

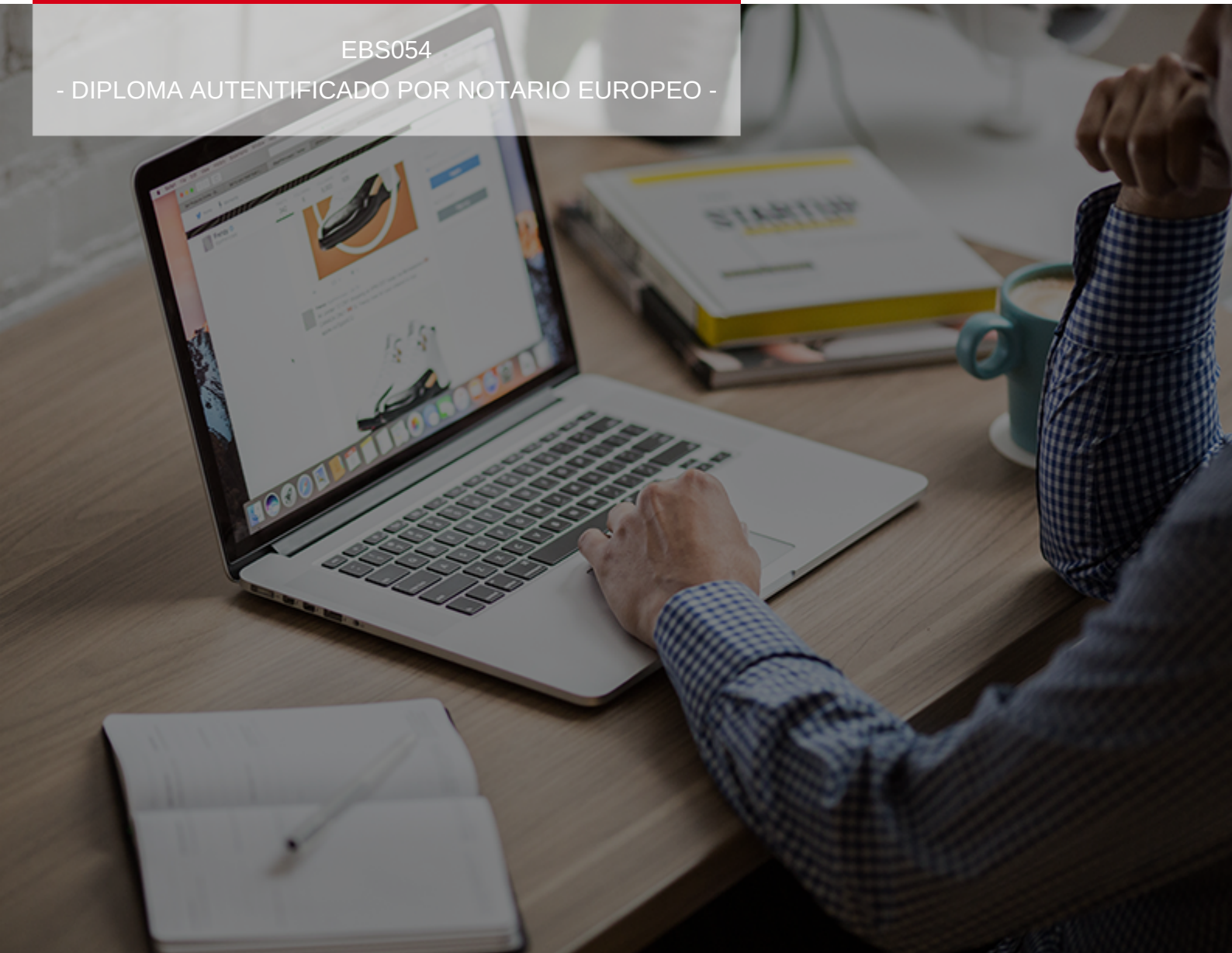
CURSO

CERTIFICACIÓN EXPERTO EN CIBERSEGURIDAD Y
CIBERDELINCUENCIA



EBS054

- DIPLOMA AUTENTIFICADO POR NOTARIO EUROPEO -



DESTINATARIOS

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

Permite conocer la introducción a la ciberseguridad y los ciberataques, el centri de operaciones de seguridad (SOC), la criptografía, el concepto de privacidad, la biometría, los ciberataques a contraseñas y conexiones, los ciberataques de ingeniería social y por malware, las vulnerabilidades, los análisis y la gestión de vulnerabilidades, los riesgos y los ataques, el análisis forense, el hacking ético, la seguridad de la información, la seguridad en redes, los aspectos legislativos, entre otros conceptos relacionados. Además, al final de cada unidad didáctica el alumno/a encontrará ejercicios de autoevaluación que le permitirán hacer un seguimiento del curso de forma autónoma.

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
ONLINE 
*La modalidad incluye módulos con clases en directo.

CURSO INICIAL
ONLINE 

TUTORIAS
PERSONALIZADAS 

IDIOMA
ESPAÑOL 

DURACION
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 CIBERSEGURIDAD Y CIBERDELINCUENCIA** ”, 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.

CONTENIDO FORMATIVO

PARTE 1

CIBERSEGURIDAD, PREVENCIÓN Y GESTIÓN DE CIBERATAQUES

INTRODUCCIÓN

MÓDULO 1. INTRODUCCIÓN A LA CIBERSEGURIDAD Y LOS CIBERATAQUES

UNIDAD DIDÁCTICA 1. CIBERSEGURIDAD

1. Funciones
2. Diferenciación de conceptos relacionados
3. Ciberseguros

UNIDAD DIDÁCTICA 2. CENTRO DE OPERACIONES DE SEGURIDAD (SOC)

1. Servicios del SOC
2. Figura del *chief information security officer* (CISO)
 - Funciones
 - Competencias y habilidades
3. Cultura de la ciberseguridad en las empresas

UNIDAD DIDÁCTICA 3. CIBERINTELIGENCIA DE LA AMENAZA

1. Campos de actuación
2. Aspectos diferenciales entre ciberseguridad y ciberinteligencia
3. Tipos de ciberinteligencia
 - Ciberinteligencia estratégica
 - Ciberinteligencia táctica
 - Ciberinteligencia operacional
4. Figura del analista en ciberinteligencia
 - Tareas
 - Competencias y habilidades

UNIDAD DIDÁCTICA 4. VENTAJAS DE LA INTELIGENCIA ARTIFICIAL EN CIBERSEGURIDAD

RESUMEN

AUTOEVALUACIÓN

MÓDULO 2. CRIPTOGRAFÍA

UNIDAD DIDÁCTICA 1. CONCEPTO DE PRIVACIDAD

UNIDAD DIDÁCTICA 2. FUNDAMENTOS DE LA ENCRIPCIÓN Y DE LA CRIPTOGRAFÍA

1. Usos principales

UNIDAD DIDÁCTICA 3. TIPOS DE CIFRADO

1. Cifrados clásicos
 - Cifrado del César
 - Cifrado de Vigenère
2. Cifrado de clave simétrica
 - Algoritmo DES
 - Algoritmo AES
3. Cifrado de clave asimétrica
 - Algoritmo RSA
 - Algoritmo Diffie Hellman
 - Algoritmo Rabin
 - Algoritmo DSA
4. Cifrado híbrido

UNIDAD DIDÁCTICA 4. APLICACIONES DE LA CRIPTOGRAFÍA

1. Firma electrónica
2. Certificado digital
3. Autenticación

UNIDAD DIDÁCTICA 5. MÉTODOS DE OCULTACIÓN DE INFORMACIÓN (ESTEGANOGRAFÍA)

UNIDAD DIDÁCTICA 6. SISTEMAS BLOCKCHAIN

UNIDAD DIDÁCTICA 7. CRIPTOGRAFÍA EN REDES

1. Red TOR
2. *Deep web*
3. *Dark web*

RESUMEN

AUTOEVALUACIÓN

MÓDULO 3. BIOMETRÍA

UNIDAD DIDÁCTICA 1. ¿QUÉ ES LA BIOMETRÍA?

1. Usos
2. Beneficios

UNIDAD DIDÁCTICA 2. COMPONENTES DE UN SISTEMA BIOMÉTRICO

UNIDAD DIDÁCTICA 3. TIPOS DE BIOMETRÍA

1. Biometría fisiológica
 - Reconocimiento facial
 - Reconocimiento ocular
 - Reconocimiento por huella
 - Otros métodos fisiológicos
2. Biometría de comportamiento
 - Reconocimiento de voz
 - Reconocimiento de firma
 - Otros métodos de comportamiento

UNIDAD DIDÁCTICA 4. RIESGOS Y VULNERABILIDADES EN SISTEMAS BIOMÉTRICOS

UNIDAD DIDÁCTICA 5. BUENAS PRÁCTICAS DE REDUCCIÓN DE

RIESGOS EN BIOMETRÍA

RESUMEN

AUTOEVALUACIÓN

MÓDULO 4. CIBERATAQUES A CONTRASEÑAS Y CONEXIONES

UNIDAD DIDÁCTICA 1. DELINCUENCIA INFORMÁTICA: CIBERATAQUES

1. Afectación de los ciberataques
2. Etapas de un ciberataque

UNIDAD DIDÁCTICA 2. ATAQUES A CONTRASEÑAS

1. Ataque por fuerza bruta
2. Ataque por diccionario

UNIDAD DIDÁCTICA 3. ATAQUES A CONEXIONES

1. Redes trampa
2. Suplantación
3. Ataque a *cookies*
4. *Spoofing*
5. Ataque DDoS
6. Inyección SQL
7. Escaneo de puertos
8. *Sniffing*

RESUMEN

AUTOEVALUACIÓN

MÓDULO 5. CIBERATAQUES DE INGENIERÍA SOCIAL Y POR MALWARE

UNIDAD DIDÁCTICA 1. ¿QUÉ ES LA INGENIERÍA SOCIAL?

UNIDAD DIDÁCTICA 2. ATAQUES POR INGENIERÍA SOCIAL

1. *Spam*
2. *Phishing*
3. *Vishing*
4. *Smishing*
5. *Baiting* o gancho
6. *Shoulder surfing*
7. *Dumpster diving*

UNIDAD DIDÁCTICA 3. CONCEPTO DE MALWARE

UNIDAD DIDÁCTICA 4. ATAQUES POR MALWARE

1. Virus
2. Troyanos
3. Gusanos
4. *Software* espía o *spyware*
5. Apps maliciosas
6. *Adware*
7. *Botnets*

8. *Rogueware*
9. *Criptojacking*

RESUMEN

AUTOEVALUACIÓN

MÓDULO 6. VULNERABILIDADES

UNIDAD DIDÁCTICA 1. ¿QUÉ SON LAS VULNERABILIDADES?

UNIDAD DIDÁCTICA 2. COMMON VULNERABILITY SCORING SYSTEM (CVSS)

1. Métricas base
 - Acceso vectorial (AV)
 - Complejidad de acceso (AC)
 - Autenticación (AC)
 - Impactos
2. Métricas temporales
 - Explotabilidad (E)
 - Nivel de remediación (RL)
 - Informe de confianza (RC)
3. Métricas ambientales
 - Daño potencial colateral
 - Distribución de objetivos
 - Requisitos de confidencialidad, integridad y disponibilidad
4. Cálculo CVSS tras el establecimiento de las métricas

UNIDAD DIDÁCTICA 3. PRINCIPALES TIPOS DE VULNERABILIDADES

1. *Buffer overflow* o desbordamiento de *buffer*
2. Condición de carrera
3. Error de formato en cadenas
4. *Cross site scripting*
5. Inyección de SQL
6. Control de acceso débil
7. Denegación de servicio

RESUMEN

AUTOEVALUACIÓN

MÓDULO 7. ANÁLISIS Y GESTIÓN DE VULNERABILIDADES, RIESGOS Y ATAQUES

UNIDAD DIDÁCTICA 1. ¿QUE ENGLOBA LA GESTIÓN DE RIESGOS?

1. Análisis de riesgos
2. Tratamiento de riesgos

UNIDAD DIDÁCTICA 2. MEDICIÓN DEL RIESGO

1. Nivel de peligrosidad del ciberincidente
2. Niveles de notificación obligatoria

UNIDAD DIDÁCTICA 3. FASES DE LA GESTIÓN DE CIBERINCIDENTES

1. Preparación

2. Identificación
3. Contención
4. Mitigación
5. Recuperación
6. Actuaciones tras el incidente

UNIDAD DIDÁCTICA 4. POLÍTICA DE GESTIÓN DE RIESGOS

1. Política de protección de datos
2. Política de contraseñas
3. Política de actualizaciones
4. Política de almacenamiento y copias de seguridad
5. Política sobre el uso de equipos, aplicaciones y correo electrónico
6. Política sobre el uso de redes inalámbricas
7. Políticas de clasificación de la información

RESUMEN

AUTOEVALUACIÓN

MÓDULO 8. ANÁLISIS FORENSE

UNIDAD DIDÁCTICA 1. ¿EN QUÉ CONSISTE UN ANÁLISIS FORENSE?

1. Principios
2. Fases
 - Recogida de información
 - Análisis
 - Redacción del informe

UNIDAD DIDÁCTICA 2. EVIDENCIAS DIGITALES

1. Cadena de custodia
2. Evidencias *online* y *offline*
3. Datos volátiles y datos estáticos
4. Pautas generales de recolección de evidencias

UNIDAD DIDÁCTICA 3. ANÁLISIS FORENSE SEGÚN EL SISTEMA OPERATIVO

1. Windows
2. MacOS
3. Linux

UNIDAD DIDÁCTICA 4. ANÁLISIS FORENSE DE REDES

UNIDAD DIDÁCTICA 5. ANÁLISIS FORENSE DE WEBS

UNIDAD DIDÁCTICA 6. OTRAS APLICACIONES DEL ANÁLISIS FORENSE

1. Análisis de dispositivos móviles
2. Análisis de bases de datos
3. Análisis de correo electrónico
4. Análisis en entornos *cloud*

UNIDAD DIDÁCTICA 7. RECUPERACIÓN DE ARCHIVOS

RESUMEN

AUTOEVALUACIÓN

MÓDULO 9. HACKING ÉTICO

UNIDAD DIDÁCTICA 1. ¿QUÉ ES EL HACKING ÉTICO?

1. Perfil del *hacker* ético
2. Beneficios

UNIDAD DIDÁCTICA 2. ETAPAS DEL HACKING ÉTICO

1. Planificación
2. Reconocimiento
3. Acceso y análisis
4. Documentación del proceso
5. Análisis tras la aplicación de las vulnerabilidades reportadas

RESUMEN

AUTOEVALUACIÓN

MÓDULO 10. SEGURIDAD DE LA INFORMACIÓN

UNIDAD DIDÁCTICA 1. CONCEPTO DE SEGURIDAD DE LA INFORMACIÓN

UNIDAD DIDÁCTICA 2. FUNDAMENTOS DE LA SEGURIDAD DE LA INFORMACIÓN

1. Confidencialidad
2. Integridad
3. Disponibilidad
4. Autenticidad y no repudio
5. Trazabilidad

UNIDAD DIDÁCTICA 3. GESTIÓN INTERNA O EXTERNA DE LA SEGURIDAD

UNIDAD DIDÁCTICA 4. CONTROLES DE SEGURIDAD

1. Controles preventivos
2. Controles de detección
3. Controles correctivos
4. Controles de monitorización

RESUMEN

AUTOEVALUACIÓN

MÓDULO 11. SEGURIDAD WEB Y DE SISTEMAS

UNIDAD DIDÁCTICA 1. PROTOCOLO HTTP/HTTPS

UNIDAD DIDÁCTICA 2. INYECCIONES

1. HTML
2. iFrame
3. SQL

UNIDAD DIDÁCTICA 3. CONTROL DE ACCESOS Y AUTENTICACIÓN

UNIDAD DIDÁCTICA 4. CICLO DE VIDA DE DESARROLLO DE SOFTWARE

SEGURO (SDLC)

UNIDAD DIDÁCTICA 5. SEGURIDAD EN LA NUBE

UNIDAD DIDÁCTICA 6. SEGURIDAD EN EL *BIG DATA*

RESUMEN

AUTOEVALUACIÓN

MÓDULO 12. SEGURIDAD IoT

UNIDAD DIDÁCTICA 1. INTERNET DE LAS COSAS (IoT)

1. Arquitectura IoT

UNIDAD DIDÁCTICA 2. CIBERSEGURIDAD EN DISPOSITIVOS IoT

1. Amenazas en dispositivos IoT
 - Deficiencias en la transmisión de datos
 - Deficiencias en el *hardware*
 - Deficiencias en el *software*
 - Deficiencias en la configuración
2. Evaluación de la seguridad de IoT

UNIDAD DIDÁCTICA 3. MANTENIMIENTO DE LA SEGURIDAD DE IoT

RESUMEN

AUTOEVALUACIÓN

MÓDULO 13. SEGURIDAD EN REDES

UNIDAD DIDÁCTICA 1. PROTOCOLOS TCP/IP

UNIDAD DIDÁCTICA 2. CORTAFUEGOS

UNIDAD DIDÁCTICA 3. SISTEMAS Y HERRAMIENTAS DE PROTECCIÓN DE REDES

1. SIEM
2. IDS
3. IPS
4. DLP
5. VPN

UNIDAD DIDÁCTICA 4. SEGURIDAD EN REDES INALÁMBRICAS

1. *Wired equivalent privacy* (WEP)
2. *Wifi protected access* (WPA)
 - WPA
 - WPA 2
 - WPA3

RESUMEN

AUTOEVALUACIÓN

MÓDULO 14. ASPECTOS LEGISLATIVOS

UNIDAD DIDÁCTICA 1. INTRODUCCIÓN AL DERECHO ESPAÑOL

UNIDAD DIDÁCTICA 2. PROTECCIÓN DE DATOS

UNIDAD DIDÁCTICA 3. REAL DECRETO 43/2021, DE 26 DE ENERO

UNIDAD DIDÁCTICA 4. ESQUEMA NACIONAL DE SEGURIDAD

UNIDAD DIDÁCTICA 5. CIBERDELINCUENCIA EN EL DERECHO PENAL

RESUMEN

AUTOEVALUACIÓN

SOLUCIONARIO

BIBLIOGRAFÍA COMPLEMENTARIA

PARTE 2

ÁMBITOS DE LA SEGURIDAD NACIONAL: CIBERSEGURIDAD

I. PROTECCIÓN DE DATOS

1. Real Decreto 389/2021, de 1 de junio, por el que se aprueba el Estatuto de la Agencia Española de Protección de Datos
2. Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales
3. Ley Orgánica 7/2021, de 26 de mayo, de protección de datos personales tratados para fines de prevención, detección, investigación y enjuiciamiento de infracciones penales y de ejecución de sanciones penales
4. Real Decreto-ley 12/2018, de 7 de septiembre, de seguridad de las redes y sistemas de información. [Inclusión parcial]
5. Real Decreto-ley 14/2019, de 31 de octubre, por el que se adoptan medidas urgentes por razones de seguridad pública en materia de administración digital, contratación del sector público y telecomunicaciones
6. Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas. [Inclusión parcial]
7. Instrucción 1/2006, de 8 de noviembre, de la Agencia Española de Protección de Datos, sobre el tratamiento de datos personales con fines de vigilancia a través de sistemas de cámaras o videocámaras
8. Resolución de 9 de marzo de 2016, de la Presidencia de la Comisión Nacional de los Mercados y la Competencia, por la que se crea el fichero de datos de carácter personal "Registro de grupos de interés"

II. CIBERAMENAZAS Y SEGURIDAD EN EL CIBERESPACIO. COOPERACIÓN EN MATERIA DE SEGURIDAD

1. Real Decreto-ley 12/2018, de 7 de septiembre, de seguridad de las redes y sistemas de información
2. Real Decreto 43/2021, de 26 de enero, por el que se desarrolla el Real Decreto-ley 12/2018, de 7 de septiembre, de seguridad de las redes y sistemas de información
3. Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad
4. Orden ESS/775/2014, de 7 de mayo, por la que se crea el Comité de Seguridad de los Sistemas de Información de la Seguridad Social
5. Orden PRA/33/2018, de 22 de enero, por la que se publica el Acuerdo del Consejo de Seguridad Nacional, por el que se regula el Consejo Nacional de Ciberseguridad
6. Orden PCI/487/2019, de 26 de abril, por la que se publica la Estrategia Nacional de Ciberseguridad 2019, aprobada por el Consejo de Seguridad Nacional

III. INFRAESTRUCTURAS CRÍTICAS EN ESPAÑA

1. Resolución de 8 de septiembre de 2015, de la Secretaría de Estado de Seguridad, por la que se aprueban los nuevos contenidos mínimos de los Planes de Seguridad del Operador y de los Planes de Protección Específicos
2. Ley 8/2011, de 28 de abril, por la que se establecen medidas para la protección de las infraestructuras críticas
3. Real Decreto 704/2011, de 20 de mayo, por el que se aprueba el Reglamento de protección de las infraestructuras críticas

IV. USO EFICIENTE DE LAS TECNOLOGÍAS DE LA INFORMACIÓN

1. Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad