Masters Profesionales

Master en Seguridad de la Información y las Comunicaciones

INESEM BUSINESS SCHOOL

Índice

Master en Seguridad de la Información y las Comunicaciones

SOBRE INESEM

BUSINESS SCHOOL

INESEM Business School como Escuela de Negocios Online tiene por objetivo desde su nacimiento trabajar para fomentar y contribuir al desarrollo profesional y personal de sus alumnos. Promovemos ***una enseñanza multidisciplinar e integrada***, mediante la aplicación de ***metodologías innovadoras de aprendizaje*** que faciliten la interiorización de conocimientos para una aplicación práctica orientada al cumplimiento de los objetivos de nuestros itinerarios formativos.

En definitiva, en INESEM queremos ser el lugar donde te gustaría desarrollar y mejorar tu carrera profesional. ***Porque sabemos que la clave del éxito en el mercado es la "Formación Práctica" que permita superar los retos que deben de afrontar los profesionales del futuro.***

Master en Seguridad de la Información y las Comunicaciones

DURACIÓN	1500
PRECIO	1795 €
MODALIDAD	Online

Entidad impartidora:

INESEM BUSINESS SCHOOL

Programa de Becas / Financiación 100% Sin Intereses

Titulación Masters Profesionales

- Titulación Expedida y Avalada por el Instituto Europeo de Estudios Empresariales "Enseñanza no oficial y no conducente a la obtención de un título con carácter oficial o certificado de profesionalidad."

Resumen

Hoy en día la seguridad informática es un tema muy importante y sensible, que abarca un gran conjunto de aspectos en continuo cambio y constante evolución, que exige que los profesionales informáticos posean conocimientos totalmente actualizados. Así, la Norma UNE-ISO/IEC 27001: 2005 está elaborada para emplearse en cualquier tipo de organización. La adecuada y correcta implementación de un SGSI permite a las empresas asegurar la continuidad del negocio, minimizar el riesgo comercial y maximizar el retorno de las inversiones y las oportunidades comerciales.

A quién va dirigido

El Master Seguridad de la Información y las Comunicaciones está dirigido a profesionales o estudiantes de la rama informática, telecomunicaciones y, en general, a todos los interesados en encaminar su carrera profesional hacia la seguridad de la información, protección de datos y seguridad en los sistemas de almacenamiento.

Objetivos

Con el Masters Profesionales **Master en Seguridad de la Información y las Comunicaciones** usted alcanzará los siguientes objetivos:

- Implementar un sistema de gestión de seguridad de información basado en el estándar ISO/IEC 27001.
- Exponer y explicar una serie de buenas prácticas para conseguir la seguridad de la información.
- Gestionar servicios en el sistema informático.
- Diseñar e Implementar sistemas seguros de acceso y transmisión de datos.
- Detectar y responder ante incidentes de seguridad informática.
- Garantizar la continuidad de las operaciones de los elementos críticos que componen los sistemas de información.
- Auditar redes de comunicación y sistemas informáticos.

¿Y, después?

Para qué te prepara

El Master Seguridad de la Información y las Comunicaciones te prepara para gestionar los planes de seguridad de la información conociendo la normativa y los sistemas de gestión. Sabrás cuáles son los criterios para realizar una Auditoría de Seguridad Informática y el procedimiento de control ante incidentes. Para la seguridad informática, estudiarás la encriptación de la información y la implantación de infraestructuras de clave pública (PKI).

Salidas Laborales

Gracias a la realización del Master Seguridad de la Información y las Comunicaciones podrás adentrarte en un sector en alza y desarrollar tu carrera profesional como Auditor de sistemas de calidad, Directivo del departamento de calidad, Responsable del Departamento de sistemas o Responsable de redes y comunicaciones, entre otras muchas profesiones.

¿Por qué elegir INESEM?

El alumno es el protagonista

01

Nuestro modelo de aprendizaje se adapta a las necesidades del alumno, quién decide cómo realizar el proceso de aprendizaje a través de itinerarios formativos que permiten trabajar de forma autónoma y flexible.

Innovación y Calidad

Ofrecemos el contenido más actual y novedosa, respondiendo a la realidad empresarial y al entorno cambiante con una alta rigurosidad académica combinada con formación práctica.

02

Empleabilidad y desarrollo profesional

03

Ofrecemos el contenido más actual y novedosa, respondiendo a la realidad empresarial y al entorno cambiante con una alta rigurosidad académica combinada con formación práctica.

INESEM Orienta

Ofrecemos una asistencia complementaria y personalizada que impulsa la carrera de nuestros alumnos a través de nuestro Servicio de Orientación de Carrera Profesional permitiendo la mejora de competencias profesionales mediante programas específicos.

04

Facilidades Económicas y Financieras

05

Ofrecemos a nuestros alumnos facilidades para la realización del pago de matrículas 100% sin intereses así como un sistema de Becas para facilitar el acceso a nuestra formación.

$

Módulo 1. **Introducción a la seguridad de la información**

Módulo 2. **Sistema de gestión de seguridad de la información**

Módulo 3. **Auditoria de seguridad informática**

Módulo 4. **Prevención y gestión de ciberataques**

Módulo 5. **Seguridad en las redes de datos**

Módulo 6. **Administración de servicios en el sistema informático**

Módulo 7. **Proyecto fin de máster**

Módulo 1.
Introducción a la seguridad de la información

Unidad didáctica 1.
Descripción de la seguridad de la información

1. La sociedad de la información
2. ¿Qué se entiende por seguridad de la información?
3. ¿Por qué tener en cuenta la seguridad de la información?
4. Fundamentos de la seguridad de la información: confidencialidad, integridad y disponibilidad
5. Fuentes de los riesgos de la seguridad
6. Controles para garantizar la seguridad de la información
7. Cómo conseguir la seguridad de la información

Unidad didáctica 2.
Normativa básica sobre seguridad de la información

1. Marco legal y jurídico de la seguridad de la información
2. Normativa comunitaria sobre seguridad de la información
3. Normativa de calidad sobre la gestión de la seguridad de la información: Norma ISO 27000
4. La seguridad de la información en la legislación española

Unidad didáctica 3.
Descripción de la norma iso/iec 27002 para la implantación de un sistema de seguridad

1. ¿Qué es la norma ISO/IEC 27002?
2. Ámbito de aplicación de la Norma ISO/IEC 27002
3. Detalle de la Norma ISO/IEC 27002
4. Controles de los riesgos de seguridad

Unidad didáctica 4.
La gestión de políticas de seguridad y de los activos que intervienen en las mismas

1. Qué son las políticas de seguridad de la información
2. Cómo organizar la seguridad de la información
3. Cómo implantar la seguridad de la información
4. Agentes externos: el control de acceso a terceros
5. Medidas de control a los agentes de seguridad de la información
6. Adjudicación de funciones a los activos de seguridad de la información
7. Clasificación de la información

Unidad didáctica 5.
Seguridad de la información de los recursos humanos

1. Seguridad de la información propia de los recursos humanos
2. Precauciones de seguridad antes de la contratación
3. Precauciones de seguridad durante el periodo de contratación
4. Precauciones de seguridad en la finalización de la relación laboral o cambio de puesto de trabajo
5. Precauciones de seguridad de la información con respecto a la seguridad física y ambiental o del entorno
6. Las zonas seguras
7. Los sistemas de protección y seguridad

Unidad didáctica 6.

Gestión de los sistemas de comunicaciones

1. Introducción a la gestión de las comunicaciones y operaciones
2. Procedimientos y responsabilidades operacionales
3. Prestación externa de los servicios
4. Creación de una metodología para la gestión del sistema
5. Gestión de la seguridad frente a códigos maliciosos y móviles
6. Planificación de las copias de seguridad de la información
7. Planificación y control de la seguridad de la red
8. Gestión de medios
9. Controles en el intercambio de información
10. La seguridad en organizaciones con comercio electrónico
11. Controles para la detección de actividades no autorizadas

Unidad didáctica 7.

El control de acceso a los sistemas de información

1. Qué persigue el control de accesos
2. Objetivos de los sistemas de control de accesos
3. Administración de acceso de usuario
4. Obligaciones del usuario
5. Controles de seguridad de acceso a la red
6. Controles a nivel de sistema operativo
7. Controles a nivel de aplicación
8. Seguridad en dispositivos móviles y teletrabajo

Unidad didáctica 8.

Implantación de sistemas de información

1. 1. Justificación de los de sistemas de información
2. Especificaciones de seguridad de los sistemas de información
3. Normas para la gestión de información en las aplicaciones
4. Protecciones a través de controles criptográficos
5. Protección de los archivos del sistema
6. Protección y control de los procesos de desarrollo y soporte
7. Administración y control de la vulnerabilidad técnica

Unidad didáctica 9.

Administración de incidentes en la seguridad de la información y de la continuidad del negocio

1. Administración de incidentes en la seguridad de la información
2. Revisión y comunicación de eventos y puntos débiles en la seguridad de la información
3. Control de incidentes y optimizaciones en la seguridad de la información
4. Ajustes para la mejora de la continuidad del negocio
5. Controles de la seguridad de la información

Unidad didáctica 10.

Ejecución de los requerimientos legales y técnicos

1. Observancia de los requerimientos legales
2. Ejecución de las políticas y estándares de seguridad
3. Cuestiones a observar en la auditoría de los sistemas de información

Módulo 2.
Sistema de gestión de seguridad de la información

Unidad didáctica 1.
La norma une-iso/iec 27001:2014

1. Estándares y Normas Internacionales sobre los SGSI: Familia de Normas ISO 27000
2. La Norma UNE-ISO/IEC 27001:2014. Objeto y ámbito de aplicación
3. Análisis Diferencial de la Norma UNE-ISO/IEC 27001:2014
4. Términos de referencia
5. Importancia de implantar un sistema de seguridad de la información

Unidad didáctica 2.
Los sistemas de gestión de la seguridad de la información

1. La seguridad de la información
2. Implantación de sistemas de seguridad de la información
3. Cómo documentar un sistema de seguridad de información

Unidad didáctica 3.
Cometido de la dirección en los planes de seguridad

1. Implicación de la dirección
2. Administración de los recursos
3. Estudio e implantación de una política de gestión de la seguridad

Unidad didáctica 4.
Control y supervisión de los sistemas de gestión de la información por parte de la dirección

1. Supervisión del sistema de gestión de la información
2. Perfeccionamiento del sistema de gestión de la seguridad de la información

Módulo 3.
Auditoria de seguridad informática

Unidad didáctica 1.
Criterios sobre auditoría informática

1. Código deontológico aplicado a la auditoría informática
2. Tipos de auditoría aplicables a los sistemas de información
3. Orientaciones para construir un equipo auditor
4. Controles a realizar para llevar a cabo una auditoría
5. Muestras a tomar para llevar el control de la auditoría
6. Herramientas informáticas para la auditoría (Computer Assisted Audit Tools)
7. Requerimientos que deben cumplir los hallazgos de auditoría
8. Implantación de criterios para agrupar los hallazgos como observaciones o no conformidades
9. Normativas y metodologías a aplicar en la auditoría de sistemas de información

Unidad didáctica 2.
La normativa de protección de datos de carácter personal

1. Disposiciones generales de protección de datos de carácter personal
2. Normativa europea, la directiva 95/46/CE
3. Normativa nacional, Ley Orgánica para el Tratamiento Automatizado de Datos (LORTAD), Ley Orgánica de Protección de Datos (LOPD) y Reglamento de Desarrollo de La Ley Orgánica de Protección de Datos (RD 1720/2007)
4. Registro y control de los ficheros con datos de carácter personal pertenecientes a organizaciones
5. Detalle de las medidas de seguridad para la protección de los datos de carácter personal recogidas en el Real Decreto 1720/2007
6. Normas para el desarrollo de la auditoría bienal obligatoria de ley orgánica 15-1999 de protección de datos de carácter personal

Unidad didáctica 3.
Riesgos propios de los sistemas de información

1. El análisis de riesgos en los sistemas de información
2. Identificación de las vulnerabilidades y amenazas a los sistemas de información.
3. Tipos de código malicioso
4. Elementos del análisis de riesgos y sus relaciones
5. Métodos de control de análisis de riesgos
6. Los activos involucrados en el análisis de riesgos y su valoración
7. Las amenazas que pueden afectar a los activos identificados
8. Detalle de las vulnerabilidades existentes en los sistemas de información
9. Control y mejora del proceso de auditoría y comparación de vulnerabilidades
10. Identificación de los sistemas de prevención en el análisis de riesgos y su efecto sobre las vulnerabilidades y amenazas
11. Creación de escenarios de riesgo para el estudio de los pares activo-amenaza
12. Estudio de la probabilidad e impacto de materialización de los escenarios
13. Determinación del nivel de riesgo para los distintos pares de activo y amenaza
14. Establecimiento de los criterios de evaluación del riesgo para determinar el nivel de aceptación de un riesgo
15. Alternativas de gestión de riesgos
16. Normas para la creación del plan de gestión de riesgos
17. Introducción a la metodología NIST SP 800-30
18. Introducción a la metodología Magerit versión 2

Unidad didáctica 4.
Herramientas para la auditoría de sistemas

1. Herramientas del sistema operativo
2. Herramientas de redes y sus dispositivos
3. Herramientas de testeo de vulnerabilidades
4. Herramientas para análisis de protocolos
5. Analizadores de páginas web
6. Ataques de diccionario y fuerza bruta

Unidad didáctica 5.
Participación de los cortafuegos en auditorías de sistemas informáticos

1. Introducción a los cortafuegos
2. Partes de un cortafuegos de red
3. Clasificación de los cortafuegos por funcionalidad y ubicación
4. Diseños de cortafuegos de red
5. Diseños avanzados de cortafuegos de red

Unidad didáctica 6.

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

Módulo 4.

Prevención y gestión de ciberataques

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 Malware
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 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
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
6. Proceso para la comunicación del incidente a terceros

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
5. Guía para la selección de las herramientas de análisis forense

Módulo 5.
Seguridad en las redes de datos

Unidad didáctica 1.
Criptografía

1. Perspectiva histórica y objetivos de la criptografía
2. Teoría de la información
3. Propiedades de la seguridad que se pueden controlar mediante la aplicación de la criptografía
4. Criptografía de clave privada o simétrica
5. Criptografía de clave pública o asimétrica
6. Algoritmos criptográficos más utilizados
7. Funciones hash y los criterios para su utilización
8. Protocolos de intercambio de claves
9. Herramientas de cifrado

Unidad didáctica 2.
Aplicación de una infraestructura de clave pública (pki)

1. Identificación de los componentes de una PKI y sus modelos de relaciones
2. Autoridad de certificación y sus elementos
3. Política de certificado y declaración de prácticas de certificación (CPS)
4. Lista de certificados revocados (CRL)
5. Funcionamiento de las solicitudes de firma de certificados (CSR)
6. Infraestructuras de gestión de privilegios (PMI)
7. Campos de certificados de atributos
8. Aplicaciones que se apoyan en la existencia de una PKI

Unidad didáctica 3.

Seguridad en las comunicaciones

1. Las redes privadas virtuales
2. Protocolo IPSec
3. Protocolos SSL y SSH
4. Sistemas SSL VPN
5. Túneles cifrados
6. Ventajas e inconvenientes de las distintas alternativas para la implantación de la tecnología de VPN

Módulo 6.

Administración de servicios en el sistema informático

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. ISO 27001:2017
2. Legislación: Leyes aplicables a los SGSI (RGPD)

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.

Métricas para controlar y optimizar el rendimiento de sistemas

1. Marco para el uso de métricas e indicadores
2. Identificación de los elementos a controlar
3. Normas para seleccionar correctamente los indicadores
4. Definir los límites de rendimiento en los sistemas
5. Recolección y análisis de los datos aportados por los indicadores

Unidad didáctica 5.

Implantación del proceso de monitorización de sistemas y comunicaciones

1. Los dispositivos usados en las comunicaciones
2. Estudio de los protocolos y servicios de comunicaciones
3. Configuración de los equipos de comunicaciones
4. Procesos y herramientas de control
5. Herramientas de monitorización de sistemas
6. Administración de la información y eventos de seguridad (SIM/SEM)
7. Gestión de eventos de elementos de red y filtrado

Unidad didáctica 6.

Selección del sistema de registro en función de los requerimientos de la organización

1. 1. Determinación del periodo de almacenamiento
2. Los requerimientos legales en cuanto al registro
3. Medidas de control para cubrir las exigencias de seguridad
4. Identificación de responsables en los sistemas de registro
5. Sistemas de almacenamiento
6. Factores para seleccionar el sistema de almacenamiento

Unidad didáctica 7.

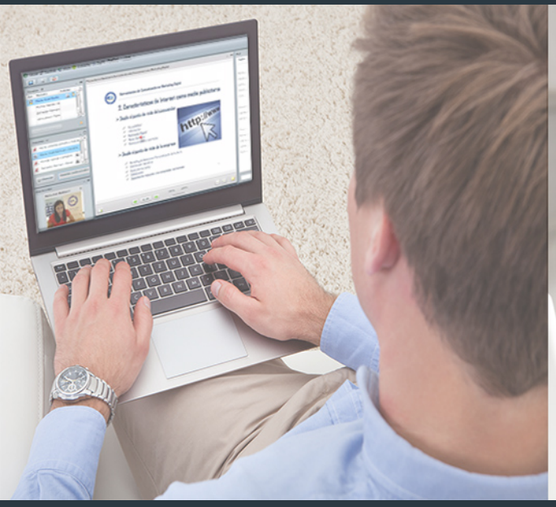
Gestión del control de accesos a los sistemas de información

1. Mecanismos para validación de usuarios
2. Sistemas usados para el control de accesos, tanto físicos como remotos
3. Legislación aplicable al control de accesos y asignación de privilegios
4. Roles en la organización de acuerdo a las funciones
5. Active Directory y servidores LDAP
6. Sistemas de gestión de identidades y autorizaciones (IAM)
7. Sistemas Single Sign On (SSO)

Módulo 7.
Proyecto fin de máster

metodología de aprendizaje

La configuración del modelo pedagógico por el que apuesta INESEM, requiere del uso de herramientas que favorezcan la colaboración y divulgación de ideas, opiniones y la creación de redes de conocimiento más colaborativo y social donde los alumnos complementan la formación recibida a través de los canales formales establecidos.



Con nuestra metodología de aprendizaje online, el alumno comienza su andadura en INESEM Business School a través de un campus virtual diseñado exclusivamente para desarrollar el itinerario formativo con el objetivo de mejorar su perfil profesional. El alumno debe avanzar de manera autónoma a lo largo de las diferentes unidades didácticas así como realizar las actividades y autoevaluaciones correspondientes.

El 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.

Nuestro sistema de aprendizaje se fundamenta en *cinco pilares* que facilitan el estudio y el desarrollo de competencias y aptitudes de nuestros alumnos a través de los siguientes entornos:

Secretaría

Sistema que comunica al alumno directamente con nuestro asistente virtual permitiendo realizar un seguimiento personal de todos sus trámites administrativos.

Campus Virtual

Entorno Personal de Aprendizaje que permite gestionar al alumno su itinerario formativo, accediendo a multitud de recursos complementarios que enriquecen el proceso formativo así como la interiorización de conocimientos gracias a una formación práctica, social y colaborativa.

Revista Digital

Espacio de actualidad donde encontrar publicaciones relacionadas con su área de formación. Un excelente grupo de colabradores y redactores, tanto internos como externos, que aportan una dosis de su conocimiento y experiencia a esta red colaborativa de información.

Comunidad

Espacio de encuentro que pemite el contacto de alumnos del mismo campo para la creación de vínculos profesionales. Un punto de intercambio de información, sugerecias y experiencias de miles de usuarios.

Webinars

Píldoras formativas mediante el formato audiovisual para complementar los itinerarios formativos y una práctica que acerca a nuestros alumnos a la realidad empresarial.

SERVICIO DE **Orientación** de Carrera

Nuestro objetivo es el asesoramiento para el desarrollo de tu carrera profesional. Pretendemos capacitar a nuestros alumnos para su adecuada adaptación al mercado de trabajo facilitándole su integración en el mismo. Somos el aliado ideal para tu crecimiento profesional, aportando las capacidades necesarias con las que afrontar los desafíos que se presenten en tu vida laboral y alcanzar el éxito profesional. Gracias a nuestro Departamento de Orientación de Carrera se gestionan más de 500 convenios con empresas, lo que nos permite contar con una plataforma propia de empleo que avala la continuidad de la formación y donde cada día surgen nuevas oportunidades de empleo. Nuestra bolsa de empleo te abre las puertas hacia tu futuro laboral.

Financiación y becas

En INESEM

Ofrecemos a nuestros alumnos facilidades económicas y financieras para la realización del pago de matrículas,

todo ello
100%
sin intereses.

INESEM continúa ampliando su programa de becas para acercar y posibilitar el aprendizaje continuo al máximo número de personas. Con el fin de adaptarnos a las necesidades de todos los perfiles que componen nuestro alumnado.

Masters Profesionales

Master en Seguridad de la Información y las Comunicaciones