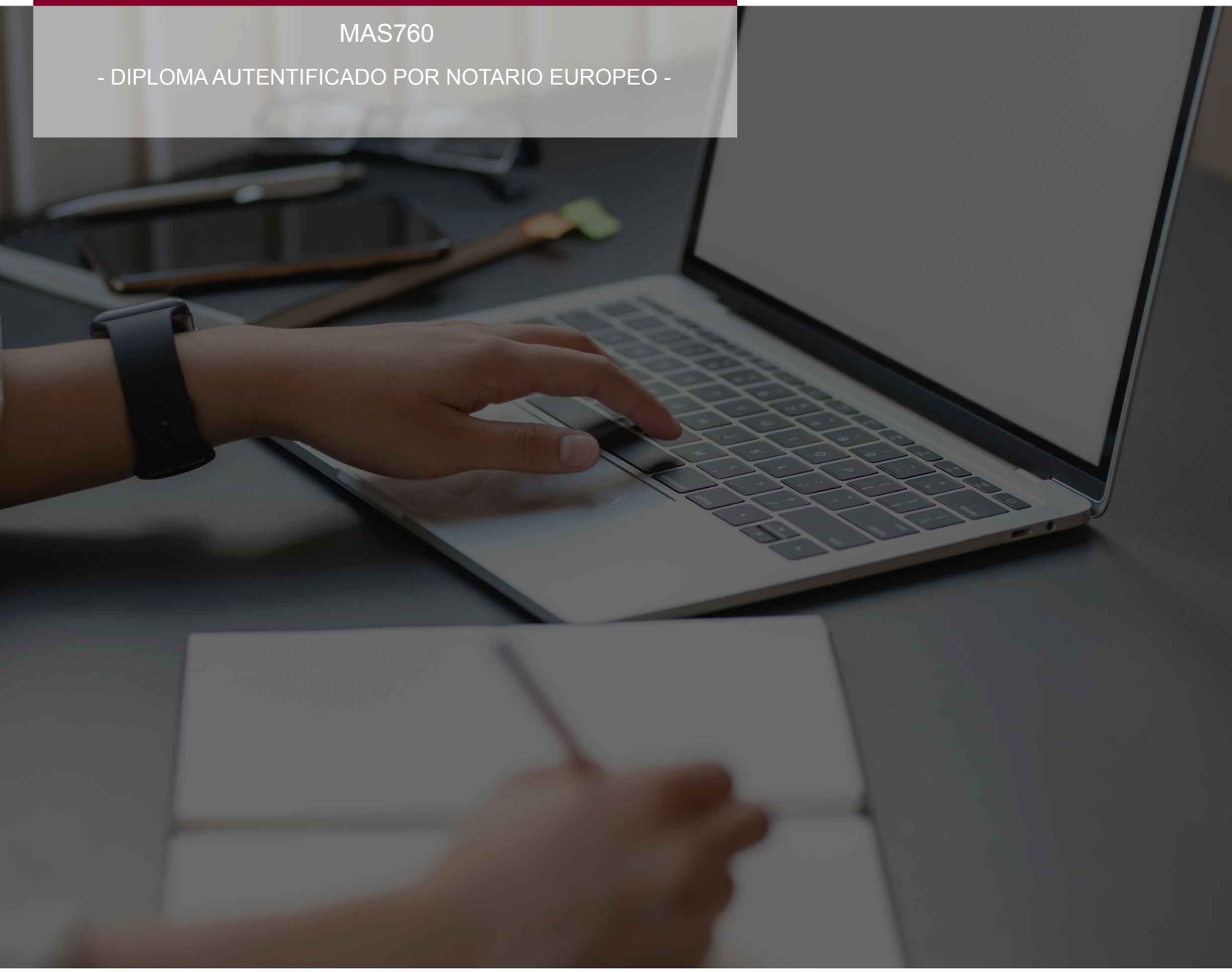
MÁSTER

MÁSTER EN SEGURIDAD INFORMÁTICA EN EL ÁMBITO EMPRESARIAL

esneca BUSINESS SCHOOL

MAS760

- DIPLOMA AUTENTIFICADO POR NOTARIO EUROPEO -



CUM LAUDE

aeen asociación española de escuelas de negocios

CECAP

DESTINATARIOS

El **Máster en Seguridad Informática en el Ámbito Empresarial** está destinado a todas aquellas personas que pretendan adquirir todos los conocimientos necesarios en este ámbito profesional y poder desarrollarlos de forma eficiente en el mundo laboral.

Permite conocer la introducción a la seguridad, las políticas de seguridad, la auditoria y normativa de seguridad, las estrategias de seguridad, la exploración de las redes, los ataques remotos y locales, la seguridad en las redes inalámbricas, la criptografía y criptoanálisis, la autenticación, la validación de identificación en las redes y la clasificación de los ataques, entre otros conceptos relacionados. Además, al final de cada unidad didáctica el alumno/a encontrará ejercicios de autoevaluación, que le permitirá hacer una seguimiento autónomo sobre los conocimientos adquiridos a lo largo del estudio.

El alumno recibirá acceso a un curso inicial donde encontrará información sobre la metodología de aprendizaje, la titulación que recibirá, el funcionamiento del Campus Virtual, qué hacer una vez el alumno haya finalizado e información sobre Grupo Esneca Formación. Además, el alumno dispondrá de un servicio de **clases en directo**.

FICHA TÉCNICA

CARGA HORARIA
600H

MODALIDAD
ONLINE
*La modalidad incluye módulos con clases en directo

CURSO INICIAL
ONLINE

TUTORIAS
PERSONALIZADAS

IDIOMA
CASTELLANO

DURACIÓN
HASTA UN AÑO
*Prorrogable

IMPORTE

VALOR ORIGINAL: ~~2380€~~
VALOR ACTUAL: 595€

CERTIFICACIÓN OBTENIDA

Una vez finalizados los estudios y superadas las pruebas de evaluación, el alumno recibirá un diploma que certifica el "**MÁSTER EN SEGURIDAD INFORMÁTICA EN EL ÁMBITO EMPRESARIAL**", de ESNECA BUSINESS SCHOOL, avalada por nuestra condición de socios de la CECAP y AEEN, máximas instituciones españolas en formación y de calidad.

Los diplomas, además, llevan el sello de Notario Europeo, que da fe de la validez, contenidos y autenticidad del título a nivel nacional e internacional.

REDES SOCIALES

www.facebook.com/esnecaschool

linkedin.com/school/esneca-business-school

@esneca.business.school

www.esneca.com

www.twitter.com/ESNECA

www.esneca.com/blog

CONTENIDO FORMATIVO

UNIDAD DIDÁCTICA 1. INTRODUCCIÓN A LA SEGURIDAD

1. Introducción a la seguridad de información.
2. Modelo de ciclo de vida de la seguridad de la información.
3. Confidencialidad, integridad y disponibilidad. Principios de protección de la seguridad de la información.
4. Políticas de seguridad.
5. Tácticas de ataque.
6. Concepto de hacking.
7. Árbol de ataque.
8. Lista de amenazas para la seguridad de la información.
9. Vulnerabilidades.
10. Vulnerabilidades en sistemas Windows.
11. Vulnerabilidades en aplicaciones multiplataforma.
12. Vulnerabilidades en sistemas Unix y Mac OS.
13. Buenas prácticas y salvaguardas para la seguridad de la red.
14. Recomendaciones para la seguridad de su red.

UNIDAD DIDÁCTICA 2. POLÍTICAS DE SEGURIDAD.

1. Introducción a las políticas de seguridad.
2. ¿Por qué son importantes las políticas?
3. Qué debe de contener una política de seguridad.
4. Lo que no debe contener una política de seguridad.
5. Cómo conformar una política de seguridad informática.
6. Hacer que se cumplan las decisiones sobre estrategia y políticas.

UNIDAD DIDÁCTICA 3. AUDITORIA Y NORMATIVA DE SEGURIDAD.

1. Introducción a la auditoría de seguridad de la información y a los sistemas de gestión de seguridad de la información.
2. Ciclo del sistema de gestión de seguridad de la información.
3. Seguridad de la información.
4. Definiciones y clasificación de los activos.
5. Seguridad humana, seguridad física y del entorno.
6. Gestión de comunicaciones y operaciones.
7. Control de accesos.
8. Gestión de continuidad del negocio.
9. Conformidad y legalidad.

UNIDAD DIDÁCTICA 4. ESTRATEGIAS DE SEGURIDAD.

1. Menor privilegio.
2. Defensa en profundidad.
3. Punto de choque.
4. El eslabón más débil.
5. Postura de fallo seguro.
6. Postura de negación establecida: lo que no está prohibido.
7. Postura de permiso establecido: lo que no está permitido.
8. Participación universal.
9. Diversificación de la defensa.
10. Simplicidad.

UNIDAD DIDÁCTICA 5. EXPLORACIÓN DE LAS REDES.

1. Exploración de la red.
2. Inventario de una red. Herramientas del reconocimiento.
3. NMAP Y SCANLINE.
4. Reconocimiento. Limitar y explorar.
5. Reconocimiento. Exploración.
6. Reconocimiento. Enumerar.

UNIDAD DIDÁCTICA 6. ATAQUES REMOTOS Y LOCALES.

1. Clasificación de los ataques.
2. Ataques remotos en UNIX.
3. Ataques remotos sobre servicios inseguros en UNIX.
4. Ataques locales en UNIX.
5. ¿Qué hacer si recibimos un ataque?

UNIDAD DIDÁCTICA 7. SEGURIDAD EN REDES ILANÁMBRICAS

1. Introducción.
2. Introducción al estándar inalámbrico 802.11 - WIFI
3. Topologías.
4. Seguridad en redes Wireless. Redes abiertas.
5. WEP.
6. WEP. Ataques.
7. Otros mecanismos de cifrado.

UNIDAD DIDÁCTICA 8. CRIPTOGRAFÍA Y CRIPTOANÁLISIS.

1. Criptografía y criptoanálisis: introducción y definición.
2. Cifrado y descifrado.
3. Ejemplo de cifrado: relleno de una sola vez y criptografía clásica.
4. Ejemplo de cifrado: criptografía moderna.
5. Comentarios sobre claves públicas y privadas: sesiones.

UNIDAD DIDÁCTICA 9. AUTENTICACIÓN.

1. Validación de identificación en redes.
2. Validación de identificación en redes: métodos de autenticación.
3. Validación de identificación basada en clave secreta compartida: protocolo.
4. Establecimiento de una clave compartida: intercambio de claves Diffie-Hellman.
5. Validación de identificación usando un centro de distribución de claves.
6. Protocolo de autenticación Kerberos.
7. Validación de identificación de clave pública.
8. Validación de identificación de clave pública: protocolo de interbloqueo.