INESEM

BUSINESS SCHOOL

Curso Experto en Protección Tecnológica para Empresarios + Titulación Universitaria

+ Información Gratis

titulación de formación continua bonificada expedida por el instituto europeo de estudios empresariales

Curso Experto en Protección Tecnológica para Empresarios + Titulación Universitaria

duración total: 450 horas ***horas teleformación:*** 225 horas

precio: 0 € *

modalidad: Online

* hasta 100 % bonificable para trabajadores.

descripción

El efecto de las nuevas tecnologías ha provocado una creciente necesidad de transformación en todos los ámbitos, y la empresa no es excepción. Los empresarios deben tener conocimientos en nuevas tecnologías, el desempeño de su función debe responder a esta transformación social y económica al considerando las distintas disposiciones legales y, al mismo tiempo, la seguridad informática.

a quién va dirigido

Todos aquellos trabajadores y profesionales en activo que deseen adquirir o perfeccionar sus conocimientos técnicos en este área.

objetivos

- Conocimiento actualizado del régimen jurídico del secreto empresarial.
- Afianzar los conocimientos teóricos sobre propiedad intelectual aplicados al entorno online.
- Aplicar correctamente en el funcionamiento de la Empresa las previsiones del Reglamento (UE) 2016/679.
- Aprender a diseñar la política de seguridad informativa de la empresa o departamento.
- Conocer la figura del Compliance Officer.
- Identificar los riesgos de la empresa dentro de su ámbito normativo.
- Reconocer las vulnerabilidades y los posibles ataques a las redes y a los sistemas libres.
- Conocer los principales sistemas para la protección de la información en las redes y sistemas telemáticos.

para qué te prepara

El Curso Experto en Protección Tecnológica para Empresarios te aporta los conocimientos necesarios para establecer políticas y procedimientos en la empresa adecuados y suficientes para garantizar que cumple el marco normativo aplicable. Además, te formará en las principales herramientas, técnicas y legislación en torno a la seguridad informática en empresas y organizaciones.

salidas laborales

- Experto en nuevas tecnologías.
- Asesor Propiedad Intelectual especialmente en el entorno online.
- Abogado In-house o Of-counsel de Empresas.
- Delegado de protección de datos (DPD).
- Compliance Officer.
- Responsable del dpto. de cumplimiento.
- Director en ciberseguridad.
- Director de Seguridad Corporativa.

titulación

Una vez finalizado el curso, el alumno recibirá por parte de INESEM vía correo postal, la Titulación Oficial que acredita el haber superado con éxito todas las pruebas de conocimientos propuestas en el mismo.

Esta titulación incluirá el nombre del curso/máster, la duración del mismo, el nombre y DNI del alumno, el nivel de aprovechamiento que acredita que el alumno superó las pruebas propuestas, las firmas del profesor y Director del centro, y los sellos de la instituciones que avalan la formación recibida (Instituto Europeo de Estudios Empresariales).

INSTITUTO EUROPEO DE ESTUDIOS EMPRESARIALES

como centro de Formación acreditado para la impartición a nivel nacional de formación
EXPIDE LA SIGUIENTE TITULACIÓN

NOMBRE DEL ALUMNO/A

con D.N.I. XXXXXXXX ha superado los estudios correspondientes de

Nombre de la Acción Formativa

de XXX horas, perteneciente al Plan de Formación INESEM en la convocatoria de XXXX
Y para que surta los efectos pertinentes queda registrado con número de expediente XXXX- XXXX-XXXX-XXXXXX

Con una calificación de SOBRESALIENTE

Y para que conste expido la presente TITULACIÓN en
Granada, a (día) de (mes) de (año)

La direccion General

MARIA MORENO HIDALGO

Sello

Firma del alumno/a

NOMBRE DEL ALUMNO/A

forma de bonificación

- Mediante descuento directo en el TC1, a cargo de los seguros sociales que la empresa paga cada mes a la Seguridad Social.

metodología

El alumno comienza su andadura en INESEM a través del Campus Virtual. Con nuestra metodología de aprendizaje online, el alumno debe avanzar a lo largo de las unidades didácticas del itinerario formativo, así como realizar las actividades y autoevaluaciones correspondientes. Al final del itinerario, el alumno se encontrará con el examen final, debiendo contestar correctamente un mínimo del 75% de las cuestiones planteadas para poder obtener el título.

Nuestro equipo docente y un tutor especializado harán un seguimiento exhaustivo, evaluando todos los progresos del alumno así como estableciendo una línea abierta para la resolución de consultas.

El alumno dispone de un espacio donde gestionar todos sus trámites administrativos, la Secretaría Virtual, y de un lugar de encuentro, Comunidad INESEM, donde fomentar su proceso de aprendizaje que enriquecerá su desarrollo profesional.

materiales didácticos

- Manual teórico 'Compliance Officer Vol. 1'
- Manual teórico 'Ciberseguridad: Gestión y Herramientas'
- Manual teórico 'Ciberseguridad: Gestión de Incidentes de Seguridad Informática'
- Manual teórico 'Protección de Datos y Derechos Digitales'
- Manual teórico 'Know-How, Propiedad Intelectual e Industrial en un Mercado Digital Global'
- Manual teórico 'Compliance Officer Vol. 2'

profesorado y servicio de tutorías

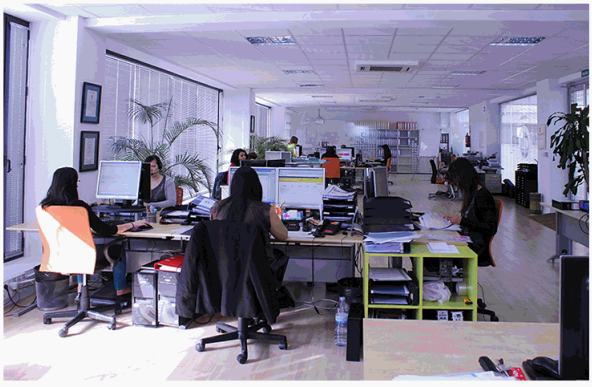
Nuestro equipo docente estará a su disposición para resolver cualquier consulta o ampliación de contenido que pueda necesitar relacionado con el curso. Podrá ponerse en contacto con nosotros a través de la propia plataforma o Chat, Email o Teléfono, en el horario que aparece en un documento denominado “Guía del Alumno” entregado junto al resto de materiales de estudio. Contamos con una extensa plantilla de profesores especializados en las distintas áreas formativas, con una amplia experiencia en el ámbito docente.

El alumno podrá contactar con los profesores y formular todo tipo de dudas y consultas, así como solicitar información complementaria, fuentes bibliográficas y asesoramiento profesional. Podrá hacerlo de las siguientes formas:

- **Por e-mail**: El alumno podrá enviar sus dudas y consultas a cualquier hora y obtendrá respuesta en un plazo máximo de 48 horas.

- **Por teléfono**: Existe un horario para las tutorías telefónicas, dentro del cual el alumno podrá hablar directamente con su tutor.

- **A través del Campus Virtual**: El alumno/a puede contactar y enviar sus consultas a través del mismo, pudiendo tener acceso a Secretaría, agilizando cualquier proceso administrativo así como disponer de toda su documentación



plazo de finalización

El alumno cuenta con un período máximo de tiempo para la finalización del curso, que dependerá de la misma duración del curso. Existe por tanto un calendario formativo con una fecha de inicio y una fecha de fin.

campus virtual online

especialmente dirigido a los alumnos matriculados en cursos de modalidad online, el campus virtual de inesem ofrece contenidos multimedia de alta calidad y ejercicios interactivos.

comunidad

servicio gratuito que permitirá al alumno formar parte de una extensa comunidad virtual que ya disfruta de múltiples ventajas: becas, descuentos y promociones en formación, viajes al extranjero para aprender idiomas...

revista digital

el alumno podrá descargar artículos sobre e-learning, publicaciones sobre formación a distancia, artículos de opinión, noticias sobre convocatorias de oposiciones, concursos públicos de la administración, ferias sobre formación, etc.

secretaría

Este sistema comunica al alumno directamente con nuestros asistentes, agilizando todo el proceso de matriculación, envío de documentación y solución de cualquier incidencia.

Además, a través de nuestro gestor documental, el alumno puede disponer de todos sus documentos, controlar las fechas de envío, finalización de sus acciones formativas y todo lo relacionado con la parte administrativa de sus cursos, teniendo la posibilidad de realizar un seguimiento personal de todos sus trámites con INESEM

programa formativo

MÓDULO 1. KNOW-HOW, PROPIEDAD INTELECTUAL E INDUSTRIAL EN UN MERCADO DIGITAL GLOBAL

UNIDAD DIDÁCTICA 1. INTRODUCCIÓN AL KNOW-HOW

1.Introducción teórica al concepto de know-how
2.Entorno de Innovación Abierta
3.Política de Gestión de Propiedad Intelectual e Industrial
4.Gestión de Propiedad Intelectual e Industrial en Proyectos de I+D+I
5.Patent Box

UNIDAD DIDÁCTICA 2. SECRETOS EMPRESARIALES E INFORMACIÓN CONFIDENCIAL

1.Jurisdicción Europea Y Española
2.Relevancia del secreto
3.Requisitos del secreto empresarial

UNIDAD DIDÁCTICA 3. PROTECCIÓN DEL KNOW-HOW

1.Gestión de la protección
2.Protección de la Propiedad Intelectual e Industrial en la era digital
3.Gestión de la Propiedad Intelectual e Industrial en explotación y defensa
4.Non Disclosure Agreement (NDA)

UNIDAD DIDÁCTICA 4. INTERACCIÓN ENTRE LA LSSI Y LA LEY DE PROPIEDAD INTELECTUAL

1.Ley de Servicios de la Sociedad de la Información y Ley de Propiedad Intelectual: una doble perspectiva
2.Derechos de propiedad intelectual sobre las páginas web
3.Acceso a contenidos desde la perspectiva de la LSSI
4.La Ley Sinde: Ley 2/2011, de 4 de marzo, de Economía Sostenible
5.Impacto de la Reforma
6.Reforma del TRLGDCU impacto en los negocios online

UNIDAD DIDÁCTICA 5. PATENTES, DISEÑOS INDUSTRIALES Y MODELOS DE UTILIDAD

1.Requisitos de una patente
2.Clases de patentes
3.Procedimiento de registro de patentes
4.Diseños industriales
5.Modelos de utilidad

UNIDAD DIDÁCTICA 6. MARCA NACIONAL Y NOMBRES COMERCIALES

1.Marco normativo La Ley 17/2001, de 7 de diciembre, de Marcas
2.Concepto de marca
3.Clases de marcas
4.Concepto de nombre comercial
5.Prohibiciones absolutas de registro
6.Prohibiciones relativas de registro
7.Marca notoria y marca renombrada
8.Marcas colectivas y de garantía

UNIDAD DIDÁCTICA 7. NOMBRES DE DOMINIO

1.Clases de nombres de dominio
2.Conflictos en nombres de dominio

UNIDAD DIDÁCTICA 8. INTRODUCCIÓN AL BIG DATA

1.¿Qué es Big Data?
2.La era de las grandes cantidades de información: historia del big data
3.La importancia de almacenar y extraer información
4.Big Data enfocado a los negocios
5.Open Data

6.Información pública
7.IoT (Internet of Things - Internet de las cosas)

MÓDULO 2. PROTECCIÓN DE DATOS Y DERECHOS DIGITALES

UNIDAD DIDÁCTICA 1. PROTECCIÓN DE DATOS: CONTEXTO NORMATIVO

1.Normativa General de Protección de Datos
2.Privacidad y protección de datos en el panorama internacional
3.La Protección de Datos en Europa
4.La Protección de Datos en España
5.Estándares y buenas prácticas

UNIDAD DIDÁCTICA 2. REGLAMENTO EUROPEO DE PROTECCIÓN DE DATOS (RGPD). FUNDAMENTOS

1.El Reglamento UE 2016/679
2.Ámbito de aplicación del RGPD
3.Definiciones
4.Sujetos obligados
5.Ejercicio Resuelto. Ámbito de Aplicación

UNIDAD DIDÁCTICA 3. PRINCIPIOS DE LA PROTECCIÓN DE DATOS

1.El binomio derecho/deber en la protección de datos
2.Licitud del tratamiento de los datos
3.Lealtad y transparencia
4.Finalidad del tratamiento de los datos: la limitación
5.Minimización de datos
6.Exactitud y Conservación de los datos personales

UNIDAD DIDÁCTICA 4. LEGITIMACIÓN PARA EL TRATAMIENTO DE LOS DATOS PERSONALES EN EL RGPD

1.El consentimiento del interesado en la protección de datos personales
2.El consentimiento: otorgamiento y revocación
3.El consentimiento informado: finalidad, transparencia, conservación, información y deber de comunicación al interesado
4.Eliminación del Consentimiento tácito en el RGPD
5.Consentimiento de los niños
6.Categorías especiales de datos
7.Datos relativos a infracciones y condenas penales
8.Tratamiento que no requiere identificación
9.Bases jurídicas distintas del consentimiento

UNIDAD DIDÁCTICA 5. DERECHOS DE LOS CIUDADANOS EN LA PROTECCIÓN DE SUS DATOS PERSONALES

1.Derechos de las personas respecto a sus Datos Personales
2.Transparencia e Información
3.Acceso, Rectificación, Supresión (Olvido)
4.Oposición
5.Decisiones individuales automatizadas
6.Portabilidad de los Datos
7.Limitación del tratamiento
8.Excepciones a los derechos
9.Casos específicos
10.Ejercicio resuelto. Ejercicio de Derechos por los Ciudadanos

UNIDAD DIDÁCTICA 6. PROTECCIÓN DE DATOS DE CARÁCTER PERSONAL: MEDIDAS DE CUMPLIMIENTO EN EL RGPD

1.Las políticas de Protección de Datos
2.Posición jurídica de los intervinientes. Responsables, corresponsables, Encargados, subencargado del Tratamien y sus representantes. Relaciones entre ellos y formalización
3.El Registro de Actividades de Tratamiento: identificación y clasificación del tratamiento de datos

UNIDAD DIDÁCTICA 7. LA RESPONSABILIDAD PROACTIVA

1.El Principio de Responsabilidad Proactiva
2.Privacidad desde el Diseño y por Defecto. Principios fundamentales
3.Evaluación de Impacto relativa a la Protección de Datos (EIPD) y consulta previa. Los Tratamientos de Alto Riesg
4.Seguridad de los datos personales. Seguridad técnica y organizativa
5.Las Violaciones de la Seguridad. Notificación de Violaciones de Seguridad
6.El Delegado de Protección de Datos (DPD). Marco normativo
7.Códigos de conducta y certificaciones

UNIDAD DIDÁCTICA 8. TRANSFERENCIAS INTERNACIONALES DE DATOS EN EL RGPD

1.El Movimiento Internacional de Datos
2.El sistema de decisiones de adecuación
3.Transferencias mediante garantías adecuadas
4.Normas Corporativas Vinculantes
5.Excepciones
6.Autorización de la autoridad de control
7.Suspensión temporal
8.Cláusulas contractuales

UNIDAD DIDÁCTICA 9. LAS AUTORIDADES DE CONTROL

1.Autoridades de Control: Aproximación
2.Potestades
3.Régimen Sancionador
4.Comité Europeo de Protección de Datos (CEPD)
5.Procedimientos seguidos por la AEPD
6.La Tutela Jurisdiccional
7.El Derecho de Indemnización

UNIDAD DIDÁCTICA 10. DERECHOS DIGITALES RELACIONADOS CON LA PROTECCIÓN DE DATOS

1.Derecho de Rectificación en Internet
2.Derecho a la Actualización de informaciones en medios de comunicación digitales
3.Derecho al Olvido en búsquedas de Internet
    1.- Derecho al Olvido en Google
    2.- Proceso ante Google

UNIDAD DIDÁCTICA 11. DERECHOS DIGITALES DE LOS TRABAJADORES

1.Derecho a la intimidad y uso de dispositivos digitales en el ámbito laboral
2.Derecho a la desconexión digital en el ámbito laboral
3.Derecho a la intimidad frente al uso de dispositivos de video-vigilancia y de grabación de sonido en el lugar de trabajo
4.Derecho a la intimidad ante la utilización de sistemas de geolocalización en el ámbito laboral
    1.- Medidas de seguridad sobre los datos de geolocalización
    2.- La Geolocalización acorde con la Agencia Española de Protección de Datos
5.Ejercicio resuelto: Geolocalización acorde con la AEPD
6.Derechos digitales en la negociación colectiva

UNIDAD DIDÁCTICA 12. DERECHOS DIGITALES DE LOS MENORES DE EDAD

1.Protección de los menores en Internet
2.Protección de datos de los menores en Internet
    1.- Tratamiento de datos por los centros educativos
    2.- Tratamiento de datos por Asociaciones de Madres y Padres de Alumnos (AMPA)
3.Ejercicio resuelto: Tratamiento de datos por Asociaciones de Madres y Padres de Alumnos (AMPA)

UNIDAD DIDÁCTICA 13. CUESTIONES PRÁCTICAS SOBRE DERECHOS DIGITALES

1.Video tutorial: Introducción a la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales
2.Video tutorial: Esquema normativo de Derechos Digitales
3.Sentencias Imprescindibles de Derechos Digitales

MÓDULO 3. CIBERSEGURIDAD: SEGURIDAD DESDE EL PUNTO DE VIST EMPRESARIAL Y TÉCNICO (HOMOLOGADO + 8 CRÉDITOS ECTS)

UNIDAD FORMATIVA 1. CIBERSEGURIDAD: GESTIÓN Y HERRAMIENTAS

UNIDAD DIDÁCTICA 1. GESTIÓN Y HERRAMIENTAS DE CIBERSEGURIDAD: INTRODUCCIÓN Y CONCEPTOS BÁSICOS

1.La sociedad de la información
- 1.- ¿Qué es la seguridad de la información?
- 2.- Importancia de la seguridad de la información

2.Seguridad de la información: Diseño, desarrollo e implantación
- 1.- Descripción de los riesgos de la seguridad
- 2.- Selección de controles

3.Factores de éxito en la seguridad de la información

4.Vídeo tutorial: relación entre la ciberseguridad y el Big Data

UNIDAD DIDÁCTICA 2. NORMATIVA SOBRE EL SISTEMA DE GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN (SGSI)

1.Estándares y Normas Internacionales sobre los SGSI
- 1.- Familia de Normas ISO 27000
- 2.- La Norma UNE-EN-ISO/IEC 27001:2014
- 3.- Buenas prácticas en seguridad de la información, Norma ISO/IEC 27002

2.Normativa aplicable a los SGSI
- 1.- Normativa comunitaria sobre seguridad de la información
- 2.- Legislación Española sobre seguridad de la información
- 3.- El Instituto Nacional de Ciberseguridad (INCIBE)

UNIDAD DIDÁCTICA 3. POLÍTICA DE SEGURIDAD: ANÁLISIS Y GESTIÓN DE RIESGOS

1.Plan de implantación del SGSI

2.Análisis de riesgos
- 1.- Análisis de riesgos: Aproximación
- 2.- Principales tipos de vulnerabilidades, fallos de programa, programas maliciosos y su actualización permanent 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
- 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 riesg 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

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. AUDITORÍA DE CIBERSEGURIDAD

1.Criterios Generales en la Auditoría de Seguridad de la Informática
1.- Código deontológico de la función de auditoría
2.- Relación de los distintos tipos de auditoría en el marco de los sistemas de información
3.- Criterios a seguir para la composición del equipo auditor
4.- Tipos de pruebas a realizar en el marco de la auditoría, pruebas sustantivas y pruebas de cumplimiento
5.- Tipos de muestreo a aplicar durante el proceso de auditoría
6.- Utilización de herramientas tipo CAAT (Computer Assisted Audit Tools)
7.- Explicación de los requerimientos que deben cumplir los hallazgos de auditoría
8.- Aplicación de criterios comunes para categorizar los hallazgos como observaciones o no conformidades
9.- Relación de las normativas y metodologías relacionadas con la auditoría de sistemas de información comúnmente aceptadas

2.Aplicación de la normativa de protección de datos de carácter personal
1.- Normativa de referencia: Reglamento General de Protección de Datos y Ley Orgánica de Protección de Datos 3/2018
2.- Principios generales de la protección de datos de carácter personal
3.- Legitimación para el tratamiento de datos personales
4.- Medidas de responsabilidad proactiva
5.- Los derechos de los interesados
6.- Delegado de Protección de Datos

3.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

4.Descripción de los aspectos sobre cortafuego en auditorías de sistemas de información
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.Guías para la ejecución de las distintas fases de la auditoría de sistemas de información
1.- Normas para la implantación de la auditoría de la documentación
2.- Instrucciones para la elaboración del plan de auditoría
3.- Pruebas de auditoría
4.- Instrucciones para la elaboración del informe de auditoría

UNIDAD DIDÁCTICA 5. COMUNICACIONES SEGURAS: SEGURIDAD POR NIVELES

1.Seguridad a nivel físico
1.- Tipos de ataques
2.- Servicios de Seguridad
3.- Medidas de seguridad a adoptar

2.Seguridad a nivel de enlace
1.- Tipos de ataques
2.- Medidas de seguridad a adoptar

3.Seguridad a nivel de red
1.- Datagrama IP
2.- Protocolo IP
3.- Protocolo ICMP

4.- Protocolo IGMP
5.- Tipos de Ataques
6.- Medidas de seguridad a adopta
4.Seguridad a nivel de transporte
1.- Protocolo TCP
2.- Protocolo UDP
3.- Tipos de Ataques
4.- Medidas de seguridad a adoptar
5.Seguridad a nivel de aplicación
1.- Protocolo DNS
2.- Protocolo Telnet
3.- Protocolo FTP
4.- Protocolo SSH
5.- Protocolo SMTP
6.- Protocolo POP
7.- Protocolo IMAP
8.- Protocolo SNMP
9.- Protocolo HTTP
10.- Tipos de Ataques
11.- Medidas de seguridad a adoptar

UNIDAD FORMATIVA 2. CIBERSEGURIDAD: GESTIÓN DE INCIDENTES DE SEGURIDAD INFORMÁTICA

UNIDAD DIDÁCTICA 1. SISTEMAS DE DETECCIÓN Y PREVENCIÓN DE INTRUSIONES (IDS/IPS)

1.Conceptos generales de gestión de incidentes, detección de intrusiones y su prevención
2.Identificación y caracterización de los datos de funcionamiento del sistema
3.Arquitecturas más frecuentes de los IDS
4.Relación de los distintos tipos de IDS/IPS por ubicación y funcionalidad
5.Criterios de seguridad para el establecimiento de la ubicación de los IDS/IPS

UNIDAD DIDÁCTICA 2. IMPLANTACIÓN Y PUESTA EN PRODUCCIÓN DE SISTEMAS IDS/IPS

1.Análisis previo
2.Definición de políticas de corte de intentos de intrusión en los IDS/IPS
3.Análisis de los eventos registrados por el IDS/IPS
4.Relación de los registros de auditoría del IDS/IPS
5.Establecimiento de los niveles requeridos de actualización, monitorización y pruebas del IDS/IPS

UNIDAD DIDÁCTICA 3. CONTROL MALWARE

1.Sistemas de detección y contención de Malware
2.Herramientas de control de Malware
3.Criterios de seguridad para la configuración de las herramientas de protección frente a Malware
4.Determinación de los requerimientos y técnicas de actualización de las herramientas de protección frente a Malwa
5.Relación de los registros de auditoría de las herramientas de protección frente a Malware
6.Establecimiento de la monitorización y pruebas de las herramientas de protección frente a Malware
7.Análisis de Malware mediante desensambladores y entornos de ejecución controlada

UNIDAD DIDÁCTICA 4. RESPUESTA ANTE INCIDENTES DE SEGURIDAD

1.Procedimiento de recolección de información relacionada con incidentes de seguridad
2.Exposición de las distintas técnicas y herramientas utilizadas para el análisis y correlación de información y evento de seguridad
3.Proceso de verificación de la intrusión
4.Naturaleza y funciones de los organismos de gestión de incidentes tipo CERT nacionales e internacionales

UNIDAD DIDÁCTICA 5. PROCESO DE NOTIFICACIÓN Y GESTIÓN DE INTENTOS DE INTRUSIÓN

1.Establecimiento de las responsabilidades
2.Categorización de los incidentes derivados de intentos de intrusión

3.Establecimiento del proceso de detección y herramientas de registro de incidentes
4.Establecimiento del nivel de intervención requerido en función del impacto previsible
5.Establecimiento del proceso de resolución y recuperación de los sistemas
1.- Respaldo y recuperación de los datos
2.- Actualización del Plan de Recuperación
3.- Errores comunes al formular un DRP
6.Proceso para la comunicación del incidente a terceros

UNIDAD DIDÁCTICA 6. ANÁLISIS FORENSE INFORMÁTICO

1.Conceptos generales y objetivos del análisis forense
1.- Tipos de análisis forense
2.Exposición del Principio de Lockard
3.Guía para la recogida de evidencias electrónicas
1.- Evidencias volátiles y no volátiles
2.- Etiquetado de evidencias
3.- Cadena de custodia
4.- Ficheros y directorios ocultos
5.- Información oculta del sistema
6.- Recuperación de ficheros borrados
4.Guía para el análisis de las evidencias electrónicas recogidas
5.Guía para la selección de las herramientas de análisis forense

MÓDULO 4. COMPLIANCE OFFICER

UNIDAD FORMATIVA 1. DOMINIO 1. MARCO LEGAL E INTERNACIONAL Y ANTECEDENTES DEL COMPLIANCE

UNIDAD DIDÁCTICA 1. MARCO LEGAL NACIONAL E INTERNACIONAL Y ANTECEDENTES DEL COMPLIANCE

1.FCPA
2.Committee of Sponsoring Organizations of the treadway Commission (COSO), COSO III
3.Sentencing reform Act
4.Ley Sarbanes-Oxley
5.OCDE. Convenio Anticohecho
6.Convenio de las Naciones Unidas contra la corrupción y el sector privado
7.Normativa de Italia. Decreto Legislativo nº231, de 8 de junio de 2001
8.Normativa de Reino Unido. UKBA
9.Normativa de Francia. Ley Sapin II

UNIDAD DIDÁCTICA 2. COMPLIANCE EN LA EMPRESA

1.Gobierno Corporativo
2.El Compliance en la empresa
3.Relación del Compliance con otras áreas de la empresa

UNIDAD DIDÁCTICA 3. APROXIMACIÓN AL COMPLIANCE PROGRAM

1.Beneficios para mi empresa del Compliance Program
2.Ámbito de actuación
3.Materias incluídas en un programa de cumplimiento
4.Normativa del Sector Farmacéutico

UNIDAD FORMATIVA 2. DOMINIO 2. SISTEMAS DE GESTIÓN DEL RIESGO

UNIDAD DIDÁCTICA 1. EVALUACIÓN DE RIESGOS

1.Concepto general de riesgo empresarial
2.Tipos de riesgos en la empresa
3.Identificación de los riesgos en la empresa
4.Estudio de los riesgos
5.Impacto y probabilidad de los riesgos en la empresa
6.Evaluación de los riesgos

UNIDAD DIDÁCTICA 2. CONTROLES DE RIESGOS
1.Políticas y procedimientos
2.Controles de Procesos
3.Controles de Organización
4.Código Ético
5.Cultura de Cumplimiento

UNIDAD DIDÁCTICA 3. CONTROLES INTERNOS EN LA EMPRESA
1.Concepto de Controles Internos
2.Realización de Controles e Implantación
3.Plan de Monitorización
4.Medidas de Control de acceso físicas y de acceso lógico
5.Otras medidas de control

UNIDAD DIDÁCTICA 4. SISTEMAS DE GESTIÓN DEL RIESGO (ISO 31000:2018)
1.Descripción General de la Norma ISO 31000 Risk Management
2.Términos y definiciones de la norma ISO 31000
3.Principios de la norma ISO 31000
4.Marco de referencia de la norma ISO 31000
5.Procesos de la norma ISO 31000

UNIDAD FORMATIVA 3. DOMINIO 3. SISTEMAS DE GESTIÓN ANTISOBORNO

UNIDAD DIDÁCTICA 1. SISTEMAS DE GESTIÓN ANTISOBORNO (ISO 37001:2016)
1.Descripción general de la norma ISO 37001
2.Términos y definiciones de la norma ISO 37001
3.Contexto de la organización según la norma ISO 37001
4.Liderazgo en la norma ISO 37001
5.Planificación en la norma ISO 37001
6.Apoyo según la norma ISO 37001
7.Operación en base a la norma ISO 37001
8.Evaluación del desempeño según la norma ISO 37001
9.Mejora según la norma ISO 37001

UNIDAD FORMATIVA 4. DOMINIO 4. PROFUNDO CONOCIMIENTO EN MATERIA LEGAL NACIONAL E INTERNACIONAL DE LA RESPONSABILIDAD PENAL (O ASIMILADA) DE LA PERSONA JURÍDICA, CRITERIOS DE APLICACIÓN, ATENUACIÓN Y EXONERACIÓN

UNIDAD DIDÁCTICA 1. NORMATIVA INTERNACIONAL DE LA RESPONSABILIDAD PENAL DE LAS PERSONAS JURÍDICAS
1.Contexto histórico internacional
2.Modelos de responsabilidad de la persona jurídica
3.Derecho comparado en materia de responsabilidad penal de las personas jurídicas
4.Compatibilidad de sanciones penales y administrativas. Principio non bis in ídem

UNIDAD DIDÁCTICA 2. SISTEMA ESPAÑOL DE RESPONSABILIDAD PENAL DE LAS PERSONAS JURÍDICAS
1.Concepto de persona jurídica
2.Antecedentes e incorporación de la Responsabilidad Penal de las Personas Jurídicas en el Código Penal Español
3.Criterios de aplicación, atenuación y exoneración de responsabilidad penal de las personas jurídicas
4.Penas aplicables a las personas jurídicas
5.Delitos imputables a las personas jurídicas
6.Determinación de la pena

UNIDAD FORMATIVA 5. DOMINIO 5. SISTEMAS DE GESTIÓN DE COMPLIANCE

UNIDAD DIDÁCTICA 1. INVESTIGACIONES Y DENUNCIAS DENTRO DE LA EMPRESA
1.Necesidad de implantar un canal de denuncias en la empresa
2.Denuncias internas: Implantación
3.Gestión de canal de denuncias internas
4.Recepción y gestión de denuncias

5.¿Qué trato se le da a una denuncia?
6.Investigación de una denuncia

UNIDAD DIDÁCTICA 2. SISTEMAS DE GESTIÓN DE COMPLIANCE (ISO 37301)

1.Aproximación a la Norma ISO 37301
2.Aspectos fundamentales de la Norma ISO 37301
3.Contexto de la organización
4.Liderazgo
5.Planificación
6.Apoyo
7.Operaciones
8.Evaluación del desempeño
9.Mejora continua

UNIDAD FORMATIVA 6. DOMINIO 6. AUDITORÍA Y TÉCNICAS DE AUDITORÍA ISO PARA SISTEMAS DE GESTIÓN DEL COMPLIANCE

UNIDAD DIDÁCTICA 1. ASPECTOS CONCEPTUALES DE LA ISO 19011

1.Introducción y contenido de la norma ISO 19011
2.Quién y en qué auditorías se debe usar la ISO 19011
3.Términos y definiciones aplicadas a la auditoría de sistemas de gestión
4.Principios de la auditoría de sistemas de gestión

UNIDAD DIDÁCTICA 2. PLANIFICACIÓN Y GESTIÓN DEL PROGRAMA DE AUDITORÍA SEGÚN LA ISO 19011

1.Introducción a la creación del programa de auditoría
2.Establecimiento e implementación del programa de auditoría
3.Objetivos y alcance del programa y de auditoría
4.Establecimiento del programa: Funciones, responsabilidades y competencias del responsable del programa
5.Evaluación de los riesgos del programa de auditoría
6.Procedimientos y métodos
7.Gestión de recursos
8.Monitoreo, seguimiento y mejora del programa de auditoría
9.Establecimiento y mantenimiento de registros y administración de resultados

UNIDAD DIDÁCTICA 3. REALIZACIÓN DE UNA AUDITORÍA CONFORME LA ISO 19011

1.Generalidades en la realización de la auditoría
2.Inicio de la auditoría
3.Actividades preliminares de la auditoría
4.Actividades para llevar a cabo la auditoría
5.Preparación y entrega del informe final
6.Finalización y seguimiento de la auditoría
7.Calidad en el proceso de auditoría

UNIDAD DIDÁCTICA 4. COMPETENCIA Y EVALUACIÓN DE AUDITORES

1.El auditor de los sistemas de gestión
2.Cualificación de la competencia del auditor
3.Independencia del auditor
4.Funciones y responsabilidades de los auditores

UNIDAD FORMATIVA 7. DOMINIO 7. FUNCIONES Y RESPONSABILIDADES DEL COMPLIANCE OFFICER

UNIDAD DIDÁCTICA 1. LA FIGURA DEL COMPLIANCE OFFICER

1.Introducción a la figura del Compliance Officer o responsable del cumplimiento
2.Formación y experiencia profesional del Compliance Officer
3.Titularidad y delegación de deberes
4.La responsabilidad penal del Compliance Officer
5.La responsabilidad civil del Compliance Officer

UNIDAD DIDÁCTICA 2. FUNCIONES DEL COMPLIANCE OFFICER

1.Aproximación a las funciones del Compliance Officer
2.Asesoramiento y Formación
3.Servicio comunicativo y sensibilización
4.Resolución práctica de incidencias e incumplimientos

UNIDAD FORMATIVA 8. DOMINIO 8. OTROS CONOCIMIENTOS DEL COMPLIANCE OFFICER

UNIDAD DIDÁCTICA 1. LA LIBRE COMPETENCIA Y COMPLIANCE

1.Introducción al Derecho de la Competencia
2.Prácticas restrictivas de la competencia
3.El Régimen de Control de Concentraciones
4.Ayudas de Estado (State Aid)
5.Prevención del abuso de mercado
6.Concepto y abuso de mercado
7.Comunicación de operaciones sospechosas
8.Posibles consecuencias derivadas de infracciones de la normativa sobre competencia
9.¿Por qué y cómo establecer un Competition Compliance Programme?

UNIDAD DIDÁCTICA 2. BLANQUEO DE CAPITALES Y FINANCIACIÓN DEL TERRORISMO

1.Prevención del Blanqueo de Capitales y financiación del terrorismo: Conceptos básicos
2.Normativa y organismos en materia de Prevención del Blanqueo de Capitales y Financiación del Terrorismo
3.Medidas y procedimientos de diligencia debida
4.Sujetos obligados
5.Obligaciones de información

UNIDAD DIDÁCTICA 3. PROTECCIÓN DE DATOS PERSONALES EN LA ORGANIZACIÓN

1.Protección de datos personales: Conceptos básicos
2.Principios generales de la protección de datos
3.Normativa de referencia en materia de protección de datos