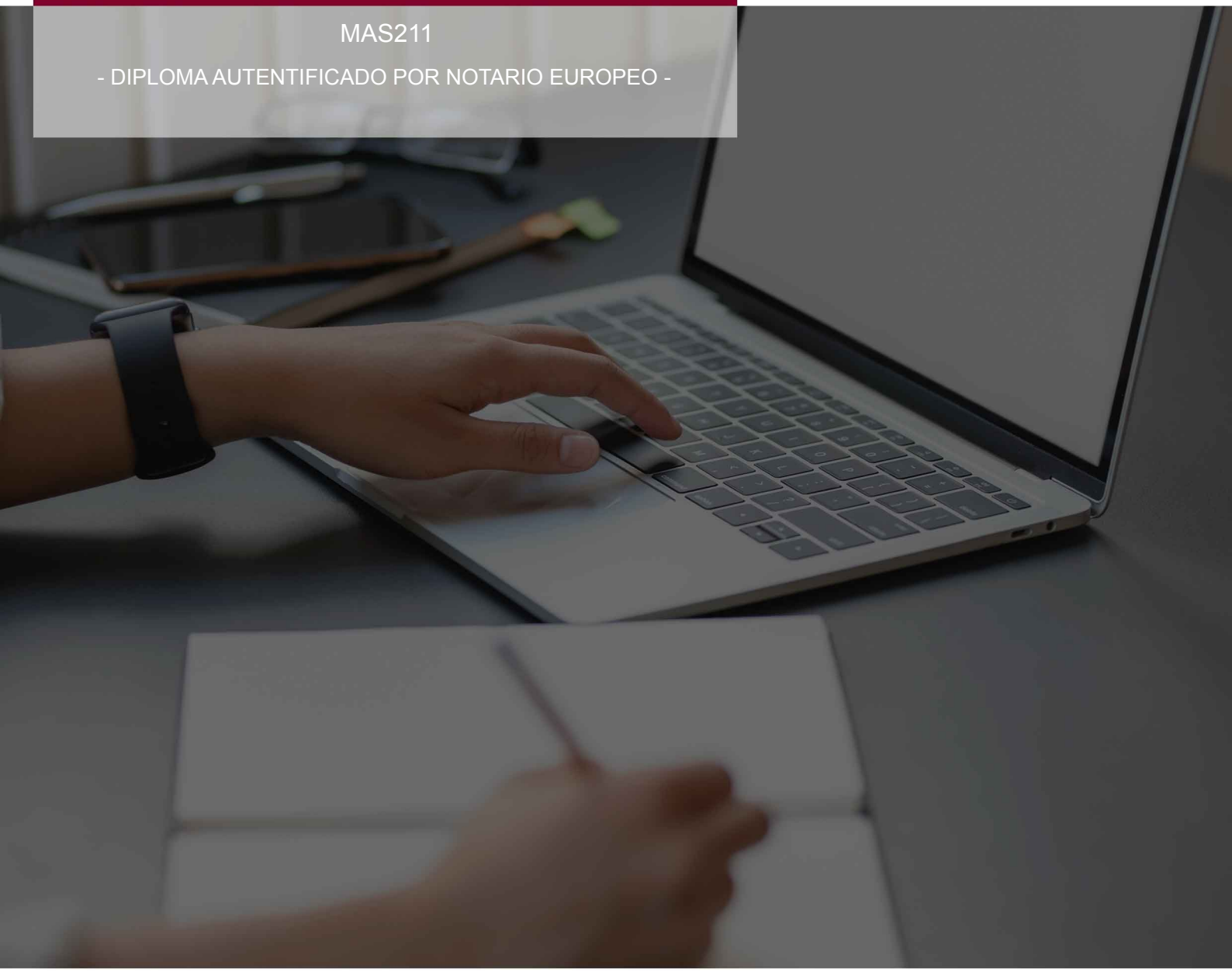
MÁSTER

MÁSTER EN GESTIÓN Y AUDITORÍA DE SISTEMAS DE SEGURIDAD DE LA INFORMACIÓN

esneca BUSINESS SCHOOL

MAS211

- DIPLOMA AUTENTIFICADO POR NOTARIO EUROPEO -



e: CUM LAUDE

aen asociación española de escuelas de negocios

CECAP

DESTINATARIOS

Este curso está dirigido a todas aquellas personas que pretendan adquirir los conocimientos necesarios en seguridad de la información: Normativa esencial sobre seguridad de la información, Implantación y seguimiento del sistema de seguridad UNE-ISO/IEC 27001:2014 y seguridad de equipos informáticos.

A través de este conjunto de materiales didácticos el alumnado podrá obtener una visión de la gestión de sistemas de seguridad de la información ISO 27001. Al final de cada unidad didáctica el alumno encontrará ejercicios de autoevaluación para poder evaluar el nivel y los conocimientos adquiridos en cada apartado.

En ambas modalidades 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
A DISTANCIA/ONLINE
*Ambas modalidades incluyen 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 GESTIÓN Y AUDITORÍA DE SISTEMAS DE SEGURIDAD DE LA INFORMACIÓN**", 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

MÓDULO 1. LA SEGURIDAD DE LA INFORMACIÓN

UNIDAD DIDÁCTICA 1. NATURALEZA Y DESARROLLO DE LA SEGURIDAD DE LA INFORMACIÓN

1. La sociedad de la información
2. ¿Qué es la seguridad de la información?
3. Importancia de la seguridad de la información
4. Principios básicos de seguridad de la información: confidencialidad, integridad y disponibilidad
    - Principio Básico de Confidencialidad
    - Principio Básico de Integridad
    - Disponibilidad
5. Descripción de los riesgos de la seguridad
6. Selección de controles
7. Factores de éxito en la seguridad de la información

UNIDAD DIDÁCTICA 2. NORMATIVA ESENCIAL SOBRE SEGURIDAD DE LA INFORMACIÓN

1. Marco legal y jurídico de la seguridad de la información
2. Normativa comunitaria sobre seguridad de la información
    - Planes de acción para la utilización más segura de Internet
    - Estrategias para una sociedad de la información más segura
    - Ataques contra los sistemas de información
    - La lucha contra los delitos informáticos
    - La Agencia Europea de Seguridad de las Redes y de la información (ENISA)
3. Normas sobre gestión de la seguridad de la información: Familia de Normas ISO 27000
    - Familia de Normas ISO 27000
    - Norma ISO/IEC 27002:2009
4. Legislación española sobre seguridad de la información
    - La protección de datos de carácter personal
    - La Ley Orgánica - de 13 de diciembre, de Protección de Datos de Carácter Personal
    - El Real Decreto - de 21 de diciembre, por el que se aprueba el Reglamento de desarrollo de la Ley Orgánica - de 13 de diciembre, de protección de datos de carácter personal
    - La Agencia Española de Protección de Datos
    - El Real Decreto - de 8 de enero, por el que se regula el Esquema Nacional de Seguridad en el ámbito de la Administración Electrónica
    - Ley - de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas
    - La Ley - de 11 de julio, de servicios de la sociedad de la información y del comercio electrónico
    - La Ley - de 9 de mayo, General de Telecomunicaciones
    - La Ley - de 19 de diciembre, de firma electrónica
    - La Ley de propiedad intelectual
    - La Ley de propiedad industrial

UNIDAD DIDÁCTICA 3. BUENAS PRÁCTICAS EN SEGURIDAD DE LA INFORMACIÓN: NORMA ISO/IEC 27002

1. Aproximación a la norma ISO/IEC 27002
2. Alcance de la Norma ISO/IEC 27002
3. Estructura de la Norma ISO/IEC 27002
    - Las cláusulas del control de seguridad
    - Las principales categorías de seguridad
4. Evaluación y tratamiento de los riesgos de seguridad
    - Evaluación de los riesgos de seguridad
    - Tratamiento de los riesgos de seguridad

UNIDAD DIDÁCTICA 4. POLÍTICA DE SEGURIDAD, ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN Y GESTIÓN DE ACTIVOS

1. Política de seguridad de la información
    - Etapas en el desarrollo de una política de seguridad de la información
    - Características esenciales de una política de seguridad de la información
    - Documento de política de la seguridad de la información
    - Revisión de la política de seguridad de la información
2. Organización de la seguridad de la información
3. Organización interna de la seguridad de la información
    - Compromiso de la dirección con la seguridad de la información
    - Coordinación de la seguridad de la información
    - Asignación de responsabilidad de seguridad de la información
    - Autorización de procesos para facilidades procesadoras de la información
    - Acuerdos de confidencialidad para la protección de la información
    - Contacto con las autoridades y con grupos de interés especial en los incidentes de seguridad
    - Revisión independiente de la seguridad de la información
4. Grupos o personas externas: el control de acceso a terceros
    - Identificación de los riesgos de seguridad relacionados con personas externas
    - Tratamiento de la seguridad de la información en las relaciones con los clientes
    - Tratamiento de la seguridad de la información en acuerdos con terceros
5. Clasificación y control de activos de seguridad de la información
6. Responsabilidad por los activos de seguridad de la información
    - Inventario de los activos de seguridad de la información
    - Propiedad de los activos de seguridad de la información
    - Uso aceptable de los activos de seguridad de la información
7. Clasificación de la información
    - Lineamientos de clasificación de la información
    - Etiquetado y manejo de información

UNIDAD DIDÁCTICA 5. SEGURIDAD FÍSICA, AMBIENTAL Y DE LOS RECURSOS HUMANOS

1. Seguridad de la información ligada a los recursos humanos
2. Medidas de seguridad de la información antes del empleo
    - Establecimiento de roles y responsabilidades de los candidatos
    - Investigación de antecedentes de los candidatos para el empleo
    - Términos y condiciones del empleo
3. Medidas de seguridad de la información durante el empleo
    - Responsabilidades de la gerencia o dirección de la organización

- Conocimiento, educación y capacitación en seguridad de la información
- Incumplimiento de las previsiones relativas a la seguridad de la información: el proceso disciplinario

4. Seguridad de la información en la finalización de la relación laboral o cambio de puesto de trabajo
   - Responsabilidades de terminación
   - Devolución de los activos
   - Cancelación de los derechos de acceso a la información
5. Seguridad de la información ligada a la seguridad física y ambiental o del entorno
6. Las áreas seguras
   - El perímetro de seguridad física
   - Los controles de ingreso físico
   - Seguridad de oficinas, locales, habitaciones y medios
   - Protección contra amenazas internas y externas a la información
   - El trabajo en áreas aseguradas
   - Áreas de carga y descarga
7. Los equipos de seguridad
   - Seguridad en el emplazamiento y protección de equipos
   - Instalaciones de suministro seguras
   - Protección del cableado de energía y telecomunicaciones
   - Mantenimiento de los equipos
   - Seguridad de los equipos fuera de las instalaciones
   - Reutilización o retirada segura de equipos
   - Retirada de materiales propiedad de la empresa
   - Equipo de usuario desatendido
   - Política de puesto de trabajo despejado y pantalla limpia

UNIDAD DIDÁCTICA 6. GESTIÓN DE LAS COMUNICACIONES Y OPERACIONES

1. Aproximación a la gestión de las comunicaciones y operaciones
2. Procedimientos y responsabilidades operacionales
   - Documentación de los procesos de operación
   - La gestión de cambios en los medios y sistemas de procesamiento de información
   - Gestión de capacidades
   - Separación de los recursos de desarrollo, prueba y operación para reducir los riesgos de acceso no autorizado
3. Gestión de la prestación de servicios de terceras partes
   - Política de seguridad de la información en las relaciones con los proveedores
   - Requisitos de seguridad en contrato con terceros
   - Cadena de suministros de tecnología de la información y de las comunicaciones
4. Planificación y aceptación del sistema
   - Políticas para la seguridad de la información
   - Revisión de las políticas para la seguridad de la información
5. Protección contra códigos maliciosos y móviles
   - Controles contra el código malicioso
   - Control contra códigos móviles
6. Copias de seguridad de la información
7. Gestión de la seguridad de la red
   - Los controles de red
   - La seguridad de los servicios de red

- Segregación en redes

8. Gestión de medios
   - Gestión de medios removibles o extraíbles
   - Eliminación de soportes o medios
   - Soportes físicos en tránsito
   - La seguridad de la documentación del sistema
9. El intercambio de información
   - Políticas y procedimientos de intercambio de información
   - Acuerdos de intercambio
   - Seguridad de los soportes físicos en tránsito
   - Mensajería electrónica
   - Acuerdos de confidencialidad o no revelación
10. Los servicios de comercio electrónico
   - Información relativa al comercio electrónico
   - Las transacciones en línea
   - La seguridad de la información puesta a disposición pública
11. Supervisión para la detección de actividades no autorizadas
   - Registro de eventos
   - Protección de la información de los registros
   - La protección de la información de los registros
   - Sincronización de reloj

UNIDAD DIDÁCTICA 7. EL CONTROL DE ACCESOS A LA INFORMACIÓN

1. El control de accesos: generalidades, alcance y objetivos
2. Requisitos de negocio para el control de accesos
   - Política de control de acceso
3. Gestión de acceso de usuario
   - Registro del usuario
   - Gestión o administración de privilegios
   - Gestión de contraseñas de usuario
   - Revisión de los derechos de acceso de usuario
4. Responsabilidades del usuario
   - El uso de contraseñas
   - Protección de equipos desatendidos
   - Política de puesto de trabajo despejado y pantalla limpia
5. Control de acceso a la red
   - La política de uso de los servicios en red
   - Autentificación de los usuarios de conexiones externas
   - Identificación de equipos en las redes
   - Diagnóstico remoto y protección de los puertos de configuración
   - Segregación de las redes
   - Control de la conexión a la red
   - El control de routing o encaminamiento de red
6. Control de acceso al sistema operativo
   - Procedimientos seguros de inicio de sesión
   - Identificación y autentificación del usuario
   - El sistema de gestión de contraseñas
   - El uso de los recursos del sistema
   - La desconexión automática de sesión
   - Limitación del tiempo de conexión
7. Control de acceso a las aplicaciones y a la información
   - Restricciones del acceso a la información

- Aislamiento de sistemas sensibles

8. Informática móvil y teletrabajo
   - Los ordenadores portátiles y las comunicaciones móviles
   - El teletrabajo

UNIDAD DIDÁCTICA 8. ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE LOS SISTEMAS DE INFORMACIÓN

1. Objetivos del desarrollo y mantenimiento de sistemas de información
2. Requisitos de seguridad de los sistemas de información
3. Tratamiento correcto de la información en las aplicaciones
   - Validación de los datos de entrada
   - El control de procesamiento interno
   - La integridad de los mensajes
   - Validación de los datos de salida
4. Controles criptográficos
   - Política de uso de los controles criptográficos
   - Gestión de claves
5. Seguridad de los archivos del sistema
   - Control del software en explotación
   - Protección de los datos de prueba en el sistema
   - El control de acceso al código fuente de los programas
6. Seguridad de los procesos de desarrollo y soporte
   - Procedimientos para el control de cambios
   - Revisión técnica de aplicaciones tras efectuar cambios en el sistema operativo
   - Restricciones a los cambios en los paquetes de software
   - Entorno de desarrollo seguro
   - Externalización de software por terceros
7. Gestión de la vulnerabilidad técnica

UNIDAD DIDÁCTICA 9. GESTIÓN DE INCIDENTES EN LA SEGURIDAD DE LA INFORMACIÓN Y DE LA CONTINUIDAD DEL NEGOCIO

1. La gestión de incidentes en la seguridad de la información
2. Notificación de eventos y puntos débiles en la seguridad de la información
   - Notificación de los eventos en la seguridad de la información
   - Notificación de puntos débiles de la seguridad
3. Gestión de incidentes y mejoras en la seguridad de la información
   - Responsabilidades y procedimientos
   - Aprendizaje de los incidentes de seguridad de la información
   - Recopilación de evidencias
4. Gestión de la continuidad del negocio
5. Aspectos de la seguridad de la información en la gestión de la continuidad del negocio
   - Inclusión de la seguridad de la información en el proceso de gestión de la continuidad del negocio
   - Continuidad del negocio y evaluación de riesgos
   - Desarrollo e implantación de planes de continuidad del negocio que incluyan la seguridad de la información
   - Marco de referencia para la planificación de la continuidad del negocio
   - Pruebas, mantenimiento y reevaluación de los planes de continuidad

UNIDAD DIDÁCTICA 10. CUMPLIMIENTO DE LAS PREVISIONES LEGALES Y TÉCNICAS

1. Cumplimiento de los requisitos legales
    - Normativa aplicable
    - Derechos de propiedad intelectual
    - Protección de registros organizacionales
    - Privacidad de la información personal
    - Prevención del mal uso de los medios de procesamiento de la información
    - Regulación de los controles criptográficos
2. Cumplimiento de las políticas y estándares de seguridad, y cumplimiento técnico
    - Cumplimiento de las políticas y estándares de seguridad
    - Verificación del cumplimiento técnico
3. Consideraciones de la auditoría de los sistemas de información
    - Controles de auditoría de los sistemas de información
    - Protección de las herramientas de auditoría de los sistemas de información

MÓDULO 2. EL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN

UNIDAD DIDÁCTICA 11. LA NORMA UNE-EN-ISO/IEC 27001:2017

1. Objeto y ámbito de aplicación
2. Relación con la Norma ISO/IEC 27002:2009
3. Definiciones y términos de referencia
4. Beneficios aportados por un sistema de seguridad de la información
5. Introducción a los sistemas de gestión de seguridad de la información

UNIDAD DIDÁCTICA 12. IMPLANTACIÓN DEL SISTEMA DE SEGURIDAD EN LA ORGANIZACIÓN

1. Contexto
2. Liderazgo
3. Planificación
    - Acciones para tratar los riesgos y oportunidades
    - Objetivos de seguridad de la información y planificación para su consecución
4. Soporte

UNIDAD DIDÁCTICA 13. SEGUIMIENTO DE LA IMPLANTACIÓN DEL SISTEMA

1. Operación
2. Evaluación del desempeño
    - Seguimiento, medición, análisis y evaluación
    - Auditoría interna
    - Revisión por la dirección
3. Mejora
    - No conformidad y acciones correctivas
    - Mejora continua