LAW&SAFETY
SCHOOL

MÁSTER

MASTER INTERNACIONAL EN GESTIÓN Y AUDITORÍA DE SISTEMAS DE SEGURIDAD DE LA INFORMACIÓN ISO 27001:2014

DIPLOMA AUTENTIFICADO POR NOTARIO EUROPEO

LAW009

AEC
ASOCIACIÓN ESPAÑOLA PARA LA CALIDAD

FE PÚBLICA NOTARIAL · CONSEJO GENERAL DEL NOTARIADO ESPAÑOL · NOTARIADO EUROPA · 0165397863

ESPAÑA
NIHIL PRIUS FIDE
NOTARIO

DESTINATARIOS

Este máster internacional en gestión y auditoría de sistemas de seguridad de la información ISO 27001:2014está dirigido a empresarios, directivos, emprendedores y trabajadores. Permite conocer la gestión de sistemas de seguridad de la información ISO 27001, la seguridad del la información, el sistema de gestión de seguridad de la información y la seguridad en equipos informáticos.

MODALIDAD

- **A DISTANCIA**: una vez recibida tu matrícula, enviaremos a tu domicilio el pack formativo que consta de los manuales de estudio y del cuaderno de ejercicios.

DURACIÓN

La duración del curso es de 600 horas.

IMPORTE

IMPORTE ORIGINAL: ~~1780€~~

IMPORTE ACTUAL: 890€

CERTIFICACIÓN OBTENIDA

Una vez finalizados los estudios y superadas las pruebas de evaluación, el alumno recibirá un diploma que certifica el "MASTER INTERNACIONAL EN GESTIÓN Y AUDITORÍA DE SISTEMAS DE SEGURIDAD DE LA INFORMACIÓN ISO 27001:2014", de LAW&SAFETY BUSINESS SCHOOL, avalada por nuestra condición de socios de la AEC, máxima institución española 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.

CONTENIDO FORMATIVO

PARTE 1. GESTIÓN DE SISTEMAS DE SEGURIDAD DE LA INFORMACIÓN ISO 27001

MÓDULO I. LA SEGURIDAD DEL 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 persona
    - La Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal
    - El Real Decreto 1720/2007, de 21 de diciembre, por el que se aprueba el Reglamento de desarrollo de la Ley Orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal
    - La Agencia Española de Protección de Datos
    - El Real Decreto 3/2010, de 8 de enero, por el que se regula el Esquema Nacional de Seguridad en el ámbito de la Administración Electrónica
    - La Ley 11/2007, de 22 de junio, de Acceso Electrónico de los Ciudadanos a los Servicios Públicos
    - La Ley 34/2002, de 11 de julio, de servicios de la sociedad de la información y del comercio electrónico
    - La Ley 9/2014, de 9 de mayo, General de Telecomunicaciones
    - La Ley 59/2003, 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 77
    - 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
    - Aseguramiento de oficinas, locales, habitaciones y medios
    - Protección contra amenazas internas y externas a la información
    - El trabajo en áreas aseguradas
    - Control y aislamiento de 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

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
    - Segregación de tareas o deberes para reducir las modificaciones no autorizadas
    - 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
    - Provisión o entrega del servicio
    - Supervisión y revisión de los servicios prestados por terceros
    - Gestión de cambios en los servicios prestados por terceros
4. Planificación y aceptación del sistema
    - Gestión de capacidades de los sistemas
    - Aceptación del sistema de información nuevo o actualizado
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
8. Gestión de medios

- Gestión de medios removibles o extraíbles
- Eliminación de soportes o medios
- Procedimientos para el manejo de la información
- La seguridad de la documentación del sistema

9. El intercambio de información
    - Políticas y procedimientos de intercambio de información
    - Acuerdos de intercambio de información y software
    - Seguridad de los soportes físicos en tránsito
    - Seguridad de la información en el uso de la mensajería electrónica
    - Los sistemas de información empresariales
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 incidencias o de auditoría
    - Supervisión del uso del sistema
    - La protección de la información de los registros
    - Mantenimiento de los registros del administrador del sistema y del operador
    - El registro de fallos
    - Sincronización de reloj entre los equipos

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 información3
    - 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
    - Las fugas de información
    - Desarrollo 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 237
    - 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 II. EL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN

UNIDAD DIDÁCTICA 11. LA NORMA UNE-EN-ISO/IEC 27001:2014

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
    - Acciones para tratar los riesgos y oportunidades
    - Objetivos de seguridad de la información y planificación para su consecución
3. 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

PARTE 2. SEGURIDAD EN EQUIPOS INFORMÁTICOS

UNIDAD DIDÁCTICA 1. CRITERIOS GENERALES COMÚNMENTE ACEPTADOS SOBRE SEGURIDAD DE LOS EQUIPOS INFORMÁTICOS

1. Modelo de seguridad orientada a la gestión del riesgo relacionado con el uso de los sistemas de información

2. Relación de las amenazas más frecuentes, los riesgos que implican y las salvaguardas más frecuentes
3. Salvaguardas y tecnologías de seguridad más habituales
4. La gestión de la seguridad informática como complemento a salvaguardas y medidas tecnológicas

UNIDAD DIDÁCTICA 2. ANÁLISIS DE IMPACTO DE NEGOCIO

1. Identificación de procesos de negocio soportados por sistemas de información
2. Valoración de los requerimientos de confidencialidad, integridad y disponibilidad de los procesos de negocio
3. Determinación de los sistemas de información que soportan los procesos de negocio y sus requerimientos de seguridad

UNIDAD DIDÁCTICA 3. GESTIÓN DE RIESGOS

1. Aplicación del proceso de gestión de riesgos y exposición de las alternativas más frecuentes
2. Metodologías comúnmente aceptadas de identificación y análisis de riesgos
3. Aplicación de controles y medidas de salvaguarda para obtener una reducción del riesgo

UNIDAD DIDÁCTICA 4. PLAN DE IMPLANTACIÓN DE SEGURIDAD

1. Determinación del nivel de seguridad existente de los sistemas frente a la necesaria en base a los requerimientos de seguridad de los procesos de negocio.
2. Selección de medidas de salvaguarda para cubrir los requerimientos de seguridad de los sistemas de información
3. Guía para la elaboración del plan de implantación de las salvaguardas seleccionadas

UNIDAD DIDÁCTICA 5. PROTECCIÓN DE DATOS DE CARÁCTER PERSONAL

1. Principios generales de protección de datos de carácter personal
2. Infracciones y sanciones contempladas en la legislación vigente en materia de protección de datos de carácter personal
3. Identificación y registro de los ficheros con datos de carácter personal utilizados por la organización
4. Elaboración del documento de seguridad requerido por la legislación vigente en materia de protección de datos de carácter personal

UNIDAD DIDÁCTICA 6. SEGURIDAD FÍSICA E INDUSTRIAL DE LOS SISTEMAS. SEGURIDAD LÓGICA DE SISTEMAS

1. Determinación de los perímetros de seguridad física
2. Sistemas de control de acceso físico más frecuentes a las instalaciones de la organización y a las áreas en las que estén ubicados los sistemas informáticos
3. Criterios de seguridad para el emplazamiento físico de los sistemas informáticos
4. Exposición de elementos más frecuentes para garantizar la calidad y continuidad del suministro eléctrico a los sistemas informáticos
5. Requerimientos de climatización y protección contra incendios aplicables a los sistemas informáticos
6. Elaboración de la normativa de seguridad física e industrial para la organización
7. Sistemas de ficheros más frecuentemente utilizados
8. Establecimiento del control de accesos de los sistemas informáticos a la red de comunicaciones de la organización
9. Configuración de políticas y directivas del directorio de usuarios

10. Establecimiento de las listas de control de acceso (ACLs) a ficheros
11. Gestión de altas, bajas y modificaciones de usuarios y los privilegios que tienen asignados
12. Requerimientos de seguridad relacionados con el control de acceso de los usuarios al sistema operativo
13. Sistemas de autenticación de usuarios débiles, fuertes y biométricos
14. Relación de los registros de auditoría del sistema operativo necesarios para monitorizar y supervisar el control de accesos
15. Elaboración de la normativa de control de accesos a los sistemas informáticos

UNIDAD DIDÁCTICA 7. IDENTIFICACIÓN DE SERVICIOS

1. Identificación de los protocolos, servicios y puertos utilizados por los sistemas de información
2. Utilización de herramientas de análisis de puertos y servicios abiertos para determinar aquellos que no son necesarios
3. Utilización de herramientas de análisis de tráfico de comunicaciones para determinar el uso real que hacen los sistemas de información de los distintos protocolos, servicios y puertos

UNIDAD DIDÁCTICA 8. ROBUSTECIMIENTO DE SISTEMAS

1. Modificación de los usuarios y contraseñas por defecto de los distintos sistemas de información
2. Configuración de las directivas de gestión de contraseñas y privilegios en el directorio de usuarios
3. Eliminación y cierre de las herramientas, utilidades, servicios y puertos prescindibles
4. Configuración de los sistemas de información para que utilicen protocolos seguros donde sea posible
5. Actualización de parches de seguridad de los sistemas informáticos
6. Protección de los sistemas de información frente a código malicioso
7. Gestión segura de comunicaciones, carpetas compartidas, impresoras y otros recursos compartidos del sistema
8. Monitorización de la seguridad y el uso adecuado de los sistemas de información

UNIDAD DIDÁCTICA 9. IMPLANTACIÓN Y CONFIGURACIÓN DE CORTAFUEGOS

1. Relación de los distintos tipos de cortafuegos por ubicación y funcionalidad
2. Criterios de seguridad para la segregación de redes en el cortafuegos mediante Zonas Desmilitarizadas / DMZ
3. Utilización de Redes Privadas Virtuales / VPN para establecer canales seguros de comunicaciones
4. Definición de reglas de corte en los cortafuegos
5. Relación de los registros de auditoría del cortafuegos necesarios para monitorizar y supervisar su correcto funcionamiento y los eventos de seguridad
6. Establecimiento de la monitorización y pruebas del cortafuegos