. Sistemas operativos.
3.1.5. ¿Cómo trabajan juntos?

3.2. Modelos de seguridad:
3.2.1. Trusted Computing Base.
3.2.2. State Machine Model.
3.2.3. Information Flow Model.
3.2.4. Noninterference Model.
3.2.5. Access Control Matrix.
3.2.6. Bell-LaPadula.
3.2.7. Biba.
3.2.8. Clar-Wilson.

3.3. Métodos seguros de operaciones:
3.3.1. Vulnerabilidades de las arquitecturas de seguridad.

3.4. Métodos de evaluación de sistemas:
3.4.1. The Orange Book.
3.4.2. The Red Book.

3.5. Seguridad IT:
3.5.1. Common Criteria.
3.5.2. Certificación y acreditación.
3.5.3. Sistemas abiertos y sistemas cerrados.

→ MÓDULO 4. Seguridad de red y telecomunicaciones

12 horas

4.1. Modelo OSI.

4.2. Modelo TCP / IP:
4.2.1. Protocolo IP.
4.2.2. Transmission Control Protocol (TCP).
4.2.3. User Datagram Protocol (UDP).
4.2.4. Dinamic Host Configuration Protocol (DHCP).
4.2.5. Internet Control Message Protocol (ICMP).
4.2.6. Internet Group Management Protocol (IGMP).
4.2.7. Routing Information Protocol (RIP).
4.2.8. Virtual Router Redundancy Protocol (VRRP).

Tel. 902 021 206 - attcliente@iniciativasempresariales.com - www.iniciativasempresariales.com

Contenido del curso

4.2.9. Remote Procedure Calls (RPC).
4.2.10. Simple Mail Transfer Protocol (SMTP) y Enhanced Simple Mail Transfer Protocol (ESMTP).
4.2.11. File Transfer Protocol (FTP).
4.2.12. Hypertext Transfer Protocol (HTTP).

4.3. Dispositivos de red:
4.3.1. Cortafuegos.
4.3.2. Canales de comunicación seguros.
4.3.3. Tunnelling.
4.3.4. TTL/SSL.
4.3.5. VLAN.
4.3.6. Remote access.
4.3.7. Remote access services.
4.3.8. Virtual applications and desktops.

4.4. Seguridad en los componentes de red.

4.5. Tecnologías Wireless:
4.5.1. Comunicaciones Wireless.
4.5.2. Ataques a la infraestructura WLAN.
4.5.3. Seguridad en la telefonía móvil.

4.6. Ataques a la red.

→ MÓDULO 5. Seguridad en las operaciones

12 horas

Las operaciones de seguridad son todas aquellas operaciones que implican la seguridad de las personas, las aplicaciones, el equipamiento y la globalidad del entorno. En este módulo conoceremos qué rol y responsabilidad tiene el departamento de seguridad y cómo se gestionan los incidentes.

5.1. El rol del departamento de operaciones:
5.1.1. Gestión administrativa.
5.1.2. Personal de seguridad y red.
5.1.3. Responsabilidad.
5.1.4. Niveles de corte.

5.2. Responsabilidades del departamento:
5.2.1. Ocurrencias no habituales o inexplicables.

Tel. 902 021 206 - attcliente@iniciativasempresariales.com - www.iniciativasempresariales.com

Contenido del curso

5.2.2. Desviaciones de los estándares.
5.2.3. Identificación y gestión de activos.
5.2.4. Controles de sistema.
5.2.5. Recuperación de confianza.
5.2.6. Preocupaciones de seguridad.
5.2.7. Controles de entrada y de salida.
5.2.8. Seguridad de acceso remoto.

5.3. Continuidad de las operaciones (SLA´S):
5.3.1. Tolerancia a errores.
5.3.2. Copias de seguridad.
5.3.3. Discos y almacenamiento de datos.

5.4. Gestión de la configuración y gestión del cambio:
5.4.1. Líneas de base.
5.4.2. Gestión del cambio.
5.4.3. Proceso de gestión del cambio.

5.5. Gestión de incidentes:
5.5.1. Mediciones de seguridad, métricas y reportes.
5.5.2. Gestión de las tecnologías de seguridad.
5.5.3. Controles de frontera.
5.5.4. Detección.
5.5.5. Sistemas anti-malware.
5.5.6. Gestión de los eventos de seguridad de información.
5.5.7. Respuesta.
5.5.8. Remedio y revisión.
5.5.9. Gestión de problemas.

5.6. Ejercicios de vulnerabilidad.

→ MÓDULO 6. Desarrollo seguro de software

8 horas

6.1 Gestión del ciclo de vida del desarrollo.

6.2. Modelos de desarrollo del software:
6.2.1. Build and Fix Model.
6.2.2. Waterfall Model.
6.2.3. V-Shaped Model (V-Model).

Tel. 902 021 206 - attcliente@iniciativasempresariales.com - www.iniciativasempresariales.com

Contenido del curso

6.2.4. Prototyping.
6.2.5. Modelo incremental.
6.2.6. Spiral Model.
6.2.7. Agile Model.

6.3. Bases de datos:
6.3.1. Arquitectura de los sistemas de gestión de Bases de Datos.
6.3.2. Bases de datos relacionales.
6.3.3. Transacciones de bases de datos.
6.3.4. Seguridad en bases de datos multinivel.
6.3.5. Otros mecanismos de seguridad.
6.3.6. ODBC.
6.3.7. Agregación.
6.3.8. Data mining.

6.4. Gestión del conocimiento.

6.5. Programación en tecnología orientada a objetos.

6.6. Mecanismos de protección del software.

→ MÓDULO 7. Criptografía

6 horas

La función principal de los sistemas de criptografía es convertir un mensaje escrito en texto plano a un mensaje cifrado mediante una serie de transposiciones o substituciones. En este módulo conoceremos la historia de la criptografía, qué tipos hay y cuáles son los principales ataques que se producen.

7.1. Historia de la criptografía.

7.2. Criptografía básica, conceptos de criptografía.

7.3. Criptografía moderna:
7.3.1. Algoritmos de clave simétrica.
7.3.2. Algoritmos de clave asimétrica.

7.4. Criptografía simétrica:
7.4.1. Data Encryption Standard (DES).
7.4.2. Triple DES.
7.4.3. International Data Encryption Algorithm (IDEA).
7.4.4. Blowfish.
7.4.5. AES (Advanced Encryption Standard).

Tel. 902 021 206 - attcliente@iniciativasempresariales.com - www.iniciativasempresariales.com

Contenido del curso

7.4.6. Gestión de clave simétrica.

7.5. Criptografía asimétrica:
7.5.1. Algoritmos asimétricos.
7.5.2. RSA.
7.5.3. Algoritmo de Diffie-Hellmann.
7.5.4. El Gamal.
7.5.5. Ventajas e inconvenientes de los algoritmos de claves asimétricas.

7.6. Funciones HASH:
7.6.1. Algoritmos Hash.
7.6.2. Ataques a algoritmos hash y códigos de autenticación de mensajes.

7.7. Ataques de criptografía.

7.8. Implementación de criptografía.

→ MÓDULO 8. Seguridad física y de entorno

4 horas

La defensa de perímetro nos ayuda a prevenir, detectar y corregir accesos físicos no autorizados. Este módulo nos ayudará a entender qué es la defensa del perímetro y cómo seleccionar, diseñar y configurar un centro de datos.

8.1. Defensa de perímetro.

8.2. Selección, diseño y configuración de sitio.

8.3. Sistemas de defensa.

8.4. Controles ambientales.

Contenido del curso

→ MÓDULO 9. Continuidad de negocio y recuperación de desastres

10 horas

Cuando pensamos en el Plan de Continuidad de Negocio no es suficiente con centrarnos en hacer copias de seguridad y comprar hardware redundante. Son conceptos muy importantes pero, a la vez, pequeñas piezas del conjunto de operaciones de la empresa. En este módulo veremos qué medidas preventivas hay que tomar para asegurar la continuidad de los procesos de TI y del negocio, así como estrategias del plan.

9.1. Plan de continuidad de negocio:
9.1.1. Integrar la Gestión del Plan de Continuidad en el Programa de Seguridad de la Empresa.
9.1.2. Política del Plan de Continuidad de Negocio.
9.1.3. Gestión del proyecto.

9.2. Plan de recuperación de desastres:
9.2.1. Documentar el plan.
9.2.2. Respuesta.
9.2.3. Activar el equipo.
9.2.4. Comunicación.
9.2.5. Valoraciones.
9.2.6. Restauración.

9.3. Medidas preventivas:
9.3.1. Medidas preventivas contra ataques.
9.3.2. Gestión de parches y vulnerabilidades.
9.3.3. Sistemas de gestión de vulnerabilidades.

9.4. Estrategias de recuperación:
9.4.1. Implementación de la estrategia de recuperación de datos.
9.4.2. Estrategias de recuperación de sitio.
9.4.3. Sitios móviles.
9.4.4. Acuerdos de proceso de datos.
9.4.5. Centros de proceso de datos múltiples.

9.5. Pruebas del plan:
9.5.1. Checklist.
9.5.2. Test de Llamada.
9.5.3. Structured Walk-Through Test.
9.5.4. Simulation Test.
9.5.5. Parallel test.
9.5.6. Interruption test.

Tel. 902 021 206 - attcliente@iniciativasempresariales.com - www.iniciativasempresariales.com

Autor

El contenido y las herramientas pedagógicas del curso CISO (Chief Information Security Officer) han sido elaboradas por un equipo de especialistas dirigidos por:

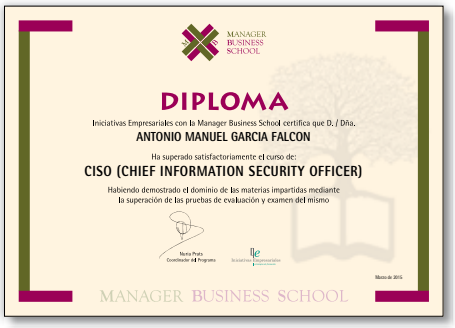
Xavier Vela

Ingeniero Técnico en Informática de Gestión por la Universidad Autónoma de Barcelona. Posgrado en Dirección de Sistemas de Información, Microsoft Certified Systems Administration, ITIL v3 Foundation, Prince2 Foundation, COBIT5 Foundation y Certified Information Systems Security Officer por Mile2.
Cuenta con más de 10 años de experiencia en departamentos de sistemas y soporte al usuario y está especializado en la gestión completa del centro de proceso de datos, la seguridad tecnológica de los activos informáticos de la empresa y el estudio e implementación de planes de contingencia y seguridad para las organizaciones.

El autor y su equipo de colaboradores estarán a disposición de los alumnos para resolver sus dudas y ayudarles en el seguimiento del curso y el logro de objetivos.

Titulación

Una vez realizado el curso el alumno recibirá el diploma que le acredita como **experto en CISO (Chief Information Security Officer).** Para ello, deberá haber realizado la totalidad de las pruebas de evaluación que constan en los diferentes apartados. Este sistema permite que los diplomas entregados por Iniciativas Empresariales y Manager Business School gocen de garantía y seriedad dentro del mundo empresarial.


MANAGER BUSINESS SCHOOL

DIPLOMA

Iniciativas Empresariales con la Manager Business School certifica que D. / Dña.

ANTONIO MANUEL GARCIA FALCON

Ha superado satisfactoriamente el curso de:

CISO (CHIEF INFORMATION SECURITY OFFICER)

Habiendo demostrado el dominio de las materias impartidas mediante la superación de las pruebas de evaluación y examen del mismo

MANAGER BUSINESS SCHOOL