Centro de Entrenamiento Autorizado PLATINO

TRAYECTORIA 27 AÑOS 1998 - 2025 CALIDAD COMPROMISO

DIPLOMADO INSTITUTO LINUX

LINUX SYSTEM SECURITY

LPIC-3 (303)

Certificación UTN-FRD + Linux Professional Institute (opcionales)

LPIC-3 ENTERPRISE PROFESSIONAL SECURITY

100% ONLINE

Linux Professional Institute · THE LINUX FOUNDATION · UTN FACULTAD REGIONAL DELTA · USP Universidade de São Paulo · LINUX INTERNATIONAL The Voice of Linux Users · LINUX ARGENTINA

ESTRUCTURA GENERAL DEL DIPLOMADO

MÓDULO 1:
Conceptos generales de seguridad y políticas

Clases 1 a 4

- Seguridad en capas
- Gestión de políticas de seguridad
- Gestión de riesgos y amenazas
- Normas y estándares (ISO 27001, CIS)

MÓDULO 2:
Control de acceso y autenticación

Clases 5 a 10

- Contraseñas seguras y políticas de cuenta
- PAM y autenticación basada en módulos
- LDAP y Kerberos
- Políticas de bloqueo, sudo y auditoría de acceso
- Control de sesiones y tiempos

MÓDULO 3:
Seguridad en red

Clases 11 a 16

- Principios de seguridad de red
- Firewall con iptables y nftables
- VPNs con OpenVPN y WireGuard
- Seguridad en servicios SSH, FTP, HTTP
- Detección de intrusiones (Snort, Suricata)

MÓDULO 4:
Criptografía y certificados

Clases 17 a 22

- Criptografía simétrica y asimétrica
- GPG, OpenSSL y gestión de claves
- Infraestructura de clave pública (PKI)
- Certificados digitales, CSR, CA
- SSL/TLS y configuración segura de servicios

MÓDULO 5:
Seguridad del sistema operativo

Clases 23 a 28

- Hardening de sistemas: servicios mínimos, usuarios, permisos
- Seguridad del bootloader (GRUB)
- Particiones seguras y montaje restringido
- Logs y rotación de registros
- Detección de rootkits y binarios comprometidos

MÓDULO 6:
Seguridad de aplicaciones y servicios

Clases 29 a 34

- Configuración segura de Apache, Nginx, Postfix
- Políticas de acceso por aplicación
- Análisis de vulnerabilidades
- Uso de herramientas como Lynis, OpenVAS
- Protección de bases de datos (MySQL/PostgreSQL)

MÓDULO 7:
SELinux y AppArmor

Clases 35 a 38

- Principios de control de acceso obligatorio (MAC)
- Implementación y monitoreo con SELinux
- Políticas, contextos y herramientas
- AppArmor: perfiles y modo de operación

MÓDULO 8:
Monitoreo, alertas y respuesta a incidentes

Clases 39 a 42

- Monitoreo con herramientas como Nagios, Zabbix
- Detección de comportamientos anómalos
- Gestión de alertas y notificaciones
- Procedimientos de respuesta ante incidentes

MÓDULO 9:
Cumplimiento, auditoría y forense básico

Clases 43 a 45

- Auditoría de seguridad en Linux
- Cumplimiento con normativas
- Introducción al análisis forense
- Preservación de evidencias

MÓDULO 10:
Preparación para el examen LPIC-3 (303 - Security)

Clases 46 a 48

- Revisión temática completa
- Simulacros de examen
- Estrategias de abordaje
- Cierre académico