

# LPIC-3 Enterprise Security

## Descrición

O curso LPIC-3: Security está deseñado para profesionais de TI que buscan dominar a administración avanzada de sistemas Linux cun enfoque especializado en seguridade, control de acceso, criptografía e protección de redes.

Durante a formación profundízase na configuración e auditoría de sistemas seguros, a detección de intrusións, a xestión de políticas de seguridade, o cifrado de datos e a protección de servizos críticos.

O contido cobre todos os obxectivos oficiais da certificación LPI 303 - Security, e combina teoría, demostracións e laboratorios prácticos orientados á defensa e endurecemento de contornos Linux en infraestruturas corporativas.

Este curso proporciona as competencias necesarias para deseñar, implementar e manter sistemas Linux altamente seguros e resilientes, adaptados aos estándares actuais de cumprimento e ás mellores prácticas do sector.

## Obxectivos

- Configurar e administrar mecanismos de criptografía simétrica, asimétrica e de clave pública (GPG, OpenSSL).
- Implementar sistemas seguros de autenticación, control de acceso e xestión de usuarios.
- Aplicar medidas de endurecemento do sistema operativo e servizos críticos.
- Configurar firewalls, VPNs e redes seguras utilizando iptables/nftables e ferramentas de cifrado de rede.
  - Protexer servizos como SSH, HTTP, DNS, correo e FTP fronte a ataques e vulnerabilidades.
  - Implementar sistemas de detección de intrusións (IDS) e realizar auditorías de seguridade.
  - Xestionar actualizacións, parches e automatización de medidas preventivas.
  - Asegurar contedores e contornos virtualizados.
  - Deseñar e executar plans de copia de seguridade e recuperación ante desastres.
  - Desenvolver e implementar políticas e documentación de seguridade corporativa.

## Dirixido a

O curso está dirixido a administradores/as de sistemas, enxeñeiros/as de seguridade e profesionais de TI con ampla experiencia en Linux que desexen especializarse na seguridade de sistemas e redes.

O perfil ideal inclúe profesionais que xa posúan a certificación LPIC-2 ou un nivel equivalente de coñecemento técnico, e que sexan responsables da protección, supervisión e cumprimento normativo de contornos Linux empresariais.

É especialmente axeitado para quen traballa en infraestruturas críticas, centros de datos, servizos cloud ou contornos mixtos, e busca elevar o nivel de seguridade, dispoñibilidade e confianza dos seus sistemas.

Recoméndase experiencia práctica en configuración de redes, servizos de sistema e administración avanzada de Linux.

### BENEFICIOS

Opción gratuita dun exame de certificación oficial

Diploma de asistencia

## Perfil do docente

Instrutor acreditado por LPI para a impartición do curso LPIC-3 Enterprise Security

### PROGRAMA

Programación 2025/26

### TIPO

CURSO

### MATRÍCULA

Gratuíta

### PERIODO INSCRICIÓN

15/06/2026 - 31/08/2026

### PROBA DE SELECCIÓN

01/09/2026 (18:30)

### CRITERIOS DE SELECCIÓN

Proba técnica presencial no CNTG en Santiago de Compostela

### Nº PRAZAS

20 (Mínimo 10)

### METODOLOXÍA

Virtual

## LPIC-3 Enterprise Security

<b>TIPO DE EDICIÓN</b>	Edición única (desempregados/as e ocupados/as)
<b>DURACIÓN</b>	48 horas
<b>DATA INICIO</b>	07/09/2026
<b>DATA FIN</b>	18/09/2026
<b>HORARIO</b>	De luns a xoves de 16:00 a 21:00 horas. Venres de 16:30 a 20:
<b>LUGAR DE DOCENCIA</b>	Edificio localizado na r/Airas Nunes s/n, barrio de Conxo, en
<b>CERTIFICACIÓN OFICIAL</b>	Sí
<b>EXAME CERTIFICACIÓN</b>	LPIC-3 303-200
<b>MÓDULOS TRANSVERSAIS</b>	Igualdade de 5 horas
<b>TECNOLOXÍA</b>	LPI
<b>PERIODO DOCENCIA</b>	07/09/2026 - 18/09/2026

## Temario

Módulo 1: Criptografía

Módulo 2: Control de acceso e autenticación

Módulo 3: Seguridade no sistema operativo Linux

Módulo 4: Seguridade na rede

Módulo 5: Protección de servizos de rede

Módulo 6: Detección de intrusións e auditoría

Módulo 7: Xestión de actualizacións e parches de seguridade

Módulo 8: Seguridade de aplicacións e contedores

Módulo 9: Copias de seguridade seguras e recuperación ante desastres

Módulo 10: Cumprimento, políticas e documentación de seguridade