



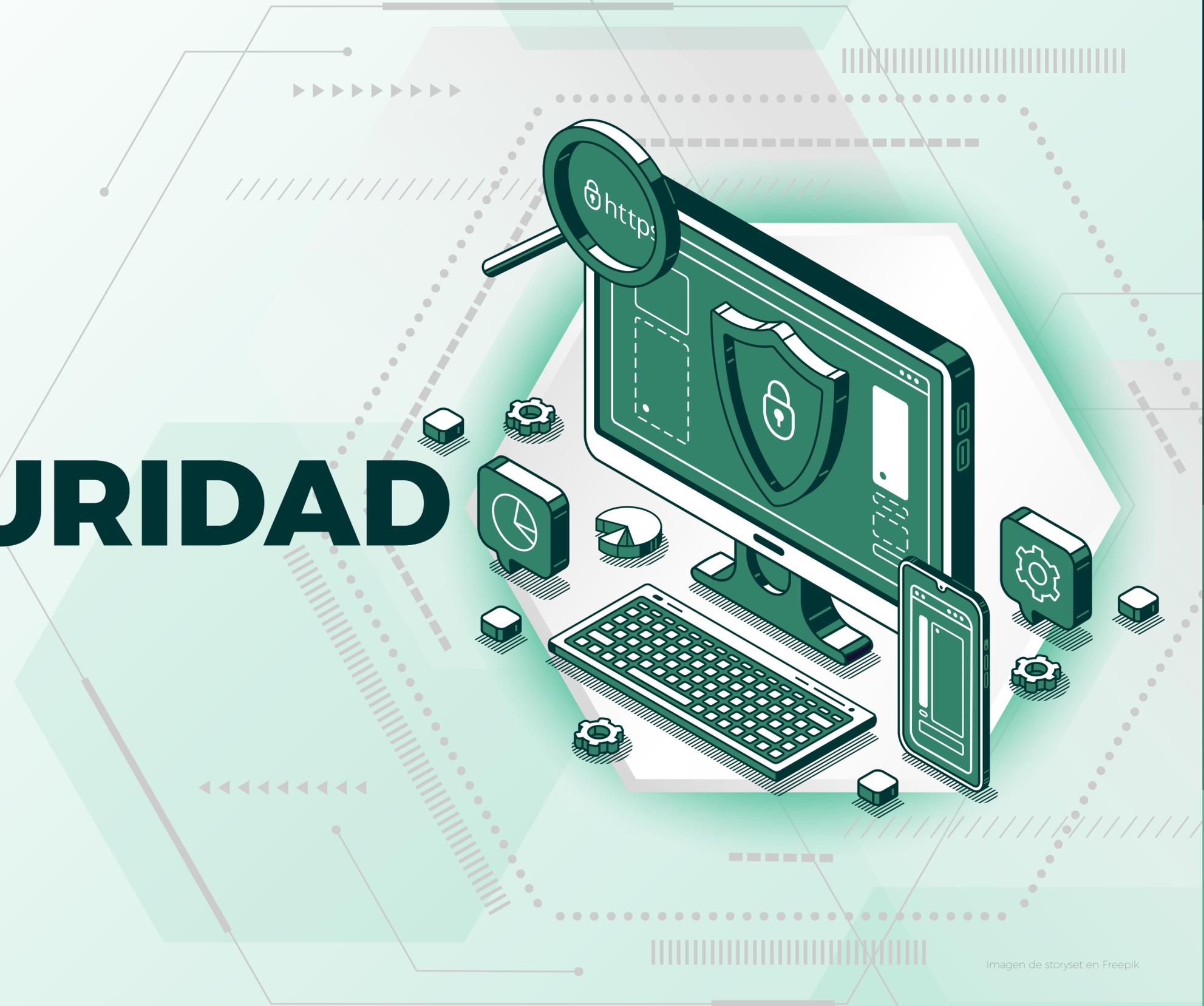
UTN FACULTAD
REGIONAL
DELTA

DIPLOMADO

CIBERSEGURIDAD

Certificación UTN-FRD

**100%
ONLINE**



DIPLOMADO

CIBERSEGURIDAD

Certificación UTN-FRD



¡Puedes hacerlo desde cualquier lugar del mundo, de manera sincrónica o asincrónica!

No requiere asistencia presencial.

Tendrás **acceso las 24 horas del día a la plataforma de capacitación y a las clases en vivo** sobre los diferentes temas.

El diplomado consta de **24 clases** de 2 horas c/u, **48 horas totales**,

CLASE 1

Introducción al Ethical Hacking

¿Qué es el “ethical hacking”?

Valores fundamentales.

Objetivos de la seguridad informática.

Análisis de riesgos.

Puesta en marcha de una política de seguridad.

CLASE 2

Footprinting

¿Qué saben los buscadores de nuestro objetivo?

Servicios Web de búsqueda de información de un dominio.

Obtener información de los DNS.

Fuzzing web.

CLASE 3

System Hacking

Windows System Hacking.

Contramedidas.

Linux System Hacking.

CLASE 4

Scanning & Enumeration

Funcionamiento de Nmap.

Como usar Nmap.

CLASE 5

SQL Injection

Trabajando con SQL Injection.

CLASE 6

Web Application Vulnerabilities

Vulnerabilidades en aplicaciones web.

Funcionamiento de w3af.

Vulnerabilidades OS Command.

CLASE 7

Honeypots

¿Qué es un honeypot?

Clasificación de honeypots.

Honeypots en producción.

Honeypots en desarrollo.

CLASE 8

Linux Hacking

¿Por qué atacar sistemas Linux?

Scanlogd. Abacus Portsentry.

Sniffit. John the Ripper.

CLASE 9

Criptografía

¿Cómo es el proceso de criptografía simétrica?
¿Cómo es el proceso de criptografía asimétrica?
Introducción a firma digital.
GPG (Gnu Privacy Guard).

CLASE 10

Criptografía II

Criptografía y seguridad en computadores.

CLASE 11

Virus, Troyanos y Backdoors

Virus informáticos y sistemas operativos.
Métodos de propagación
Métodos de protección y tipos
Troyanos Backdoor de acceso remoto, Planificación.

CLASE 12

Hacking Wireless Networks

Redes Inalámbricas. Suite “aircrack-ng”.
WEP (Wired Equivalent Privacy). WPA (Wi-Fi Protected Access).
PSK (Phase Shift Keying). TKIP (Temporal Key Integrity Protocol).
AES (Advanced Encryption Standard).

CLASE 13

IDS Evasion

Evasión de firewalls
Evasión de IDS.

CLASE 14

Host Intrusion Detection System

HIDS: Host Intrusion Detection System

CLASE 15

Network IDS

NIDS: Network Intrusion Detection System.
SNORT.
Modos de ejecución.

CLASE 16

Tripwire

Instalación
Iniciando tripwire.

CLASE 17

Ingeniería Social

Phishing.
Técnicas de phishing.
Variantes.

CLASE 18

Buffer Overflow

Buffer overflow.

Desarrollo de un exploit.

CLASE 19

Session Hijacking

Hijacking.

¿Qué es el secuestro de sesiones?

Pasos para secuestrar una sesión web.

CLASE 20

Sniffers

¿Qué es un snifer?

¿Cómo trabaja un snifer?

¿Cómo ocultar su presencia?

Instalar un snifer en modo no promiscuo.

CLASE 21

Sniffers II

Prácticas de sniffing.

CLASE 22

Pentesting y Metasploit

Definición de pentesting.

Normas y certificación.

Tipos de prueba.

Distribuciones de sistemas operativos especializados.

CLASE 23

DOS

Denegación de servicios.

Métodos de ataque.

CLASE 24

Web Server Security

Hacking Web Servers.

Ataques más comunes a los servidores web.

Cómo incrementar la seguridad en servidores web.

Herramientas para atacar servidores web.