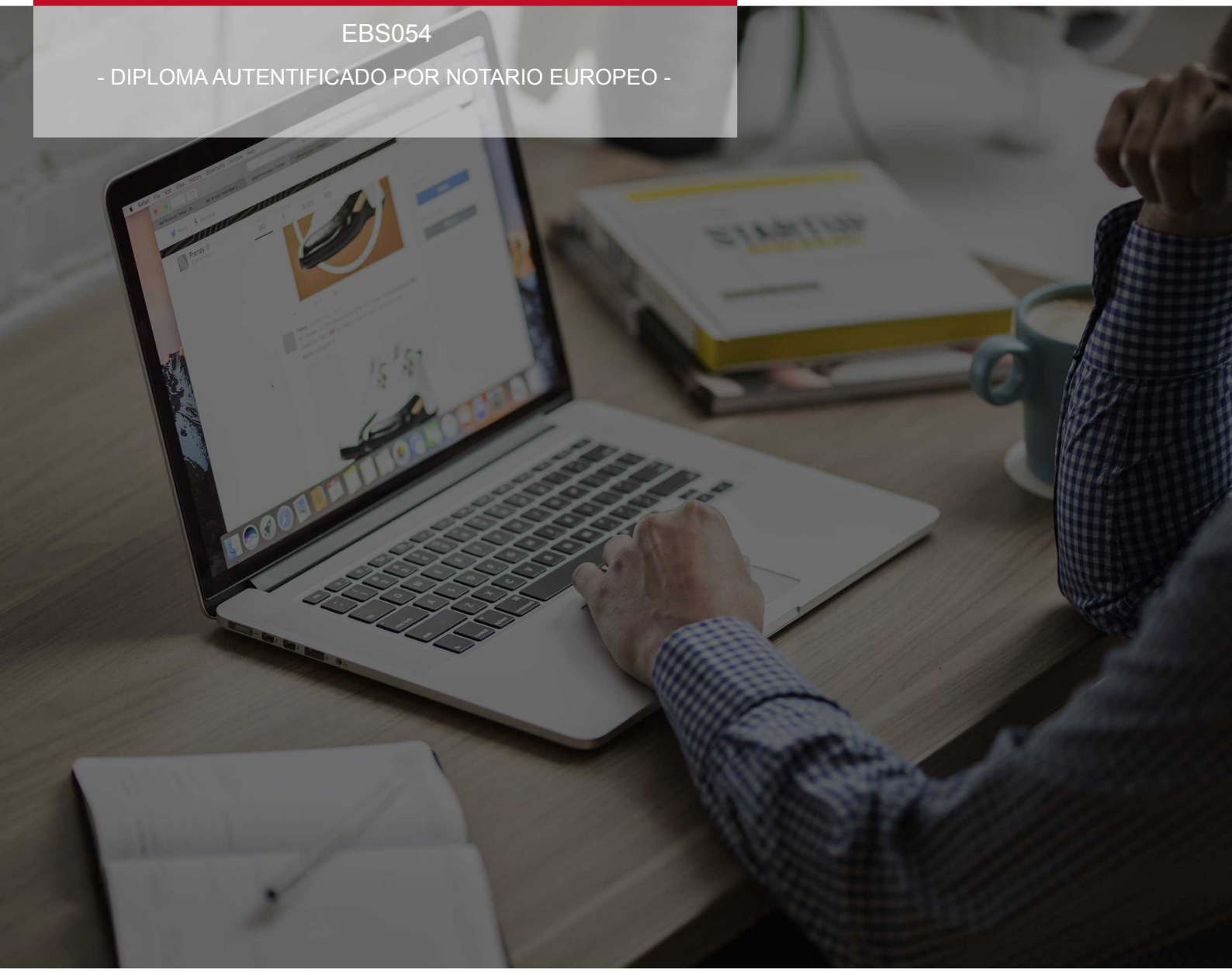
CURSO

CERTIFICACIÓN EXPERTO EN CYBERSEGURIDAD Y CYBERDELINCUENCIA

ELBS
ESCUELA DE LIDERAZGO

EBS054

- DIPLOMA AUTENTIFICADO POR NOTARIO EUROPEO -



CUM LAUDE

ESPAÑA
NIHIL PRIUS FIDE
NOTARIO

CECAP

DESTINATARIOS

El Programa está especialmente diseñado para aquellas personas que estén interesadas en adquirir conocimientos sobre **Cyberseguridad y Cyberdelincuencia** y que quieran asegurarse un recorrido ascendente en esta área, con una especial elevación y consolidación de competencias.

Permitirá adquirir las competencias profesionales necesarias para conocer el concepto y modelos de seguridad, tipos de control de acceso, autentificación de datos y posibles ataques a los sistemas informáticos, aprender las pautas y ámbitos de aplicación para el Reglamento de Seguridad y la aplicación de sus principales puntos del reglamento en Windows, saber aplicar la ley de protección de datos aplicada en España: los principios de protección de datos y la forma en que se debe aplicar, así como garantizar la continuidad de las operaciones de los elementos críticos que componen los sistemas de información, mediante acciones y procedimientos.

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
300H

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: ~~1920€~~
VALOR ACTUAL: 480€

CERTIFICACIÓN OBTENIDA

Una vez finalizados los estudios y superadas las pruebas de evaluación, el alumno recibirá un diploma que certifica el "**CERTIFICACIÓN EXPERTO EN CYBERSEGURIDAD Y CYBERDELINCUENCIA**", de ELBS ESCUELA DE LIDERAZGO, avalada por nuestra condición de socios de la CECAP, 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.

REDES SOCIALES

www.facebook.com/escuelaelbs

www.linkedin.com/company/elbs-escueladeliderazgo

@escuela_elbs_formacion

www.escuelaelbs.com

@ELBS_School

www.escuelaelbs.com/blog

CONTENIDO FORMATIVO

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

MÓDULO 2. INFORMÁTICA Y ELECTRÓNICA FORENSE

UNIDAD DIDÁCTICA 1. INFORMÁTICA, CONECTIVIDAD E INTERNET

1. La informática
    - Conceptos básicos
2. Componentes de un sistema informático
3. Estructura básica de un sistema informático
4. Unidad central de proceso en un sistema informático
    - Estructura
5. Periféricos más usuales: conexión
6. Sistema operativo
7. Internet
8. Conectividad a Internet
    - Tipos de redes
    - Red inalámbrica

UNIDAD DIDÁCTICA 2. FUNDAMENTOS DE LA INFORMÁTICA Y ELECTRÓNICA FORENSE

1. Concepto de informática forense
2. Objetivos de la informática forense
3. Usos de la informática forense
4. El papel del perito informático
5. El laboratorio informático forense
6. Evidencia digital
    - Evidencias volátiles y no volátiles
    - Etiquetado de evidencias
7. Cadena de custodia

UNIDAD DIDÁCTICA 3. CIBERSEGURIDAD

1. El ciberespacio y su seguridad
2. Riesgos y amenazas de la ciberseguridad
    - Amenazas internas y externas
    - Principales riesgos y amenazas
3. Objetivos de la ciberseguridad
4. Líneas de acción de la ciberseguridad nacional
5. Instituto Nacional de Ciberseguridad

UNIDAD DIDÁCTICA 4. CIBERCRIMINALIDAD

1. Delito informático
    - Principales características del delito informático
2. Tipos de delito informático
3. Cibercriminalidad
    - Evolución de la sociedad española en el empleo de las nuevas tecnologías. Los delitos cibernéticos

UNIDAD DIDÁCTICA 5. HACKING ÉTICO

1. ¿Qué es el hacking ético?
    - Ética hacker
    - Valores de la ética hacker
    - Fases del Hacking Ético
    - Tipo de Hacking Ético

2. Aspectos legales del hacking ético
3. Perfiles del hacker
    - Hacker de sombrero negro
    - Hacker de sombrero blanco
    - Hacker de sombrero gris
    - Otros perfiles
4. Hacktivismo

UNIDAD DIDÁCTICA 6. ANÁLISIS FORENSE

1. El análisis forense
2. Etapas de un análisis forense
    - Estudio preliminar
    - Adquisición de datos
    - Análisis e investigación
    - Presentación y realización del informe pericial
3. Tipos de análisis forense
4. Requisitos para el análisis forense
5. Principales problemas

UNIDAD DIDÁCTICA 7. SOPORTE DE DATOS

1. Adquisición de datos: importancia en el análisis forense digital
2. Modelo de capas
3. Recuperación de archivos borrados
    - Dinámica del borrado de archivos
    - Características exigibles para recuperación de archivos y datos borrados
    - Principales herramientas para recuperación de datos
    - La acción de recuperación
4. Análisis de archivos
    - Firmas características
    - Documentos
    - Archivos gráficos y multimedia
    - Archivos ejecutables

UNIDAD DIDÁCTICA 8. SISTEMA DE GESTIÓN DE SEGURIDAD EN LA INFORMACIÓN SGSI

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
8. Introducción a los sistemas de gestión de seguridad de la información
9. Beneficios aportados por un sistema de seguridad de la información

UNIDAD DIDÁCTICA 9. MARCO NORMATIVO

1. Marco normativo
2. Normativa 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. Normativa relacionada con la ciberseguridad
4. Legislación sobre delitos informáticos