CONTENIDOS

Experto Profesional en Ciberseguridad en Redes Ferroviarias

Fecha impartición: de febrero a mayo. **(375 horas)**

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

Técnicas utilizadas: ejercicios de autocomprobación y de autoevaluación.

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

- **Redes corporativas**
- **Seguridad en redes inalámbricas**
- **Seguridad en redes físicas básico**
- **Seguridad en redes físicas avanzado**
- **Ciberseguridad industrial básico**

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

Certificación: La superación de cada curso de experto dará lugar a la obtención del correspondiente Diploma de Experto Profesional expedido por el Campus ADIF-FFE.

CURSO: REDES CORPORATIVAS

Horas de dedicación: 70 horas

Nº de semanas para su realización 4

Objetivos: Capacitar a los participantes para establecer medidas, planes de acción y resolver incidencias en redes corporativas, ferroviarias e infraestructuras críticas.

Contenidos:

1. Introducción a las redes de datos.
2. Clases de redes según su extensión y topología.
3. Tipos de comunicaciones.
4. Modelo OSI.
5. Redes de área local.
6. Elementos de una red de comunicaciones.
7. Integración de redes.
8. Estudio de los componentes de la arquitectura NGN.
9. Cableado y redes Ethernet.
10. Nivel físico: los medios de transmisión.
11. Tipos de cableado.
12. Suministro de energía.
13. Puentes transparentes y switches.
14. Tolerancia a fallos.
15. Redes locales virtuales: VLAN (virtual local area networks).
16. Direccionamiento IP.
17. Direcciones IP Clase A, B, C, D, E, reservadas y públicas.
18. Subredes y superredes IP. VLSM. Sumarización de rutas.
19. Escalabilidad y enrutamiento IP.

CURSO: SEGURIDAD EN REDES INALÁMBRICAS

Horas de dedicación: 70 horas

Nº de semanas para su realización 4

Objetivos: Capacitar a los participantes para implementar medidas de seguridad en redes cableadas e inalámbricas.

Contenidos:

1. Tecnologías Inalámbricas.
2. Introducción.
3. Principales tecnologías inalámbricas en la actualidad.
4. Componentes de las LAN inalámbricas.
5. Problemas asociados a las tecnologías inalámbricas.
6. Seguridad básica.
7. Seguridad inalámbrica de primera generación.
8. Configuración de seguridad inalámbrica básica en los dispositivos.
9. Wired Equivalent Privacy (WEP).

10. Autenticación de segunda generación. WPA - WPA2.
11. Estándar IEEE 802.11.
12. Arquitectura IEEE 802.11.
13. Topologías.
14. Especificaciones de la capa física del estándar 802.11.
15. Especificaciones MAC del estándar 802.11.
16. Control de Usuarios.
17. Modelo AAA.
18. RADIUS e IEEE 802.1x.
19. Protección del tráfico de usuario.
20. Vulnerabilidades y ataques en redes inalámbricas.
21. Seguridad en la red inalámbrica.
22. Vulnerabilidades.
23. Amenazas y ataques.
24. Gestión centralizada de redes inalámbricas.
25. Modelos de gestión centralizada.
26. Sistemas de gestión Centralizada.
27. Soluciones de gestión centralizada.

CURSO: SEGURIDAD EN REDES FÍSICAS BÁSICO

Horas de dedicación: 70 horas
Nº de semanas para su realización 4

Objetivos: Capacitar a los participantes para diseñar e implementar arquitecturas de red seguras.

Contenidos:

1. Fundamentos de la seguridad en red.
2. Modelo de red segura.
3. Amenazas de red: gusanos, virus y troyanos. Ataques de red.
4. Política de seguridad. Protección básica de la red.
5. Seguridad en dispositivos de red. Protocolos de red seguros.
6. Monitorización de dispositivos.
7. Control de usuarios. Modelo AAA. RADIUS.
8. Implementación del modelo AAA: TACACS+ y Freeradius.
9. Gestión de usuarios: integración con LDAP y Active Directory.
10. Seguridad en la LAN. Amenazas y vulnerabilidades en la LAN.
11. Seguridad en la capa 2. Control de Admisión (NAS).
12. Configuraciones de seguridad en protocolos LAN.
13. Monitorización de la LAN. Control de tráfico de red.
14. Tecnologías de Firewall.
15. Listas Control de Acceso (ACL).ProtocolInspection y ACL Dinámicas.
16. Tecnologías de IDS/IPS.
17. Filtrado de contenidos.

CURSO: SEGURIDAD EN REDES FÍSICAS AVANZADO

Horas de dedicación: 70 horas

Nº de semanas para su realización 4

Objetivos: Capacitar a los participantes para diseñ ar e implementar arquitecturas de red seguras.

Contenidos:

1. Fundamentos de la criptografía. Técnicas criptográficas.
2. Hash. Integridad y autenticación de datos.
3. Encriptación. Confidencialidad de la información.
4. Certificados digitales.
6. Infraestructura PKI.
7. Redes Privadas Virtuales (VPN). Fundamentos de VPN.
8. Protocolo VPN IPSec. VPN site-to-site.
9. Conexión de redes locales privadas a través de Internet.
10. VPN Server. Servicio VPN de acceso remoto.
11. Security Appliance (ASA).
12. Introducción a los dispositivos ASA.
13. Configuración básica de dispositivos ASA.
14. Configuración de VPN ASA.
15. Administración y Monitorización de seguridad red. Diseño red segura.
16. Protocolos de monitorización y gestión de la red.
17. Servicios de alarmas y sistemas de respuesta automática.
18. Auditoría de red. Herramientas de seguridad.
19. Seguridad ante fallos del sistema y desastres.
20. Desarrollo política de seguridad.

CURSO: CIBERSEGURIDAD INDUSTRIAL BÁSICO

Horas de dedicación: 70 horas

Nº de semanas para su realización 4

Objetivos: Capacitar a los participantes para diseñar e implementar arquitecturas de red seguras y resolver incidencias en redes ferroviarias e infraestructuras críticas.

Contenidos:

1. Introducción: Ciberseguridad, resiliencia, IoT, IACS.
2. Ciberseguridad Industrial y ciberesegurIdad IT.
3. Gestión de la ciberseguridad.
4. Arqutiecturas y seguridad en redes industriales.
5. Amenazas y ataques.
6. Medidas de defensa, respuesta y recuperación.
7. Evaluación y Auditoría de seguridad.
8. Infraestructuras críticas.