INESEM

BUSINESS SCHOOL

Máster en Seguridad de la Información y las Comunicaciones

+ Información Gratis

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

Máster en Seguridad de la Información y las Comunicaciones

duración total: 1.500 horas ***horas teleformación:*** 450 horas

precio: 0 € *

modalidad: Online

* hasta 100 % bonificable para trabajadores.

descripción

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.

+ Información Gratis

a quién va dirigido

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

objetivos

- Dotar a los alumnos de los lineamientos básicos para la aplicación de la Norma ISO/IEC 27001 dentro de su organización. - Ofrecer las pautas para implementar un sistema de gestión de seguridad de información basado en el estándar ISO/IEC 27001 siguiendo los controles recomendados por el estándar ISO/IEC 27002 en sus respectivas cláusulas. - 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, mediante acciones y procedimientos. - Auditar redes de comunicación y sistemas informáticos.

para qué te prepara

El presente master pretende formar al alumnado a nivel teórico-práctico en el desempeño de todas estas funciones que, como profesionales de la implantación, gestión y auditoría de sistemas de seguridad de información, deberán poseer. El alumno conocerá la Norma UNE-ISO/IEC 27001: 2005 elaborada para emplearse en cualquier tipo de organización. En este master se mostrará la legislación asociada a la seguridad de la información.

salidas laborales

Auditor de sistemas de calidad, Directivos del Departamento de calidad, Responsables del Departamento de Sistemas, Responsables de Redes y Comunicaciones.

+ Información Gratis

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 — **Firma del alumno/a**

MARIA MORENO HIDALGO — **Sello** — 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 'Introducción a la Seguridad de la Información'
- Manual teórico 'Sistema de Gestión de Seguridad de la Información'
- Manual teórico 'Auditoría de Seguridad Informática'
- Manual teórico 'Seguridad en las Redes de Datos'
- Manual teórico 'Administración de Servicios en el Sistema Informático'
- Manual teórico 'Prevención y Gestión de Ciberataques'

profesorado y servicio de tutorías

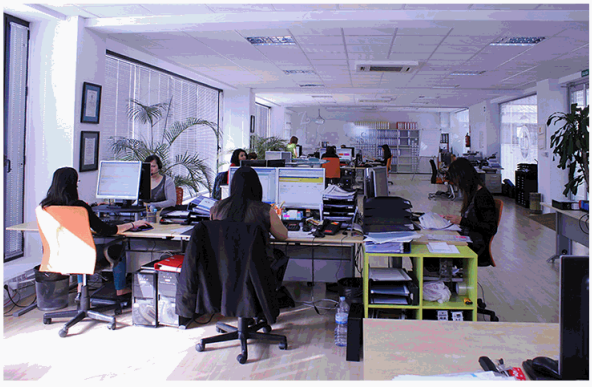
Nuestro equipo docente estará a su disposición para resolver cualquier consulta o ampliación de contenido que pueda necesitar relacionado con el curso. Podrá ponerse en contacto con nosotros a través de la propia plataforma o Chat, Email o Teléfono, en el horario que aparece en un documento denominado “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



+ Información Gratis

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

+ Información Gratis

programa formativo

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

+ Información Gratis

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 INFORMACIÓ

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

+ Información Gratis

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

+ Información Gratis

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 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
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

+ Información Gratis

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

+ Información Gratis

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

+ Información Gratis