Máster en Peritaje Informático e Informática Forense + 60 Créditos ECTS

Elige aprender en la escuela
líder en formación online

ÍNDICE

inesem business school

SOMOS INESEM

INESEM es una **Business School online** especializada con un fuerte sentido transformacional. En un mundo cambiante donde la tecnología se desarrolla a un ritmo vertiginoso nosotros somos activos, evolucionamos y damos respuestas a estas situaciones.

Apostamos por **aplicar la innovación tecnológica a todos los niveles en los que se produce la transmisión de conocimiento.** Formamos a profesionales altamente capacitados para los trabajos más demandados en el mercado laboral; profesionales innovadores, emprendedores, analíticos, con habilidades directivas y con una capacidad de añadir valor, no solo a las empresas en las que estén trabajando, sino también a la sociedad. Y todo esto lo podemos realizar con una base sólida sostenida por nuestros objetivos y valores.

Más de **18** años de experiencia

Más de **300k** estudiantes formados

Más de un **90%** tasa de empleabilidad

Hasta un **100%** de financiación

Hasta un **50%** de los estudiantes repite

Hasta un **25%** de estudiantes internacionales

Leaders driving change

Elige Inesem

ALIANZA INESEM Y UTAMED

NESEM y **UTAMED** se unen para liderar la transformación de la educación superior online.

INESEM Business School destaca como business school de referencia en formación online para profesionales, con especial énfasis en áreas como empresa, marketing, recursos humanos, tecnología y gestión empresarial. Su modelo formativo combina accesibilidad, innovación y un fuerte enfoque en el desarrollo de competencias.

UTAMED, desde su origen digital y su mirada Atlántico-Mediterránea, comparte esa visión orientada al futuro. Como universidad 100% online, apuesta por programas actualizados, multidisciplinares y adaptados a las demandas de un mercado global.

Esta alianza refuerza el puente entre la formación profesional y la formación universitaria, creando itinerarios integrados que permiten a los estudiantes avanzar en sus carreras con titulaciones avaladas académicamente y conectadas con el entorno laboral.

Ambas instituciones coinciden en ofrecer una experiencia educativa ágil, práctica y con fuerte base tecnológica, gracias a la novedosa metodología EDUCA LXP.

UTAMED

inesem business school

RANKINGS DE INESEM

INESEM Business School ha obtenido reconocimiento tanto a nivel nacional como internacional debido a su firme compromiso con la innovación y el cambio.

Para evaluar su posición en estos rankings, se consideran diversos indicadores que incluyen la percepción online y offline, la excelencia de la institución, su compromiso social, su enfoque en la innovación educativa y el perfil de su personal académico.

QS STARS RATING SYSTEM
Online Learning

Financial Magazine
Actualidad Económica & Centros de Formación

Ranking Educativo Innovatec

LOS MEJORES MASTERS EN CIBERSEGURIDAD
CyberEOP

FSO RANKING

Webometrics
RANKING WEB OF UNIVERSITIES

NOSOLOMASTER
RANKING Y OPINIONES SOBRE MASTER

webempresa

EL MUNDO

ALIANZAS Y ACREDITACIONES

Relaciones institucionales

Relaciones internacionales

Acreditaciones y Certificaciones

BY EDUCA EDTECH

Inesem es una marca avalada por **EDUCA EDTECH Group,** que está compuesto por un conjunto de experimentadas y reconocidas **instituciones educativas de formación online.** Todas las entidades que lo forman comparten la misión de **democratizar el acceso a la educación** y apuestan por la transferencia de conocimiento, por el desarrollo tecnológico y por la investigación.

EDUCA EDTECH Group

ONLINE EDUCATION

EUROINNOVA INTERNATIONAL ONLINE EDUCATION

inesem business school

INEAF BUSINESS SCHOOL

red educa.net

inesalud

EDU SPORT

EDUCA business school

ESIBE ESCUELA IBEROAMERICANA DE POSTGRADO

Educa.Pro

ceupe European Business School

UDAVINCI

CAPMAN testing solutions

Structuralia Engineering eLearning

UNIMIAMI International University of Miami

Educa PHAROS

METODOLOGÍA LXP

La metodología **EDUCA LXP** permite una experiencia mejorada de aprendizaje integrando la AI en los procesos de e-learning, a través de modelos predictivos altamente personalizados, derivados del estudio de necesidades detectadas en la interacción del alumnado con sus entornos virtuales.

EDUCA LXP es fruto de la **Transferencia de Resultados de Investigación** de varios proyectos multidisciplinares de I+D+i, con participación de distintas Universidades Internacionales que apuestan por la transferencia de conocimientos, desarrollo tecnológico e investigación.

1. Flexibilidad

Aprendizaje 100% online y flexible, que permite al alumnado estudiar donde, cuando y como quiera.

2. Accesibilidad

Cercanía y comprensión. Democratizando el acceso a la educación trabajando para que todas las personas tengan la oportunidad de seguir formándose.

3. Personalización

Itinerarios formativos individualizados y adaptados a las necesidades de cada estudiante.

4. Acompañamiento / Seguimiento docente

Orientación académica por parte de un equipo docente especialista en su área de conocimiento, que aboga por la calidad educativa adaptando los procesos a las necesidades del mercado laboral.

5. Innovación

Desarrollos tecnológicos en permanente evolución impulsados por la AI mediante Learning Experience Platform.

6. Excelencia educativa

Enfoque didáctico orientado al trabajo por competencias, que favorece un aprendizaje práctico y significativo, garantizando el desarrollo profesional.

Programas

PROPIOS UNIVERSITARIOS OFICIALES

RAZONES POR LAS QUE ELEGIR INESEM

1. Nuestra Experiencia

- Más de **18 años de experiencia.**
- Más de **300.000 alumnos** ya se han formado en nuestras aulas virtuales
- Alumnos de los 5 continentes.
- **25%** de alumnos internacionales.
- **97%** de satisfacción
- **100% lo recomiendan.**
- Más de la mitad ha vuelto a estudiar en Inesem.

2. Nuestro Equipo

En la actualidad, Inesem cuenta con un equipo humano formado por más **400 profesionales.** Nuestro personal se encuentra sólidamente enmarcado en una estructura que facilita la mayor calidad en la atención al alumnado.

3. Nuestra Metodología

100% ONLINE

Estudia cuando y desde donde quieras. Accede al campus virtual desde cualquier dispositivo.

APRENDIZAJE

Pretendemos que los nuevos conocimientos se incorporen de forma sustantiva en la estructura cognitiva

EQUIPO DOCENTE

Inesem cuenta con un equipo de profesionales que harán de tu estudio una experiencia de alta calidad educativa.

NO ESTARÁS SOLO

Acompañamiento por parte del equipo de tutorización durante toda tu experiencia como estudiante

inesem
business school

4. Calidad AENOR

- Somos Agencia de Colaboración Nº99000000169 autorizada por el Ministerio de Empleo y Seguridad Social.
- Se llevan a cabo auditorías externas anuales que garantizan la máxima calidad AENOR.
- Nuestros procesos de enseñanza están certificados por **AENOR** por la ISO 9001.

5. Somos distribuidores de formación

Como parte de su infraestructura y como muestra de su constante expansión Euroinnova incluye dentro de su organización una **editorial y una imprenta digital industrial.**

FINANCIACIÓN Y BECAS

Financia tu cursos o máster y disfruta de las becas disponibles. ¡Contacta con nuestro equipo experto para saber cuál se adapta más a tu perfil!

25% Beca **ALUMNI**

20% Beca **DESEMPLEO**

15% Beca **EMPRENDE**

15% Beca **RECOMIENDA**

15% Beca **GRUPO**

20% Beca **FAMILIA NUMEROSA**

20% Beca **DIVERSIDAD FUNCIONAL**

MÉTODOS DE PAGO

Con la Garantía de:

innovapay

Fracciona el pago de tu curso en cómodos plazos de forma segura.

mastercard maestro VISA PayPal

bizum amazon pay Pay Pay

Nos adaptamos a todos los métodos de pago internacionales:

OXXO mercado pago DISCOVER efecty Diners Club INTERNATIONAL CMR Falabella

y muchos mas...

CONFIANZA ONLINE

Protección al Comprador

inesem business school

Máster en Peritaje Informático e Informática Forense + 60 Créditos ECTS

DURACIÓN
1500 horas

MODALIDAD
ONLINE

ACOMPAÑAMIENTO
PERSONALIZADO

CREDITOS
60 ECTS

Titulación

Titulación de Máster de Formación Permanente en Peritaje Informático e Informática Forense con 1500 horas y 60 ECTS expedida por UTAMED - Universidad Tecnológica Atlántico Mediterráneo.


UTAMED

inesem business school

INESEM BUSINESS SCHOOL
UNIVERSIDAD TECNOLÓGIC ALTÁNTICO - MEDITERRÁNEO

como centro acreditado para la impartición de acciones formativas
expide el presente título propio
NOMBRE DEL ALUMNO/A
con número de documento XXXXXXXXX ha superado los estudios correspondientes de
NOMBRE DEL CURSO
con una duración de XXX horas, perteneciente al Plan de Formación de UTAMED.
Y para que surta los efectos pertinentes queda registrado con número de expediente XXXX/XXXX-XXXX-XXXXXX.
Con una calificación XXXXXXXXXXXXXX.
Y para que conste expido la presente titulación en Granada, a (día) de (mes) del (año).

NOMBRE ALUMNO/A
Firma del Alumno/a

NOMBRE DE ÁREA MANAGER
La Dirección Académica

ISO ISO IQNET LTD

Con Estatuto Consultivo, Categoría Especial del Consejo Económico y Social de la UNESCO (Núm. Resolución 604/8)

inesem business school

Descripción

continuo cambio y evolución, que exige que los profesionales informáticos posean conocimientos totalmente actualizados. Debido a lo anterior, la justicia requiere de personas especialistas que sepan realizar informes relacionados con este sector. Este Master en Peritaje Informático e Informática Forense te capacita para el libre ejercicio de Informática Forense y Pericial por cuenta propia y por cuenta ajena, así como para poder tramitar el alta en ASPEJURE para poder realizar periciales privadas o designadas por los Juzgados. Podrás realizar periciales en ámbito civil, laboral o penal, ya que la formación también abarca la parte procesal necesaria para entender la dinámica judicial.

Objetivos

- Diferenciar entre los tipos de informes periciales.
- Conocer el proceso de elaboración de los informes periciales.
- Analizar cómo valorar la prueba pericial.
- Diseñar e implementar sistemas seguros de acceso y transmisión de datos.
- Auditar redes de comunicación y sistemas informáticos

Para qué te prepara

El presente Master en Peritaje Informático e Informática Forense se encuentra dirigido a titulados en la materia que deseen obtener los conocimientos necesarios para saber realizar informes periciales y poder intervenir como perito en los juzgados y tribunales de justicia, ya sea en el ámbito civil o penal.

A quién va dirigido

Este Master en Peritaje Informático e Informática Forense está ideado para obtener los conocimientos necesarios para realizar dictámenes e informes periciales, así como intervenir como Perito en los Juzgados y Tribunales de Justicia, especialmente en el ámbito civil y penal, ya que la formación contempla el contenido de derecho procesal necesario para poder desenvolverse correctamente en los juzgados.

Salidas laborales

Este Master en Peritaje Informático e Informática Forense contiene todo lo necesario para poder ejercer como Perito Judicial. Al finalizar el curso el alumnado obtendrá un diploma que le permitirá darse de Alta como Asociado Profesional en ASPEJURE, todo ello para poder acceder a las listas de los

juzgados y ejercer como perito en Juzgados y Tribunales.

TEMARIO

MÓDULO 1. INFORMÁTICA Y ELECTRÓNICA FORENSE

UNIDAD DIDÁCTICA 1. INFORMÁTICA, CONECTIVIDAD E INTERNET

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

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
7. Cadena de custodia

UNIDAD DIDÁCTICA 3. CIBERSEGURIDAD

1. El ciberespacio y su seguridad
2. Riesgos y amenazas de la ciberseguridad
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
2. Tipos de delito informático
3. Cibercriminalidad

UNIDAD DIDÁCTICA 5. HACKING ÉTICO

1. ¿Qué es el hacking ético?
2. Aspectos legales del hacking ético
3. Perfiles del hacker
4. Hacktivismo

UNIDAD DIDÁCTICA 6. ANÁLISIS FORENSE

1. El análisis forense
2. Etapas de un análisis forense
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
4. Análisis de archivos

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
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
3. Normativa relacionada con la ciberseguridad
4. Legislación sobre delitos informáticos

MÓDULO 2. SEGURIDAD INFORMÁTICA

UNIDAD DIDÁCTICA 1. INTRODUCCIÓN Y CONCEPTOS BÁSICOS

1. La sociedad de la información
2. Diseño, desarrollo e implantación
3. Factores de éxito en la seguridad de la información

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

1. Estándares y Normas Internacionales sobre los SGSI
2. Legislación: Leyes aplicables a los SGSI

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

1. Plan de implantación del SGSI
2. Análisis de riesgos

3. Gestión de riesgos

UNIDAD DIDÁCTICA 4. AUDITORÍA DE SEGURIDAD INFORMÁTICA

1. Criterios Generales
2. Aplicación de la normativa de protección de datos de carácter personal
3. Herramientas para la auditoría de sistemas
4. Descripción de los aspectos sobre cortafuego en auditorías de sistemas de información
5. Guías para la ejecución de las distintas fases de la auditoría de sistemas de información

UNIDAD DIDÁCTICA 5. COMUNICACIONES SEGURAS: SEGURIDAD POR NIVELES

1. Seguridad a Nivel Físico
2. Seguridad a Nivel de Enlace
3. Seguridad a Nivel de Red
4. Seguridad a Nivel de Transporte
5. Seguridad a Nivel de Aplicación

UNIDAD DIDÁCTICA 6. CONFECCIÓN DEL PROCESO DE MONITORIZACIÓN DE SISTEMAS Y COMUNICACIONES

1. Identificación de los dispositivos de comunicaciones
2. Análisis de los protocolos y servicios de comunicaciones
3. Principales parámetros de configuración y funcionamiento de los equipos de comunicaciones
4. Procesos de monitorización y respuesta
5. Herramientas de monitorización de uso de puertos y servicios tipo Sniffer
6. Herramientas de monitorización de sistemas y servicios tipo Hobbit, Nagios o Cacti
7. Sistemas de gestión de información y eventos de seguridad (SIM/SEM)
8. Gestión de registros de elementos de red y filtrado (router, switch, firewall, IDS/IPS, etc)

UNIDAD DIDÁCTICA 7. SISTEMAS SIEM

1. ¿Qué es un SIEM?
2. Evolución de los sistemas SIEM: SIM, SEM y SIEM
3. Arquitectura de un sistema SIEM
4. Problemas a solventar
5. Administración de logs
6. Regulaciones IT
7. Correlación de eventos
8. Soluciones SIEM en el mercado

UNIDAD DIDÁCTICA 8. SEGURIDAD EN ENTORNOS MÓVILES

1. Aplicaciones seguras en Cloud
2. Protección de ataques en entornos de red móvil
3. Plataformas de administración de la movilidad empresarial (EMM)
4. Redes WiFi seguras

MÓDULO 3. 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 sistemas de detección de intrusos
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 de los servicios, protocolos, zonas y equipos que utiliza la organización para sus procesos de negocio
2. Definición de políticas de corte de intentos de intrusión en los IDS/IPS
3. Análisis de los eventos registrados por el IDS/IPS para determinar falsos positivos y caracterizarlos en las políticas de corte del IDS/IPS
4. Relación de los registros de auditoría del IDS/IPS necesarios para monitorizar y supervisar su correcto funcionamiento y los eventos de intentos de intrusión
5. Establecimiento de los niveles requeridos de actualización, monitorización y pruebas del IDS/IPS

UNIDAD DIDÁCTICA 3. CONTROL DE CÓDIGO MALICIOSO

1. Sistemas de detección y contención de código malicioso
2. Relación de los distintos tipos de herramientas de control de código malicioso en función de la topología de la instalación y las vías de infección a controlar
3. Criterios de seguridad para la configuración de las herramientas de protección frente a código malicioso
4. Determinación de los requerimientos y técnicas de actualización de las herramientas de protección frente a código malicioso
5. Relación de los registros de auditoría de las herramientas de protección frente a código maliciosos necesarios para monitorizar y supervisar su correcto funcionamiento y los eventos de seguridad
6. Establecimiento de la monitorización y pruebas de las herramientas de protección frente a código malicioso
7. Análisis de los programas maliciosos 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 eventos 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 en el proceso de notificación y gestión de intentos de intrusión o infecciones

2. Categorización de los incidentes derivados de intentos de intrusión o infecciones en función de su impacto potencial
3. Criterios para la determinación de las evidencias objetivas en las que se soportara la gestión del incidente
4. Establecimiento del proceso de detección y registro de incidentes derivados de intentos de intrusión o infecciones
5. Guía para la clasificación y análisis inicial del intento de intrusión o infección, contemplando el impacto previsible del mismo
6. Establecimiento del nivel de intervención requerido en función del impacto previsible
7. Guía para la investigación y diagnostico del incidente de intento de intrusión o infecciones
8. Establecimiento del proceso de resolución y recuperación de los sistemas tras un incidente derivado de un intento de intrusión o infección
9. Proceso para la comunicación del incidente a terceros, si procede
10. Establecimiento del proceso de cierre del incidente y los registros necesarios para documentar el histórico del incidente

UNIDAD DIDÁCTICA 6. ANÁLISIS FORENSE INFORMÁTICO

1. Conceptos generales y objetivos del análisis forense
2. Exposición del Principio de Lockard
3. Guía para la recogida de evidencias electrónicas
4. Guía para el análisis de las evidencias electrónicas recogidas, incluyendo el estudio de ficheros y directorios ocultos, información oculta del sistema y la recuperación de ficheros borrados
5. Guía para la selección de las herramientas de análisis forense

MÓDULO 4. GESTIÓN DE SERVICIOS EN EL SISTEMA INFORMÁTICO

UNIDAD DIDÁCTICA 1. GESTIÓN DE LA SEGURIDAD Y NORMATIVAS

1. Norma ISO 27002 Código de buenas practicas para la gestión de la seguridad de la información
2. Metodología ITIL Librería de infraestructuras de las tecnologías de la información
3. Ley orgánica de protección de datos de carácter personal
4. Normativas mas frecuentemente utilizadas para la gestión de la seguridad física

UNIDAD DIDÁCTICA 2. ANÁLISIS DE LOS PROCESOS DE SISTEMAS

1. Identificación de procesos de negocio soportados por sistemas de información
2. Características fundamentales de los procesos electrónicos
3. Estados de un proceso,
4. Manejo de señales, su administración y los cambios en las prioridades
5. Determinación de los sistemas de información que soportan los procesos de negocio y los activos y servicios utilizados por los mismos
6. Análisis de las funcionalidades de sistema operativo para la monitorización de los procesos y servicios
7. Técnicas utilizadas para la gestión del consumo de recursos

UNIDAD DIDÁCTICA 3. DEMOSTRACIÓN DE SISTEMAS DE ALMACENAMIENTO

1. Tipos de dispositivos de almacenamiento más frecuentes

2. Características de los sistemas de archivo disponibles
3. Organización y estructura general de almacenamiento
4. Herramientas del sistema para gestión de dispositivos de almacenamiento

UNIDAD DIDÁCTICA 4. UTILIZACIÓN DE MÉTRICAS E INDICADORES DE MONITORIZACIÓN DE RENDIMIENTO DE SISTEMAS

1. Criterios para establecer el marco general de uso de métricas e indicadores para la monitorización de los sistemas de información
2. Identificación de los objetos para los cuales es necesario obtener indicadores
3. Aspectos a definir para la selección y definición de indicadores
4. Establecimiento de los umbrales de rendimiento de los sistemas de información
5. Recolección y análisis de los datos aportados por los indicadores
6. Consolidación de indicadores bajo un cuadro de mandos de rendimiento de sistemas de información unificado

UNIDAD DIDÁCTICA 5. CONFECCIÓN DEL PROCESO DE MONITORIZACIÓN DE SISTEMAS Y COMUNICACIONES

1. Identificación de los dispositivos de comunicaciones
2. Análisis de los protocolos y servicios de comunicaciones
3. Principales parámetros de configuración y funcionamiento de los equipos de comunicaciones
4. Procesos de monitorización y respuesta
5. Herramientas de monitorización de uso de puertos y servicios tipo Sniffer
6. Herramientas de monitorización de sistemas y servicios tipo Hobbit, Nagios o Cacti
7. Sistemas de gestión de información y eventos de seguridad (SIM/SEM)
8. Gestión de registros de elementos de red y filtrado (router, switch, firewall, IDS/IPS, etc.)

UNIDAD DIDÁCTICA 6. SELECCIÓN DEL SISTEMA DE REGISTRO DE EN FUNCIÓN DE LOS REQUERIMIENTOS DE LA ORGANIZACIÓN

1. Determinación del nivel de registros necesarios, los periodos de retención y las necesidades de almacenamiento
2. Análisis de los requerimientos legales en referencia al registro
3. Selección de medidas de salvaguarda para cubrir los requerimientos de seguridad del sistema de registros
4. Asignación de responsabilidades para la gestión del registro
5. Alternativas de almacenamiento para los registros del sistemas y sus características de rendimiento, escalabilidad, confidencialidad, integridad y disponibilidad
6. Guía para la selección del sistema de almacenamiento y custodia de registros

UNIDAD DIDÁCTICA 7. ADMINISTRACIÓN DEL CONTROL DE ACCESOS ADECUADOS DE LOS SISTEMAS DE INFORMACIÓN

1. Análisis de los requerimientos de acceso de los distintos sistemas de información y recursos compartidos
2. Principios comúnmente aceptados para el control de accesos y de los distintos tipos de acceso locales y remotos
3. Requerimientos legales en referencia al control de accesos y asignación de privilegios

4. Perfiles de de acceso en relación con los roles funcionales del personal de la organización
5. Herramientas de directorio activo y servidores LDAP en general
6. Herramientas de sistemas de gestión de identidades y autorizaciones (IAM)
7. Herramientas de Sistemas de punto único de autenticación Single Sign On (SSO)

MÓDULO 5. PERITO JUDICIAL

UNIDAD DIDÁCTICA 1. PERITACIÓN Y TASACIÓN

1. Delimitación de los términos peritaje y tasación
2. La peritación
3. La tasación pericial

UNIDAD DIDÁCTICA 2. NORMATIVA BÁSICA NACIONAL

1. Ley Orgánica 6/1985, de 1 de julio, del Poder Judicial
2. Ley 1/2000, de 7 de enero, de Enjuiciamiento Civil
3. Ley de Enjuiciamiento Criminal, de 1882
4. Ley 1/1996, de 10 de enero, de Asistencia Jurídica Gratuita

UNIDAD DIDÁCTICA 3. LOS PERITOS

1. Concepto
2. Clases de perito judicial
3. Procedimiento para la designación de peritos
4. Condiciones que debe reunir un perito
5. Control de la imparcialidad de peritos
6. Honorarios de los peritos

UNIDAD DIDÁCTICA 4. EL RECONOCIMIENTO PERICIAL

1. El reconocimiento pericial
2. El examen pericial
3. Los dictámenes e informes periciales judiciales
4. Valoración de la prueba pericial
5. Actuación de los peritos en el juicio o vista

UNIDAD DIDÁCTICA 5. LEGISLACIÓN REFERENTE A LA PRÁCTICA DE LA PROFESIÓN EN LOS TRIBUNALES

1. Funcionamiento y legislación
2. El código deontológico del Perito Judicial

UNIDAD DIDÁCTICA 6. LA RESPONSABILIDAD

1. La responsabilidad
2. Distintos tipos de responsabilidad
3. El seguro de responsabilidad civil

UNIDAD DIDÁCTICA 7. PERITACIONES

1. La peritación médico-legal
2. Peritaciones psicológicas
3. Peritajes informáticos
4. Peritaciones inmobiliarias

MÓDULO 6. ELABORACIÓN DE INFORMES PERICIALES

UNIDAD DIDÁCTICA 1. PERITO, INFORME PERICIAL Y ATESTADO POLICIAL

1. Concepto de perito
2. Atestado policial
3. Informe pericial

UNIDAD DIDÁCTICA 2. TIPOS DE INFORMES PERICIALES I

1. Informes periciales por cláusulas de suelo
2. Informes periciales para justificación de despidos

UNIDAD DIDÁCTICA 3. TIPOS DE INFORMES PERICIALES II

1. Informes periciales de carácter económico, contable y financiero
2. Informes especiales de carácter pericial

UNIDAD DIDÁCTICA 4. LAS PRUEBAS JUDICIALES Y EXTRAJUDICIALES

1. Concepto de prueba
2. Medios de prueba
3. Clases de pruebas
4. Principales ámbitos de actuación
5. Momento en que se solicita la prueba pericial
6. Práctica de la prueba

UNIDAD DIDÁCTICA 5. ELABORACIÓN DEL INFORME TÉCNICO

1. ¿Qué es el informe técnico?
2. Diferencia entre informe técnico y dictamen pericial
3. Objetivos del informe pericial
4. Estructura del informe técnico

UNIDAD DIDÁCTICA 6. ELABORACIÓN DEL DICTAMEN PERICIAL

1. Características generales y estructura básica
2. Las exigencias del dictamen pericial
3. Orientaciones para la presentación del dictamen pericial

UNIDAD DIDÁCTICA 7. VALORACIÓN DE LA PRUEBA PERICIAL

1. Valoración de la prueba judicial
2. Valoración de la prueba pericial por Jueces y Tribunales

MÓDULO 7. CIBERDELITOS

UNIDAD DIDÁCTICA 1. CIBERDELINCUENCIA

1. ¿Qué es la ciberdelincuencia?
2. Delincuencia informática y cibercriminalidad
3. Principales tipos de cibercrimen
4. Ciberamenazas
5. Marco Legal Estatal
6. Convenio de Budapest sobre Ciberdelincuencia

UNIDAD DIDÁCTICA 2. LOS DELITOS INFORMÁTICOS EN EL CÓDIGO PENAL

1. Concepto y clasificación de los delitos informáticos
2. Características principales de los delitos informáticos
3. Acceso e interceptación ilícita
4. 4.Interferencia en los datos y en el sistema
5. Falsificación informática
6. Fraude Informático
7. Delitos sexuales
8. Delitos contra la propiedad industrial intelectual
9. Delitos contra el honor
10. Delitos contra la salud pública
11. Amenazas y coacciones

UNIDAD DIDÁCTICA 3. COMPETENCIA PARA EL ENJUICIAMIENTO DE LOS DELITOS INFORMÁTICOS

1. Principio de Universalidad
2. Efectos de cosa juzgada
3. Competencia judicial: teoría de la actividad, del resultado y de la ubicuidad
4. Temporalidad

UNIDAD DIDÁCTICA 4. EL AUTOR TECNOLÓGICO

1. Responsabilidad penal del autor
2. Proliferación de autores
3. La responsabilidad de intermediarios tecnológicos

UNIDAD DIDÁCTICA 5. CIBERVÍCTIMA

1. La importancia de la víctima en el cibercrimen
2. Prevención del cibercrimen
3. Multiplicidad de cibervíctimas
4. Victimización en el ciberespacio

UNIDAD DIDÁCTICA 6. CIBERDELITOS RELACIONADOS CON LA PRIVACIDAD Y PROTECCIÓN DE DATOS

1. ¿Por qué es importante la privacidad?
2. Privacidad y seguridad

3. Ciberdelitos que comprometen la privacidad
4. Normativa sobre privacidad y protección de datos

UNIDAD DIDÁCTICA 7. CIBERDELITOS CONTRA LA PROPIEDAD INTELECTUAL Y DERECHOS CONEXOS

1. ¿Qué es la propiedad intelectual?
2. Tipos de propiedad intelectual
3. Teorías criminológicas en delitos contra la propiedad intelectual por medios cibernéticos

UNIDAD DIDÁCTICA 8. DELINCUENCIA ORGANIZADA EN INTERNET

1. Delincuencia cibernética organizada y actores que intervienen
2. Perfil de los grupos delictivos
3. Actividades de los ciberdelitos organizados
4. Prevención de este tipo de ciberdelitos

UNIDAD DIDÁCTICA 9. CIBERDELITOS RELACIONADOS CON LA TRATA DE PERSONAS Y TRÁFICO ILÍCITO DE INMIGRANTES

1. ¿La tecnología facilita este tipo de delitos?
2. Trata de personas y tráfico ilícito de inmigrantes como ciberdelito organizado

UNIDAD DIDÁCTICA 10. CIBERDELITOS CONTRA LAS PERSONAS

1. Explotación y abuso sexual infantil
2. Hostigamiento
3. Acoso
4. Violencia de género

UNIDAD DIDÁCTICA 11. CIBERTERRORISMO

1. Hacktivismo
2. Ciberespionaje
3. Ciberterrorismo
4. Guerra cibernética
5. La guerra de la información, la desinformación y el fraude electoral

MÓDULO 8. DERECHO PROCESAL CIVIL

UNIDAD DIDÁCTICA 1. EL PROCESO CIVIL. FUNCIONES Y PRINCIPIOS

1. Aproximación al procedimiento civil
2. Aplicación de la Ley de Enjuiciamiento Civil
3. Reglas de la Buena Fe procesal

UNIDAD DIDÁCTICA 2. JURISDICCIÓN Y COMPETENCIA

1. Introducción a la jurisdicción y competencia internacional y estatal
2. Competencia internacional
3. Inmunidad de jurisdicción

4. Falta de competencia internacional
5. Competencia de la jurisdicción civil
6. Cuestiones prejudiciales
7. Competencia y falta de competencia de los juzgados y tribunales
8. Declinatoria por falta de jurisdicción o competencia
9. Reparto de asuntos

UNIDAD DIDÁCTICA 3. LA PRUEBA EN EL PROCESO CIVIL. OBJETO, NECESIDAD E INICIATIVA. PROPOSICION Y ADMISION. PRUEBA ANTICIPADA Y ASEGURAMIENTO DE LA PRUEBA. LOS MEDIOS DE PRUEBA. LAS PRESUNCIONES. LA PRUEBA PROHIBIDA

1. Diligencias preliminares
2. Prueba anticipada y aseguramiento de la prueba
3. Presentación de documentos, dictámenes, informes y otros medios o instrumentos
4. La prueba y los medios de prueba: interrogatorio de las partes, documentos públicos y privados, dictamen de peritos, dictamen judicial, testigos
5. La prueba prohibida
6. Presunciones
7. Cuestiones incidentales
8. Condena en costas en primera instancia

UNIDAD DIDÁCTICA 4. PROCESOS CIVILES. INICIACIÓN, FASES Y SENTENCIA. ESPECIAL ATENCIÓN A LA PROPOSICIÓN Y PRÁCTICA DE LA PRUEBA

1. Tipos de procesos civiles
2. Juicio ordinario
3. Juicio verbal
4. Capacidad, filiación, matrimonio y menores
5. Procesos monitorio y cambiario
6. Proposición y práctica de la prueba

UNIDAD DIDÁCTICA 5. RECURSOS

1. Disposiciones generales
2. Recurso de reposición y revisión
3. Recursos de apelación y segunda instancia
4. Recurso extraordinario por infracción procesal
5. Recurso de casación
6. Recurso en interés de la ley
7. Recurso de queja
8. Recurso de rebeldía y rescisión de sentencias

UNIDAD DIDÁCTICA 6. LA EJECUCIÓN DE SENTENCIAS. EJECUCION DE SENTENCIAS DINERARIAS. LA AVERIGUACION. EJECUCION NO DINERARIA

1. Los títulos ejecutivos
2. Ejecución provisional
3. La ejecución: partes, despacho de ejecución, oposición e impugnación, suspensión y término
4. La ejecución dineraria: requerimiento y embargo de bienes

5. Averiguación patrimonial
6. Ejecución no dineraria

UNIDAD DIDÁCTICA 7. LAS MEDIDAS CAUTELARES

1. Disposiciones generales de las medidas cautelares
2. Adopción de medidas cautelares
3. Oposición a las medidas cautelares
4. Modificación de medidas cautelares

MÓDULO 9. DERECHO PROCESAL PENAL

UNIDAD DIDÁCTICA 1. EL PROCESO PENAL. CONCEPTO. FUNCIONES, PRINCIPIOS, SISTEMAS FUNDAMENTALES DEL PROCESO PENAL

1. Conceptualización del proceso penal a través de los principios que lo configuran
2. Derechos fundamentales inherentes al proceso penal
3. El objeto en el proceso penal

UNIDAD DIDÁCTICA 2. JURISDICCIÓN Y COMPETENCIA: CONCEPTOS. ORGANIZACIÓN DE LA JURISDICCIÓN PENAL EN ESPAÑA

1. La Jurisdicción Penal. Juzgados y tribunales
2. La competencia
3. La competencia territorial y por conexión
4. La cuestión prejudicial

UNIDAD DIDÁCTICA 3. FASES DEL PROCESO PENAL

1. Fase I. Concepto, contenido y clasificación
2. Fase II. Las diligencias previas
3. Fase III. Medidas limitativas de los derechos fundamentales
4. Fase IV. Las medidas cautelares
5. Fase V. El sobreseimiento y la imputación

UNIDAD DIDÁCTICA 4. LAS PARTES EN EL PROCESO PENAL

1. Las partes en el procedimiento Penal
2. Los presupuestos procesales de las partes

UNIDAD DIDÁCTICA 5. INICIACIÓN DEL PROCESO PENAL: DENUNCIA Y QUERELLA

1. Inicio del proceso
2. La querella
3. La denuncia

UNIDAD DIDÁCTICA 6. LA ACCIÓN PENAL

1. La conducta como elemento del delito
2. Elementos de la acción

3. Teorías de la acción
4. Actos Involuntarios. Ausencia de Acción
5. La omisión
6. La responsabilidad penal de las personas jurídicas

UNIDAD DIDÁCTICA 7. LA DETENCIÓN. DERECHOS DEL DETENIDO

1. El concepto de detención: definición y aspectos generales
2. Supuestos en los que procede la detención
3. Requisitos y práctica de la detención
4. Identificación en la vía pública
5. Detención de menores
6. El menor como víctima
7. Supuestos de detenciones especiales en función de la persona

UNIDAD DIDÁCTICA 8. EL SECRETO EN EL PROCESO PENAL

1. Fase de instrucción
2. El principio técnico de Publicidad en el proceso penal
3. Fases del proceso y principio de publicidad

UNIDAD DIDÁCTICA 9. LOS INSTRUMENTOS DE PRUEBA EN EL PROCESO PENAL ESPAÑOL. ESPECIAL CONSIDERACIÓN A LA “PRUEBA PROHIBIDA”

1. Medios de prueba
2. Prueba prohibida y prueba ilícita

UNIDAD DIDÁCTICA 10. INVESTIGACIÓN DELICTIVA FACULTADA A LOS DETECTIVES PRIVADOS. ANÁLISIS DE LA CONDICIÓN DE "LEGITIMADO" PARA LA ACCIÓN PENAL

1. Legislación aplicable
2. Funciones atribuidas a los detectives privados

UNIDAD DIDÁCTICA 11. LA POLICÍA JUDICIAL. CONCEPTO Y FUNCIONES

1. Disposiciones generales
2. Regulación normativa de la Policía Judicial
3. Estructura y funciones de la Comisaría General de Policía Judicial

UNIDAD DIDÁCTICA 12. EL JUICIO ORAL

1. El Juicio Oral
2. Actuaciones previas al juicio oral
3. Artículos de previo pronunciamiento y cuestiones previas
4. Celebración del juicio: Desarrollo de la vista
5. Causas de suspensión del juicio oral

UNIDAD DIDÁCTICA 13. LA PRÁCTICA DE LA PRUEBA

1. La prueba y los actos de investigación

2. Valoración y sentencia
3. Efectos de cosa Juzgada

UNIDAD DIDÁCTICA 14. PROCESOS ESPECIALES: TRIBUNAL DEL JURADO, PROCESOS RÁPIDOS, PROCESOS DERIVADOS DE "DELITOS PRIVADOS"

1. Procedimiento abreviado
2. El juicio del jurado
3. Juicios rápidos

UNIDAD DIDÁCTICA 15. EL JUICIO POR DELITOS LEVES

1. Introducción a los juicios por delitos leves
2. Fase previa al juicio por delitos leves
3. Celebración del juicio por delitos leves
4. Prescripción de los delitos leves

UNIDAD DIDÁCTICA 16. LOS RECURSOS CONTRA LA SENTENCIA

1. Recursos ordinarios en el procedimiento penal
2. Clases de recursos
3. Recursos Ordinarios

UNIDAD DIDÁCTICA 17. ESPECIAL CONSIDERACIÓN AL RECURSO EXTRAORDINARIO DE REVISIÓN DE SENTENCIAS FIRMES

1. Recursos extraordinarios en el procedimiento penal
2. La rescisión de la cosa juzgada

MÓDULO 10. PROYECTO FINAL DE MÁSTER

inesem
business school

By
EDUCA EDTECH
Group