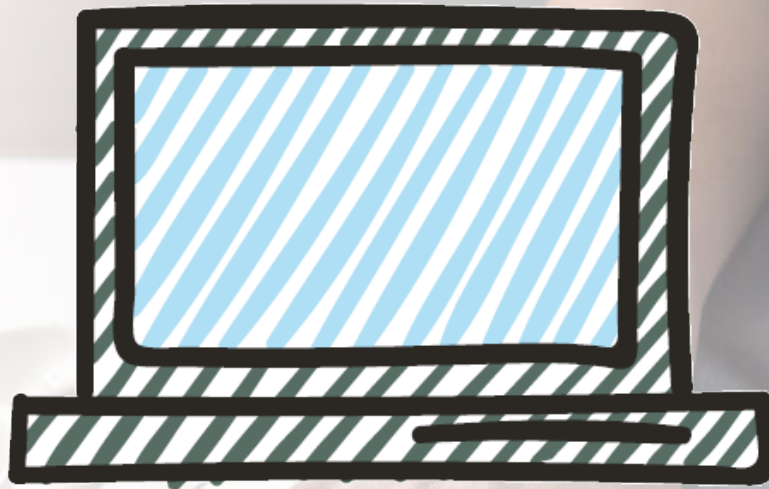


# Programa formativo

## INFORMÁTICA Y COMUNICACIONES



### Planificación de la seguridad informática en la empresa

**Duración: 80 horas**



**Grupo Glorieta**

Grupo Glorieta garantiza toda la formación impartida y la gestión de bonificaciones que realiza como entidad organizadora.

# Objetivos

- Planificación de la seguridad informática en la empresa. IFCTI01PO.
- Aprender conceptos y procedimientos generales relacionados con aquellos agentes externos que amenazan la seguridad informática de una empresa.
- Aprender todo lo relacionado con la planificación de seguridad informática de red en la empresa.
- Aprender las bases de las técnicas criptográficas más importantes de hoy y su utilidad en la vida real.
- Aprender los fundamentos sobre el proceso de autenticación en redes.
- Conocer en qué consiste una red virtual privada y como utilizarla para garantizar la seguridad de la información.
- Planificar la seguridad informática en la empresa.

# Contenidos

## **1. Debilidades, amenazas y ataques:**

- 1.1. Debilidades, amenazas y ataques.
- 1.2. Introducción.
- 1.3. Tipos de atacantes.
- 1.4. Motivaciones del atacante.
- 1.5. Metodología de un atacante determinado.
- 1.6. Vulnerabilidades y ataques comunes.
- 1.7. Herramientas de hacking.
- 1.8. Ingeniería social.
- 1.9. Prevención de ataques.
- 1.10. Respuesta a contingencias.
- 1.11. Contenidos prácticos.
- 1.12. Resumen.

## **2. Administración de la seguridad en redes:**

- 2.1. Introducción.
- 2.2. Diseño e implantación de políticas de seguridad.
- 2.3. Contenidos prácticos.
- 2.4. Resumen.

## **3. Tecnologías Criptográficas:**

- 3.1. Introducción.
- 3.2. Encriptación simétrica.
- 3.3. Encriptación asimétrica.
- 3.4. Firmas digitales.
- 3.5. Certificados digitales.
- 3.6. SSL/TLS. La herramienta de encriptación multiusos.
- 3.7. Navegación segura: HTTPS.
- 3.8. Contenidos prácticos.
- 3.9. Resumen.

## **4. Sistemas de autenticación:**

- 4.1. Introducción.
- 4.2. Tecnologías de Identificación.
- 4.3. PAP y CHAP.
- 4.4. RADIUS.
- 4.5. El protocolo 802.1X.
- 4.6. La suite de protocolos EAP: LEAP, PEAP, EAP-TLS.
- 4.7. Sistemas biométricos.
- 4.8. Contenidos prácticos.
- 4.9. Resumen.

## **5. Redes virtuales privadas:**

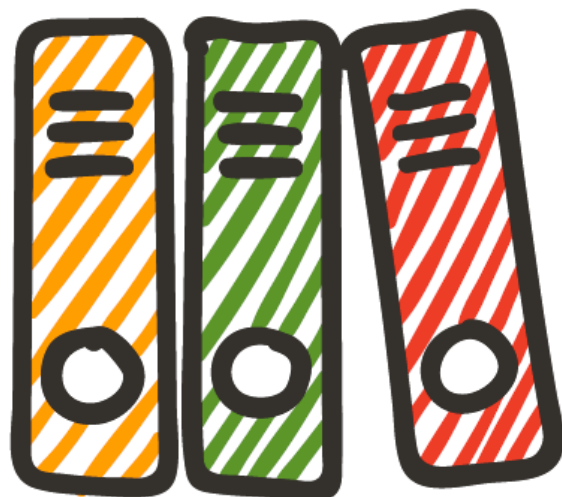
- 5.1. Introducción.
- 5.2. Beneficios y características.
- 5.3. IP Sec.
- 5.4. VPNs con SSL-TLS.
- 5.5. Contenidos prácticos.
- 5.6. Resumen.

## **6. Firewalls:**

- 6.1. Introducción.
- 6.2. Arquitectura de firewalls.
- 6.3. Filtrado de paquetes sin estados.
- 6.4. Servidores proxy.
- 6.5. Filtrado dinámico o "stateful".
- 6.6. Firewalls de siguiente generación.
- 6.7. Funciones avanzadas. Contenidos prácticos.
- 6.8. Contenidos prácticos.
- 6.9. Resumen.

## **7. Detección y prevención automatizada de intrusiones (IDS-IPS):**

- 7.1. Introducción.
- 7.2. Arquitectura de sistemas IDS.
- 7.3. Herramientas de software.
- 7.4. Captura de intrusos con honeypots.
- 7.5. Contenidos prácticos.
- 7.6. Resumen.



## **ACCESO AL CATÁLOGO GENERAL DE CURSOS**

Para más información:



**Grupo Glorieta**

**601 633 105**

**965 789 115**

[fcontinua@grupoglorieta.com](mailto:fcontinua@grupoglorieta.com)

[c.aloy@grupoglorieta.com](mailto:c.aloy@grupoglorieta.com)

[www.grupoglorieta.com](http://www.grupoglorieta.com)