CONTENIDOS

Experto Profesional
Ciberseguridad en Sistemas Ferroviarios

Fecha impartición: de junio a noviembre. **(15 ECTS)**

Metodología Aplicada: metodología de enseñanza programada e-learning a través del centro de formación virtual (CFV).

Técnicas utilizadas: ejercicios de autocomprobación y de autoevaluación además de la evaluación continua durante su impartición.

Se compone de 5 cursos online de diferente carga lectiva que suman un total de 350 horas:

- **Auditoría de seguridad**
- **Gestión de incidentes**
- **Informática forense**
- **Hacking ético**
- **Ciberseguridad avanzado**

Las 25 horas restantes corresponden al trabajo del alumno, evaluación y la tutorización.

CURSO: GESTIÓN DE INCIDENTES

Horas de dedicación: 70 horas

Nº de semanas para su realización 4

Objetivos: Capacitar a los participantes para tratar incidentes y recuperar los sistemas en infraestructuras críticas.

Contenidos:

1. Introducción a la respuesta a incidentes y su gestión proactiva.
2. Evaluación de riesgos.
3. Pasos en la respuesta y gestión de incidentes.
4. CSIRT.
5. Manejo de incidentes de seguridad de red.
6. Gestión de incidentes de código malicioso.
7. Gestión de las amenazas internas.
8. Análisis forense y respuesta a incidentes.
9. Informes de incidentes.
10. Recuperación ante incidentes.
11. Políticas de seguridad y legislación.

CURSO: CIBERSEGURIDAD AVANZADO

Horas de dedicación: 70 horas

Nº de semanas para su realización 4

Objetivos: Capacitar a los participantes para diseñar y desplegar políticas de seguridad para el aseguramiento de sistemas, detectar vulnerabilidades y establecer medidas para su corrección.

Contenidos:

1. Medición y evaluación de riesgos.
2. Monitorización y diagnóstico de redes.
3. Descripción de dispositivos e infraestructuras.
4. Controles de acceso, autenticación y autorización.
5. Protección de redes inalámbricas.
6. Securizando la nube.
7. Hosting, datos y seguridad de aplicaciones.
8. Criptografía.
9. Malware, vulnerabilidades y amenazas.
10. Ingeniería social y otros enemigos.
11. Gestión de seguridad.
12. La recuperación ante desastres y la respuesta a incidentes.

CURSO: INFORMÁTICA FORENSE

Horas de dedicación: 70 horas

Nº de semanas para su realización 4

Objetivos: Capacitar a los participantes para analizar y estudiar los incidentes para la identificación de los ataques y la implementación de medidas para la mejora de la seguridad.

Contenidos:

1. Informática forense en el mundo actual.
2. Proceso de investigación de informática forense.
3. Búsqueda e incautación de computadoras sin orden judicial.
4. La evidencia digital.
5. Procedimientos de primera respuesta.
6. Laboratorio de informática forense.
7. Descripción de los discos duros y sistemas de archivos.
8. Windows forensics.
9. Adquisición y duplicación de datos.
10. Recuperación de ficheros borrados y particiones eliminadas.
11. Investigaciones forenses empleando Accessdata ftk.
12. Investigaciones forenses empleando Encase.
13. Imágenes de archivos forenses y estenografía.
14. Aplicaciones para cracking de contraseñas.
15. Captura de registros y correlación de eventos.
16. Análisis forense de la red e investigación del tráfico de redes.
17. Investigación de ataques inalámbricos.
18. Investigación de los ataques a aplicaciones web.
19. Seguimiento de mensajes de email, investigación delitos de correo-e.
20. Mobile forensics. Informes de investigación. Testigo experto.

CURSO: AUDITORIA DE SEGURIDAD

Horas de dedicación: 70 horas

Nº de semanas para su realización 4

Objetivos: Capacitar a los participantes para auditar sistemas.

Contenidos:

1. Secretos de un auditor exitoso.
2. La gestión de la gobernanza de TI.
3. Proceso de auditoría.
4. Fundamentos de tecnología de redes.
5. Ciclo de vida de los sistemas de información.
6. Implementación de sistemas de información y operaciones.
7. Protección de activos de información.
8. Continuidad de negocio y recuperación ante desastres.

CURSO: HACKING ÉTICO

Horas de dedicación: 70 horas

Nº de semanas para su realización 4

Objetivos: Capacitar a los participantes para diseñar y desplegar políticas de seguridad para el aseguramiento de sistemas, detectar vulnerabilidades y establecer medidas para su corrección.

Contenidos:

1. Introducción al ethical hacking.
2. Footprinting y reconocimiento.
3. Escaneado de redes.
4. Enumeración.
5. Hacking de sistemas.
6. Troyanos y backdoors.
7. Virus y gusanos.
8. Sniffing.
9. Ingeniería social.
10. Denegación de servicio.
11. Secuestro de sesiones.
12. Hacking de servidores web.
13. Hacking de aplicaciones web.
14. Inyección sql.
15. Hacking de redes inalámbricas.
16. Hackeando plataformas móviles.
17. Eevasion de ids, firewalls, y honeypots.
18. Buffer overflow.
19. Criptografía.
20. Pruebas de penetración.