



La asociación de seguridad ofensiva de Coruña presenta su nuevo curso gratuito de ciberseguridad 2025. Esta vez tendrá lugar en la ciudad de Ourense.

1. Objetivos

Formar a profesionales capaces de desempeñar labores relacionadas con el campo de la ciberseguridad sin que el criterio económico suponga una barrera. Este curso se imparte en estrecha colaboración con la asociación sin ánimo de lucro Ourensec.

Las sesiones se desarrollarán de forma presencial en la sede de Ourensec situada en **Calle Cervantes, 5 bajo, 32005 Ourense**. Y tendrán lugar desde la segunda semana de Septiembre de 2025 hasta

2. Formato

3 sesiones semanales de entre 1 y 2 horas durante 12 semanas con posibilidad de realizar sesiones extraordinarias de forma telemática. Cada semana se dividirá en una o dos sesiones expositivas y una sesión práctica en la que se realizarán los ejercicios propuestos. Por tanto la duración total del curso será de (aproximadamente) 54 horas.

Llegada la mitad del curso los alumnos comenzarán a realizar un proyecto de libre elección que deberán exponer durante la última semana. Este proyecto será evaluado por un jurado, obteniendo el mejor resultado un premio simbólico.

Todos los alumnos que presenten con éxito el proyecto y hayan demostrado haber participado durante las sesiones obtendrán un certificado de aprovechamiento y podrán optar a ofertas laborales si las hubiera.

Además durante el curso se realizarán sesiones específicas para mejorar en habilidades blandas: Expresión oral, elaboración de CV, uso de LLMs, entrevistas, etc.

En tanto a la docencia, seguiremos el modelo clásico de la ASOC que trata de desdibujar la línea entre alumno y profesor fomentando la participación y la competición.

3. Público objetivo e inscripción

El curso va dirigido a todo aquel que tenga interés en la ciberseguridad, si bien no existen requisitos previos, en ningún caso se trata de un curso básico, por lo que se recomienda haber cursado o estar cursando estudios en materias relacionadas con la informática, telecomunicaciones o electrónica.

Por motivos legales, **no se aceptarán inscripciones de personas menores de 18 años.**

Para consultas relativas a las inscripciones o al curso en general, podéis contactar con el equipo de Ourensec o con la ASOC:

Contacto Ourensec:

- +34 664184254
- info@ourensec.org

Contacto ASOC:

- xabiglesias11@gmail.com

Las inscripciones se abrirán durante el mes de Agosto y permanecerán activas hasta la segunda quincena de Septiembre.

4. Calendario propuesto

En principio, todas las sesiones se presuponen entre los días Martes, Miércoles y Jueves de 19:30 a 21:30. Sin embargo, es posible que por circunstancias varias estas se desplacen. Cualquier cambio será notificado en un grupo de difusión.

Módulo 1.

S1 - 9,10,11 de Septiembre (19:30-21:30)

S2 - 16,17,18 de Septiembre (19:30-21:30)

S3 - 23,24,25 de Septiembre (19:30-21:30)

S4 - 30,01,02 de Octubre (19:30-21:30)

S5 - 07,08,09 de Octubre (19:30-21:30)

Módulo 2.

S6 - 14,15,16 de Octubre (19:30-21:30)

S7 - 21,22,23 de Octubre (19:30-21:30)

S8 - 28,29,30 de Octubre (19:30-21:30)

Módulo 3.

S9 - 04,05,06 de Noviembre (19:30-21:30)

S10 - 12,13 de Noviembre (19:30-21:30) (2 días)

Módulo 4.

S11 - 18,19,20 de Noviembre (19:30-21:30)

Módulo 5.

S12 - 25,26,27 de Noviembre (19:30-21:30)

5. Contenidos

Módulo 1: Introducción y fundamentos

Semana 1. Electrónica

- El átomo, la capa de valencia, semiconductores y unión PN
- El transistor y las puertas lógicas
- Circuitos electrónicos, flip flops, la máquina de turing
- Ejercicio propuesto: Simulador de una máquina de turing

Semana 2. Hardware

- Historia y terminología
- Memoria, caché y modos de direccionamiento
- El procesador segmentado y el especulador
- Extra: Ataques de canal paralelo, spectre y meltdown
- Gestión de la periferia, interrupciones y DMA
- Introducción al lenguaje ensamblador
- Ejercicio propuesto: Diseño de una microarquitectura

Semana 3. Sistemas operativos

- Introducción, historia y terminología
- El cargador de arranque
- Introducción a la programación en C
- Memoria virtual
- Procesos
- Sistema de ficheros
- IPC e IO
- Ejercicio propuesto: Programación de un microkernel

Semana 4. Ejecutables y contramedidas

- El formato ELF
- Proceso de carga de un ejecutable en memoria
- Introducción a los ataques de overflow
- Contramedidas
- Fundamentos de ingeniería inversa
- Ejercicio propuesto: Carga dinámica de un binario

Semana 5. Pwning

- Stack overflow
- Format string
- Return2libc
- UAF, Heap overflow y heap grooming
- Return oriented programming y SROP
- Programación de exploits y shellcode
- Ejercicio propuesto: CTF de pwning

Módulo 2: Pentesting

Semana 6. Análisis de vectores de entrada

- Introducción al pentesting: Documentación, aspectos éticos y legales
- Escaneo de puertos
- Análisis de vulnerabilidades
- Inteligencia de fuentes abiertas
- Ejercicio propuesto: Máquina HTB

Semana 7. Intrusión

- Hacking web
- Hacking en redes de área local e inalámbricas
- Ingeniería social
- Pentesting físico
- Ejercicio propuesto: Máquina HTB

Semana 8. Post-explotación

- Introducción a Active Directory
- Movimiento lateral
- Persistencia
- Ocultación
- Ejercicio propuesto: Que te pillo

Módulo 3: Respuesta ante incidentes

Semana 9. Diseño y análisis de malware

- Programación de malware
- Técnicas de análisis estático y dinámico
- Comunicaciones encubiertas, cifrado y evasión de AVs
- Ejercicio propuesto: Programación de malware y posterior análisis

Semana 10. Introducción al DFIR

- Fundamentos legales y conceptos clave
- Adquisición de evidencias
- Análisis sobre volcados de disco
- Análisis sobre volcados de memoria volátil
- Introducción al CTI y a la recuperación de información
- Ejercicio propuesto: Análisis de incidente real

Módulo 4: Gestión de la ciberseguridad

Semana 11. Introducción a la gestión de la ciberseguridad

- El papel del CISO en la empresa
- Introducción a la gestión de proyectos
- Documentación necesaria
- Implantando un stack de ciberseguridad
- Respuesta ante incidentes
- Ejercicio propuesto: Elaboración de un SGSI

Módulo 5. Taller de proyectos

Semana 12.

- Exposición de proyectos
- Fiesta de despedida, entrega de premios y diplomas

6. Otros seminarios

1. Debate y expresión oral
2. Introducción al hardware hacking
3. Creación de CV
4. Ataques de canal paralelo
5. Programación paralela
6. Uso de LLMs
7. Entrevistas de trabajo
8. Seminarios impartidos por alumnos