

## Presentación del curso de “Experto en Ciberseguridad”



Un programa diseñado por un auditor de Ciberseguridad en Redes y Sistemas con +30 años de experiencia para que aprendas las **metodologías y herramientas que usan los expertos en el día a día.**

Para iniciar, asegúrate de *leer la presentación* y completar el registro.

**Objetivo:** Capacitar al alumno en un alto nivel de conocimientos sobre Ciberseguridad, empleando herramientas y metodologías actuales e imprescindibles en toda organización.

**Público al que va dirigido:** Personal con una buena base en Redes y Sistemas

**Horas lectivas:** 180 horas

**Metodología:** Implementación del curso basada en los contenidos publicados por Alejandro Corletti Estrada, por medio de sus libros, artículos y videos, que son uno de los referentes más importantes sobre Ciberseguridad en el ámbito hispano, contando a su vez con sus más de 30 años de experiencia como auditor y docente en esta temática.

Este es el tercer nivel de nuestro programa de cursos sobre **Ciberseguridad**. Lo recomendable, aunque no es mandatorio, es que comiences con el de “**Técnico en Ciberseguridad**”, continúes con el de “**Especialista en Ciberseguridad**” para luego realizar este de “**Experto en Ciberseguridad**”.

Para poder aprovechar este curso, es necesario que tengas una base sólida en Sistemas y redes. Sin la misma, te resultará muy complicada la comprensión de muchos de los conceptos y ejercicios que realizarás durante el curso.

Aquí encontrará el temario, ejercicios y herramientas o comandos sobre los que se trabajará a lo largo del curso. El contenido del curso se divide en un total de 10 Temas.

Cada uno de estos Temas esta restringido, de forma que solamente podrás acceder a él tras cumplimentar los tests del Tema anterior. En general los tests, verán que están asociados a nuestros videos, los cuáles no podrás adelantarlos y deberás verlos al completo.

### ¿Qué aprenderás?

- Identificar dispositivos de redes y sistemas

- Trabajar con Sistemas de Detección de Intrusiones y Firewalls
- Empleo de herramientas de detección de vulnerabilidades y phishing
- Cómo opera un Blue Team y un Red Team
- Implementar un SGSI en cualquier organización
- Marco regulatorio de MITRE
- Creación de procesos de ciberseguridad eficientes

## Este curso NO es gratuito

Si aún no te has registrado como Alumno, estás viendo únicamente las secciones habilitadas para "invitado". Con este perfil, no puedes acceder a todo el desarrollo, videos, ejercicios, ni test. Para que puedas evaluar algo del mismo, tienes acceso a los temas 1 y 2.

## Matricúlate ahora

Regístrate para obtener acceso completo al curso, incluidos videos, ejercicios y exámenes.



### Matriculación en el curso

Si deseas realizar este curso, debes registrarte en el mismo. El primer paso es "Crear una cuenta de usuario" (Registrarte en la plataforma), si es que aún no estás registrado. Una vez registrado, puedes matricularte en este curso.

Tienes dos formas de matriculación:

- **Individual:** Te auto matriculas por un importe de 120 € (pago por medio de Paypal).
- **Promoción x 3:** Se auto matricula 1 usuario, pagando un importe de 250 € (pago por medio de Paypal). Una vez matriculado, nos lo notifica por mail a [info@darfe.es](mailto:info@darfe.es), indicando la dirección de correo electrónico y el nombre de los otros dos usuarios, quienes en un par de días recibirán la matrícula activa en la dirección indicada.

### TEMAS

1. Fingerprinting
2. Footprinting

3. IDSs - Snort
4. Nessus
5. Firewalls
6. SGSI
7. Antiphishing
8. MITRE
9. Red Team y Blue Team
10. OSINT

## **Breve descripción de Temario**

### **1. Fingerprinting**

Se trata de los primeros pasos en el concepto de “enumeración” de redes y sistemas. La idea es que logres un primer reconocimiento de la infraestructura que deseas analizar para ir creando un mapa de situación de la misma, identificando direcciones IP, puertos y servicios.

### **2. Footprinting**

Es la continuación natural del tema anterior, pero ahora profundizando en el detalle de cada uno de los elementos identificados a través de fingerprinting. Ahora sí que comienza un trabajo detallado de identificación de debilidades y brechas de seguridad.

### **3. IDSs – Snort**

Estos dispositivos son los verdaderos ojos de la infraestructura de red y TI. Hoy en día son una pieza fundamental. El trabajo cotidiano con los mismos, requiere un especial ciclo de vida, mantenimiento, alarmas y reportes, para que sean de verdad eficientes.

### **4. Nessus**

Se trata de uno de los escáneres más potentes del mercado. Nació como Open Source, y en la actualidad lo comercializa la empresa **Tenable**, pero... aunque esta empresa no lo difunde mucho, o trata de difuminarlo: Existe una versión gratuita para investigación y estudio, que será la que emplearemos en este capítulo.

### **5. Firewalls**

Es otra de las herramientas que no puede faltar hoy en día en nuestras redes y sistemas. Su conocimiento y dominio es obligatorio para un “Especialista en Ciberseguridad”. En este capítulo, nos centraremos en “iptables” de Linux que, fue, es y seguirá siendo el motor de la mayoría de los productos comerciales, y su potencia te sorprenderá.

### **6. SGSI**

El Sistema de Gestión de la Seguridad de la Información (SGSI), es lo que nos propone la familia de normas ISO 27000. A lo largo de este capítulo, irás viendo cómo se compone la norma, y aprenderás a implantar un SGSI en cualquier tipo de organización.

### **7. Antiphishing**

Los ataques de phishing, son la puerta de entrada de más del 80 % de las intrusiones, también son la metodología más empleada para todo tipo de fraudes. Su mejor estrategia para combatirlos es la “concienciación”. Durante este tema, desarrollaremos en detalle cómo organizar, lanzar y medir el resultado de rigurosas campañas antiphishing por medio de la herramienta Open source “GoPhish”.

## **8. MITRE**

Se trata del marco más conocido de centralización mundial de vulnerabilidades. Es imprescindible que un experto esté familiarizado con el mismo. En este tema desarrollaremos con máximo detalle, todo lo que nos ofrece esta organización.

## **9. Red Team y Blue Team**

Hoy en día, es necesario saber cómo opera el enemigo y la propia tropa en el ataque y la defensa. Ese es el rol de estos dos equipos. Durante este capítulo presentaremos las metodologías y herramientas más comunes en ambos equipos.

## **10. OSINT**

En este tema comenzamos con OSINT (Open Source Intelligence). El objetivo principal es comprender desde la base, qué es OSINT, para qué sirve y por qué es una disciplina clave en la ciberseguridad moderna, antes de empezar a usar herramientas.

OSINT no consiste en "hackear" ni en realizar actividades intrusivas. Se basa exclusivamente en la recopilación, análisis y correlación de información disponible públicamente, pero aplicada con mentalidad analítica y objetivos claros.

.