ESCUELA EUROPEA DE TECNOLOGÍA Y COMUNICACIÓN

DOBLE TITULACIÓN

MAESTRÍA INTERNACIONAL EN SEGURIDAD INFORMÁTICA + MAESTRÍA INTERNACIONAL EN COACHING TECNOLÓGICO

LTIC020

Escuela asociada a:

CECAP
CONFEDERACIÓN ESPAÑOLA DE EMPRESAS DE FORMACIÓN

AEC
ASOCIACIÓN ESPAÑOLA PARA LA CALIDAD

aeen
ASOCIACIÓN ESPAÑOLA DE ESCUELAS DE NEGOCIOS

Reconocimiento de calidad:

ICEEX
EXCELLENCE & QUALITY
CERTIFICATED: 202142

DESTINATARIOS

La doble titulación de maestría internacional en seguridad informática + maestría internacional en coaching tecnológico está dirigida a empresarios, emprendedores o trabajadores en el ámbito de la informática. Permite conocer los criterios generales sobre la seguridad de los equipos informáticos, el análisis de impacto de negocio, la gestión de riesgos, el plan de implantación, la protección de datos, la seguridad física e industrial y la auditoría de sistemas; además adquieres conocimientos de coaching tecnológico en la aplicación de diferentes técnicas.

MODALIDAD

La modalidad de la maestría es **ON-LINE** y **TUTORIZADA**

- Una vez matriculado, el alumno recibirá las claves de acceso en menos de 24 horas laborables.
- Nuestro equipo de profesores y tutores contactará con el alumno en un máximo de 48 horas tras la matrícula para guiar al alumno, acompañarlo en el inicio y a lo largo del curso, y responder a cualquier duda o pregunta que pueda surgir.

DURACIÓN

La duración del curso es de 600 horas.

IMPORTE

MONTO ORIGINAL: ~~2.190$~~

MONTO ACTUAL: 1.095$

*Importe expresado en Dólares Americanos

CERTIFICACIÓN OBTENIDA

Una vez finalizados los estudios y superadas las pruebas de evaluación, el alumno recibirá un diploma que certifica la "MAESTRÍA INTERNACIONAL EN SEGURIDAD INFORMÁTICA + MAESTRÍA INTERNACIONAL EN COACHING TECNOLÓGICO", de ESCUELA EUROPEA DE TECNOLOGÍA Y COMUNICACIÓN, avalada por nuestra condición de socios de la CECAP, AEC y AEEN, máximas instituciones españolas en formación y de calidad.

ESNECA BUSINESS SCHOOL, desde noviembre de 2016, y siguiendo su apuesta por la calidad, ha sido reconocida con el sello ICEEX de la excelencia y la calidad de la formación.

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.

La Titulación puede disponer de la APOSTILLA DE LA HAYA (Certificación Oficial que da validez a la Titulación ante el Ministerio de Educación de más de 200 países de todo el mundo).

CONTENIDO FORMATIVO

PARTE 1. LA SEGURIDAD INFORMÁTICA

MÓDULO 1. SEGURIDAD INFORMATICA

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. 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 necesario para monitorizar y supervisar su correcto funcionamiento y los eventos de seguridad
6. Establecimiento de la monitorización y pruebas de los cortafuegos

UNIDAD DIDÁCTICA 9. ANÁLISIS DE RIESGOS DE LOS SISTEMAS DE INFORMACIÓN.

1. Introducción al análisis de riesgos
2. Principales tipos de vulnerabilidades, fallos de programa, programas maliciosos y su actualización permanente, así como criterios de programación segura
3. Particularidades de los distintos tipos de código malicioso
4. Principales elementos del análisis de riesgos y sus modelos de relaciones

5. Metodologías cualitativas y cuantitativas de análisis de riesgos
6. Identificación de los activos involucrados en el análisis de riesgos y su valoración
7. Identificación de las amenazas que pueden afectar a los activos identificados previamente
8. Análisis e identificación de las vulnerabilidades existentes en los sistemas de información que permitirían la materialización de amenazas, incluyendo el análisis local, análisis remoto de caja blanca y de caja negra
9. Optimización del proceso de auditoría y contraste de vulnerabilidades e informe de auditoría
10. Identificación de las medidas de salvaguarda existentes en el momento de la realización del análisis de riesgos y su efecto sobre las vulnerabilidades y amenazas
11. Establecimiento de los escenarios de riesgo entendidos como pares activo-amenaza susceptibles de materializarse
12. Determinación de la probabilidad e impacto de materialización de los escenarios
13. Establecimiento del nivel de riesgo para los distintos pares de activo y amenaza
14. Determinación por parte de la organización de los criterios de evaluación del riesgo, en función de los cuales se determina si un riesgo es aceptable o no
15. Relación de las distintas alternativas de gestión de riesgos
16. Guía para la elaboración del plan de gestión de riesgos
17. Exposición de la metodología NIST SP 800-30
18. Exposición de la metodología Magerit versión 2

UNIDAD DIDÁCTICA 10. USO DE HERRAMIENTAS PARA LA AUDITORÍA DE SISTEMAS.

1. Herramientas del sistema operativo tipo Ping, Traceroute, etc.
2. Herramientas de análisis de red, puertos y servicios tipo Nmap, Netcat, NBTScan, etc.
3. Herramientas de análisis de vulnerabilidades tipo Nessus
4. Analizadores de protocolos tipo WireShark, DSniff, Cain Abel, etc.
5. Analizadores de páginas web tipo Acunetix, Dirb, Parosproxy, etc.
6. Ataques de diccionario y fuerza bruta tipo Brutus, John the Ripper, etc.

UNIDAD DIDÁCTICA 11. DESCRIPCIÓN DE LOS ASPECTOS SOBRE CORTAFUEGOS EN AUDITORÍAS DE SISTEMAS INFORMÁTICOS.

1. Principios generales de cortafuegos
2. Componentes de un cortafuegos de red
3. Relación de los distintos tipos de cortafuegos por ubicación y funcionalidad
4. Arquitecturas de cortafuegos de red
5. Otras arquitecturas de cortafuegos de red

UNIDAD DIDÁCTICA 12. GUÍAS PARA LA EJECUCIÓN DE LAS DISTINTAS FASES DE LA AUDITORÍA DE SISTEMAS DE INFORMACIÓN.

1. Guía para la auditoría de la documentación y normativa de seguridad existente en la organización auditada
2. Guía para la elaboración del plan de auditoría
3. Guía para las pruebas de auditoría
4. Guía para la elaboración del informe de auditoría

PARTE 2. COACHING TECNOLÓGICO

1. El coaching
2. Introducción al coaching
3. El coach
4. El ciclo del coaching
5. La mochila
6. Las 7 etapas
7. Bill Gates: La retroalimentacion
8. El feedback
9. La aceptación del error
10. El caso Pans
11. El caso Papelería Bonilla
12. Navaja de Ockham
13. Coaching ejecutivo y profesional I
14. Coaching ejecutivo y profesional II
15. Coaching personal
16. "Dejar de fumar"
17. Principios básicos para el éxito en un proceso de coaching
18. Agentes en los procesos de coaching
19. Fases del coaching
20. Análisis de la organización
21. Planificación del programa
22. Importancia de la evaluación.
23. Devolución de la información de la evaluación
24. Diseño del plan individualizado
25. Puesta en marcha del plan de acción
26. Sesiones de seguimiento
27. Evaluaciones periódicas
28. Sesión de coaching I. Como aplicar en una sesión real los conocimientos adquiridos.
29. Sesión de coaching II. Como aplicar en una sesión real los conocimientos adquiridos.
30. Manual completo de Coaching