EUROINNOVA FORMACION
INTERNATIONAL BUSINESS SCHOOL

Postgrado en Sistemas de Gestión Iso 27001: Experto Auditor Iso 27001 + Gestor de Sistemas de Seguridad de la Información 27001

Información gratis Postgrado en Sistemas de Gestión Iso 27001: Experto Auditor Iso 27001 + Gestor de Sistem

Titulación certificada por EUROINNOVA BUSINESS SCHOOL

Postgrado en Sistemas de Gestión Iso 27001: Experto Auditor Iso 27001 + Gestor de Sistemas de Seguridad de la Información 27001

Duración: 420 horas

Precio: 260 € *

Modalidad: Online

* Materiales didácticos, titulación y gastos de envío incluidos.

Postgrado en Sistemas de Gestión Iso 27001: Experto Auditor Iso 27001 + Gestor de Sistemas de Seguridad de la Información 27001

Descripción

Este Curso Online en Sistemas de Gestión Iso 27001: Experto Auditor Iso 27001 + Gestor de Sistemas de Seguridad de la Informaci 27001le ofrece una formación especializada en la materia. La Norma UNE-ISO/IEC 27001 está elaborada para emplearse en cualqui tipo de organización: pública o privada, sea cual sea su tamaño: grandes corporaciones, pequeñas y medianas empresas, etc. La adec 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.

Euroinnova Business School

Euroinnova Business School, es una escuela de negocios avalada por 5 universidades y múltiples instituciones a nivel internacional. En el siguiente enlace puede ver los **cursos Homologados**

Además Euroinnova cuenta con más de 10.000 **cursos online**

Puede matricularse hoy con un 10% de descuento, si se matricula online en el siguiente enlace:

Al formar parte de Euroinnova podrás disponer de los siguientes servicios totalmente gratis, además de pasar a formar parte de una escuela de negocios con un porcentaje de satisfacción de más del 95%, auditada por agencias externas, además de contar con el apoy de las principales entidades formativas a nivel internacional.

Postgrado en Sistemas de Gestión Iso 27001: Experto Auditor Iso 27001 + Gestor de Sistemas de Seguridad de la Información 27001

A quién va dirigido

Este Curso Online en Sistemas de Gestión Iso 27001: Experto Auditor Iso 27001 + Gestor de Sistemas de Seguridad de la Información 27001 va dirigido a empresarios que deseen implantar un sistema de gestión de la calidad. Departamentos de recursos humanos, consultoras, técnicos en medioambiente, estudiantes y licenciados universitarios que deseen encaminar su carrera profesio al incipiente mercado de la certificación, gestión y auditoría de la calidad. Profesionales de los sectores relacionados con el mundo d la calidad o el medio ambiente.

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.

Para que te prepara

Este Curso en Sistemas de Gestión Iso 27001: Experto Auditor Iso 27001 + Gestor de Sistemas de Seguridad de la Información 27001 le prepara para gestionar el departamento de calidad de una empresa, así como para conocer los elementos que intervienen en el proceso de certificación en el área de la Seguridad de la Información.

Salidas laborales

Auditor de sistemas de calidad, Directivos del Departamento de calidad.

Titulación

Doble Titulación Expedida por EUROINNOVA BUSINESS SCHOOL y Avalada por la Escuela Superior de Cualificaciones Profesionales

EUROINNOVA BUSINESS SCHOOL
TITULACIÓN EXPEDIDA POR EUROINNOVA BUSINESS SCHOOL CENTRO DE ESTUDIOS DE POSTGRADO

CUALIFICA2
Titulación Avalada Para El Desarrollo De Las Competencias Profesionales R.D. 1224/2009

Una vez finalizado el curso, el alumno recibirá por parte de Euroinnova Formación vía correo postal, la titulación que acredita el hab con éxito todas las pruebas de conocimientos propuestas en el mismo.

Esta titulación incluirá el nombre del curso/master, la duración del mismo, el nombre y DNI del alumno, el nivel de aprovechamient que acredita que el alumno superó las pruebas propuestas, las firmas del profesor y Director del centro, y los sellos de la institucione que avalan la formación recibida (Euroinnova Formación, Instituto Europeo de Estudios Empresariales y Comisión Internacional par la Formación a Distancia de la UNESCO).

EUROINNOVA FORMACION

como centro de Formación acreditado para la impartición a nivel nacional de formación
EXPIDE EL PRESENTE TÍTULO PROPIO

NOMBRE DEL ALUMNO/A

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

Nombre de la Acción Formativa

de XXX horas, perteneciente al Plan de Formación EUROINNOVA en la convocatoria de 2014
Y para que surtan los efectos pertinentes queda registrado con Número de Expediente XXXX/XXXX-XXXX-XXXX-XXXXXX
Con una calificación de SOBRESALIENTE

Y para que conste expido la presente TITULACIÓN en
Granada, a 23 de Abril de 2014

La direccion General

El/La interesado/a

Sello

Forma de financiación

- Contrarrembolso.
- Transferencia.
- Tarjeta de crédito.
- PayPal

Otros: PayU, Sofort, Western Union, SafetyPay

Llama gratis al 900831200 e informate de los pagos a plazos sin intereses que hay disponibles

Metodología

Entre el material entregado en este curso se adjunta un documento llamado Guía del Alumno dónde aparece un horario de tutorías telefónicas y una dirección de e-mail dónde podrá enviar sus consultas, dudas y ejercicios. Además recibirá los materiales didácticos que incluye el curso para poder consultarlos en cualquier momento y conservarlos una vez finalizado el mismo.La metodología a seguir es ir avanzando a lo largo del itinerario de aprendizaje online, que cuenta con una serie de temas y ejercicios. Para su evaluación, el alumno/a deberá completar todos los ejercicios propuestos en el curso. La titulación será remitida al alumno/a por correo una vez se haya comprobado que ha completado el itinerario de aprendizaje satisfactoriamente.

Materiales didácticos

- Maletín porta documentos
- Manual teórico 'Seguridad en Equipos Informáticos'
- Manual teórico 'Sistema de Gestión de Seguridad de la Información UNE-ISO/IEC 27001:2017'
- Subcarpeta portafolios
- Dossier completo Oferta Formativa
- Carta de presentación
- Guía del alumno
- Bolígrafo

Profesorado y servicio de tutorías

Nuestro centro tiene su sede en el "Centro de Empresas Granada", un moderno complejo empresarial situado en uno de los centros de negocios con mayor proyección de Andalucía Oriental. Contamos con una extensa plan 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.

Plazo de finalización

El alumno cuenta con un período máximo de 12 meses para la finalización del curso, a contar desde la fecha de recepción de las mat del mismo.

Si una vez cumplido el plazo no se han cumplido los objetivos mínimos exigidos (entrega de ejercicios y evaluaciones correspondientes), el alumno podrá solicitar una prórroga con causa justificada de 3 meses.

Bolsa de empleo

El alumno tendrá la posibilidad de incluir su currículum en nuestra bolsa de empleo y prácticas, participando así en los distintos procesos de selección y empleo gestionados por más de 2000 empresas y organismos públicos colaboradores, en todo el territorio nacional.

Agencia de colocación autorizada Nº 9900000169

Club de alumnos

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.

Programa formativo

PARTE 1. GESTIÓN DE SISTEMAS DE SEGURIDAD DE LA INFORMACIÓN ISO 27001

MÓDULO 1. LA SEGURIDAD DE LA INFORMACIÓN

UNIDAD DIDÁCTICA 1. NATURALEZA Y DESARROLLO DE LA SEGURIDAD DE LA INFORMACIÓN

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
1.- Principio Básico de Confidencialidad
2.- Principio Básico de Integridad
3.- Disponibilidad
5.Descripción de los riesgos de la seguridad
6.Selección de controles
7.Factores de éxito en la seguridad de la información

UNIDAD DIDÁCTICA 2. NORMATIVA ESENCIAL SOBRE SEGURIDAD DE LA INFORMACIÓN

1.Marco legal y jurídico de la seguridad de la información
2.Normativa comunitaria sobre seguridad de la información
1.- Planes de acción para la utilización más segura de Internet
2.- Estrategias para una sociedad de la información más segura
3.- Ataques contra los sistemas de información
4.- La lucha contra los delitos informáticos
5.- La Agencia Europea de Seguridad de las Redes y de la información (ENISA)
3.Normas sobre gestión de la seguridad de la información: Familia de Normas ISO 27000
1.- Familia de Normas ISO 27000
2.- Norma ISO/IEC 27002:2009
4.Legislación española sobre seguridad de la información
1.- La protección de datos de carácter personal
2.- La Ley Orgánica - de 13 de diciembre, de Protección de Datos de Carácter Personal
3.- El Real Decreto - de 21 de diciembre, por el que se aprueba el Reglamento de desarrollo de la Ley Orgánica - de 13 de diciembre, de protección de datos de carácter personal
4.- La Agencia Española de Protección de Datos

5.- El Real Decreto - de 8 de enero, por el que se regula el Esquema Nacional de Seguridad en el ámbito de la Administración Electrónica

6.- Ley - de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas

7.- La Ley - de 11 de julio, de servicios de la sociedad de la información y del comercio electrónico

8.- La Ley - de 9 de mayo, General de Telecomunicaciones

9.- La Ley - de 19 de diciembre, de firma electrónica

10.- La Ley de propiedad intelectual

11.- La Ley de propiedad industrial

UNIDAD DIDÁCTICA 3. BUENAS PRÁCTICAS EN SEGURIDAD DE LA INFORMACIÓN: NORMA ISO/IEC 27002

1.Aproximación a la norma ISO/IEC 27002

2.Alcance de la Norma ISO/IEC 27002

3.Estructura de la Norma ISO/IEC 27002

1.- Las cláusulas del control de seguridad

2.- Las principales categorías de seguridad

4.Evaluación y tratamiento de los riesgos de seguridad

1.- Evaluación de los riesgos de seguridad

2.- Tratamiento de los riesgos de seguridad

UNIDAD DIDÁCTICA 4. POLÍTICA DE SEGURIDAD, ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN Y GESTIÓN DE ACTIVOS

1.Política de seguridad de la información

1.- Etapas en el desarrollo de una política de seguridad de la información

2.- Características esenciales de una política de seguridad de la información

3.- Documento de política de la seguridad de la información

4.- Revisión de la política de seguridad de la información

2.Organización de la seguridad de la información

3.Organización interna de la seguridad de la información

1.- Compromiso de la dirección con la seguridad de la información

2.- Coordinación de la seguridad de la información

3.- Asignación de responsabilidad de seguridad de la información

4.- Autorización de procesos para facilidades procesadoras de la información

5.- Acuerdos de confidencialidad para la protección de la información

6.- Contacto con las autoridades y con grupos de interés especial en los incidentes de seguridad

7.- Revisión independiente de la seguridad de la información

4.Grupos o personas externas: el control de acceso a terceros

1.- Identificación de los riesgos de seguridad relacionados con personas externas

2.- Tratamiento de la seguridad de la información en las relaciones con los clientes

3.- Tratamiento de la seguridad de la información en acuerdos con terceros

5.Clasificación y control de activos de seguridad de la información

6.Responsabilidad por los activos de seguridad de la información

1.- Inventario de los activos de seguridad de la información

2.- Propiedad de los activos de seguridad de la información
3.- Uso aceptable de los activos de seguridad de la información
7.Clasificación de la información
1.- Lineamientos de clasificación de la información
2.- Etiquetado y manejo de información

UNIDAD DIDÁCTICA 5. SEGURIDAD FÍSICA, AMBIENTAL Y DE LOS RECURSOS HUMANOS

1.Seguridad de la información ligada a los recursos humanos
2.Medidas de seguridad de la información antes del empleo
1.- Establecimiento de roles y responsabilidades de los candidatos
2.- Investigación de antecedentes de los candidatos para el empleo
3.- Términos y condiciones del empleo
3.Medidas de seguridad de la información durante el empleo
1.- Responsabilidades de la gerencia o dirección de la organización
2.- Conocimiento, educación y capacitación en seguridad de la información
3.- Incumplimiento de las previsiones relativas a la seguridad de la información: el proceso disciplinario
4.Seguridad de la información en la finalización de la relación laboral o cambio de puesto de trabajo
1.- Responsabilidades de terminación
2.- Devolución de los activos
3.- Cancelación de los derechos de acceso a la información
5.Seguridad de la información ligada a la seguridad física y ambiental o del entorno
6.Las áreas seguras
1.- El perímetro de seguridad física
2.- Los controles de ingreso físico
3.- Seguridad de oficinas, locales, habitaciones y medios
4.- Protección contra amenazas internas y externas a la información
5.- El trabajo en áreas aseguradas
6.- Áreas de carga y descarga
7.Los equipos de seguridad
1.- Seguridad en el emplazamiento y protección de equipos
2.- Instalaciones de suministro seguras
3.- Protección del cableado de energía y telecomunicaciones
4.- Mantenimiento de los equipos
5.- Seguridad de los equipos fuera de las instalaciones
6.- Reutilización o retirada segura de equipos
7.- Retirada de materiales propiedad de la empresa
8.- Equipo de usuario desatendido
9.- Política de puesto de trabajo despejado y pantalla limpia

UNIDAD DIDÁCTICA 6. GESTIÓN DE LAS COMUNICACIONES Y OPERACIONES

1.Aproximación a la gestión de las comunicaciones y operaciones
2.Procedimientos y responsabilidades operacionales
1.- Documentación de los procesos de operación

2.- La gestión de cambios en los medios y sistemas de procesamiento de información
3.- Gestión de capacidades
4.- Separación de los recursos de desarrollo, prueba y operación para reducir los riesgos de acceso no autorizado

3.Gestión de la prestación de servicios de terceras partes
1.- Política de seguridad de la información en las relaciones con los proveedores
2.- Requisitos de seguridad en contrato con terceros
3.- Cadena de suministros de tecnología de la información y de las comunicaciones

4.Planificación y aceptación del sistema
1.- Políticas para la seguridad de la información
2.- Revisión de las políticas para la seguridad de la información

5.Protección contra códigos maliciosos y móviles
1.- Controles contra el código malicioso
2.- Control contra códigos móviles

6.Copias de seguridad de la información

7.Gestión de la seguridad de la red
1.- Los controles de red
2.- La seguridad de los servicios de red
3.- Segregación en redes

8.Gestión de medios
1.- Gestión de medios removibles o extraíbles
2.- Eliminación de soportes o medios
3.- Soportes físicos en tránsito
4.- La seguridad de la documentación del sistema

9.El intercambio de información
1.- Políticas y procedimientos de intercambio de información
2.- Acuerdos de intercambio
3.- Seguridad de los soportes físicos en tránsito
4.- Mensajería electrónica
5.- Acuerdos de confidencialidad o no revelación

10.Los servicios de comercio electrónico
1.- Información relativa al comercio electrónico
2.- Las transacciones en línea
3.- La seguridad de la información puesta a disposición pública

11.Supervisión para la detección de actividades no autorizadas
1.- Registro de eventos
2.- Protección de la información de los registros
3.- La protección de la información de los registros
4.- Sincronización de reloj

UNIDAD DIDÁCTICA 7. EL CONTROL DE ACCESOS A LA INFORMACIÓN

1.El control de accesos: generalidades, alcance y objetivos
2.Requisitos de negocio para el control de accesos

1.- Política de control de acceso

3.Gestión de acceso de usuario

1.- Registro del usuario

2.- Gestión o administración de privilegios

3.- Gestión de contraseñas de usuario

4.- Revisión de los derechos de acceso de usuario

4.Responsabilidades del usuario

1.- El uso de contraseñas

2.- Protección de equipos desatendidos

3.- Política de puesto de trabajo despejado y pantalla limpia

5.Control de acceso a la red

1.- La política de uso de los servicios en red

2.- Autentificación de los usuarios de conexiones externas

3.- Identificación de equipos en las redes

4.- Diagnóstico remoto y protección de los puertos de configuración

5.- Segregación de las redes

6.- Control de la conexión a la red

7.- El control de routing o encaminamiento de red

6.Control de acceso al sistema operativo

1.- Procedimientos seguros de inicio de sesión

2.- Identificación y autentificación del usuario

3.- El sistema de gestión de contraseñas

4.- El uso de los recursos del sistema

5.- La desconexión automática de sesión

6.- Limitación del tiempo de conexión

7.Control de acceso a las aplicaciones y a la información

1.- Restricciones del acceso a la información

2.- Aislamiento de sistemas sensibles

8.Informática móvil y teletrabajo

1.- Los ordenadores portátiles y las comunicaciones móviles

2.- El teletrabajo

UNIDAD DIDÁCTICA 8. ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE LOS SISTEMAS DE INFORMACIÓN

1.Objetivos del desarrollo y mantenimiento de sistemas de información

2.Requisitos de seguridad de los sistemas de información

3.Tratamiento correcto de la información en las aplicaciones

1.- Validación de los datos de entrada

2.- El control de procesamiento interno

3.- La integridad de los mensajes

4.- Validación de los datos de salida

4.Controles criptográficos

1.- Política de uso de los controles criptográficos
2.- Gestión de claves

5.Seguridad de los archivos del sistema
1.- Control del software en explotación
2.- Protección de los datos de prueba en el sistema
3.- El control de acceso al código fuente de los programas

6.Seguridad de los procesos de desarrollo y soporte
1.- Procedimientos para el control de cambios
2.- Revisión técnica de aplicaciones tras efectuar cambios en el sistema operativo
3.- Restricciones a los cambios en los paquetes de software
4.- Entorno de desarrollo seguro
5.- Externalización de software por terceros

7.Gestión de la vulnerabilidad técnica

UNIDAD DIDÁCTICA 9. GESTIÓN DE INCIDENTES EN LA SEGURIDAD DE LA INFORMACIÓN Y DE LA CONTINUIDAD DEL NEGOCIO

1.La gestión de incidentes en la seguridad de la información

2.Notificación de eventos y puntos débiles en la seguridad de la información
1.- Notificación de los eventos en la seguridad de la información
2.- Notificación de puntos débiles de la seguridad

3.Gestión de incidentes y mejoras en la seguridad de la información
1.- Responsabilidades y procedimientos
2.- Aprendizaje de los incidentes de seguridad de la información
3.- Recopilación de evidencias

4.Gestión de la continuidad del negocio

5.Aspectos de la seguridad de la información en la gestión de la continuidad del negocio
1.- Inclusión de la seguridad de la información en el proceso de gestión de la continuidad del negocio
2.- Continuidad del negocio y evaluación de riesgos
3.- Desarrollo e implantación de planes de continuidad del negocio que incluyan la seguridad de la información
4.- Marco de referencia para la planificación de la continuidad del negocio
5.- Pruebas, mantenimiento y reevaluación de los planes de continuidad

UNIDAD DIDÁCTICA 10. CUMPLIMIENTO DE LAS PREVISIONES LEGALES Y TÉCNICAS

1.Cumplimiento de los requisitos legales
1.- Normativa aplicable
2.- Derechos de propiedad intelectual
3.- Protección de registros organizacionales
4.- Privacidad de la información personal
5.- Prevención del mal uso de los medios de procesamiento de la información
6.- Regulación de los controles criptográficos

2.Cumplimiento de las políticas y estándares de seguridad, y cumplimiento técnico
1.- Cumplimiento de las políticas y estándares de seguridad
2.- Verificación del cumplimiento técnico

3.Consideraciones de la auditoría de los sistemas de información
1.- Controles de auditoría de los sistemas de información
2.- Protección de las herramientas de auditoría de los sistemas de información

MÓDULO 2. EL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN

UNIDAD DIDÁCTICA 11. LA NORMA UNE-EN-ISO/IEC 27001:2017

1.Objeto y ámbito de aplicación
2.Relación con la Norma ISO/IEC 27002:2009
3.Definiciones y términos de referencia
4.Beneficios aportados por un sistema de seguridad de la información
5.Introducción a los sistemas de gestión de seguridad de la información

UNIDAD DIDÁCTICA 12. IMPLANTACIÓN DEL SISTEMA DE SEGURIDAD EN LA ORGANIZACIÓN

1.Contexto
2.Liderazgo
3.Planificación
1.- Acciones para tratar los riesgos y oportunidades
2.- Objetivos de seguridad de la información y planificación para su consecución
4.Soporte

UNIDAD DIDÁCTICA 13. SEGUIMIENTO DE LA IMPLANTACIÓN DEL SISTEMA

1.Operación
2.Evaluación del desempeño
1.- Seguimiento, medición, análisis y evaluación
2.- Auditoría interna
3.- Revisión por la dirección
3.Mejora
1.- No conformidad y acciones correctivas
2.- Mejora continua

PARTE 2. SEGURIDAD EN EQUIPOS INFORMÁTICOS

UNIDAD DIDÁCTICA 1. CRITERIOS GENERALES COMÚNMENTE ACEPTADOS SOBRE SEGURIDAD DE LOS EQUIPOS INFORMÁTICOS

1.Modelo de seguridad orientada a la gestión del riesgo relacionado con el uso de los sistemas de información
2.Relación de las amenazas más frecuentes, los riesgos que implican y las salvaguardas más frecuentes
3.Salvaguardas y tecnologías de seguridad más habituales
4.La gestión de la seguridad informática como complemento a salvaguardas y medidas tecnológicas

UNIDAD DIDÁCTICA 2. ANÁLISIS DE IMPACTO DE NEGOCIO

1.Identificación de procesos de negocio soportados por sistemas de información
2.Valoración de los requerimientos de confidencialidad, integridad y disponibilidad de los procesos de negocio
3.Determinación de los sistemas de información que soportan los procesos de negocio y sus requerimientos de seguridad

UNIDAD DIDÁCTICA 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. PLAN DE IMPLANTACIÓN DE SEGURIDAD

1.Determinación del nivel de seguridad existente de los sistemas frente a la necesaria en base a los requerimientos de seguridad de los procesos de negocio.

2.Selección de medidas de salvaguarda para cubrir los requerimientos de seguridad de los sistemas de información

3.Guía para la elaboración del plan de implantación de las salvaguardas seleccionadas

UNIDAD DIDÁCTICA 5. PROTECCIÓN DE DATOS DE CARÁCTER PERSONAL

1.Principios generales de protección de datos de carácter personal

2.Infracciones y sanciones contempladas en la legislación vigente en materia de protección de datos de carácter personal

3.Identificación y registro de los ficheros con datos de carácter personal utilizados por la organización

4.Elaboración del documento de seguridad requerido por la legislación vigente en materia de protección de datos de carácter personal

UNIDAD DIDÁCTICA 6. SEGURIDAD FÍSICA E INDUSTRIAL DE LOS SISTEMAS. SEGURIDAD LÓGICA DE SISTEMAS

1.Determinación de los perímetros de seguridad física

2.Sistemas de control de acceso físico más frecuentes a las instalaciones de la organización y a las áreas en las que estén ubicados los sistemas informáticos

3.Criterios de seguridad para el emplazamiento físico de los sistemas informáticos

4.Exposición de elementos más frecuentes para garantizar la calidad y continuidad del suministro eléctrico a los sistemas informáticos

5.Requerimientos de climatización y protección contra incendios aplicables a los sistemas informáticos

6.Elaboración de la normativa de seguridad física e industrial para la organización

7.Sistemas de ficheros más frecuentemente utilizados

8.Establecimiento del control de accesos de los sistemas informáticos a la red de comunicaciones de la organización

9.Configuración de políticas y directivas del directorio de usuarios

10.Establecimiento de las listas de control de acceso (ACLs) a ficheros

11.Gestión de altas, bajas y modificaciones de usuarios y los privilegios que tienen asignados

12.Requerimientos de seguridad relacionados con el control de acceso de los usuarios al sistema operativo

13.Sistemas de autenticación de usuarios débiles, fuertes y biométricos

14.Relación de los registros de auditoría del sistema operativo necesarios para monitorizar y supervisar el control de accesos

15.Elaboración de la normativa de control de accesos a los sistemas informáticos

UNIDAD DIDÁCTICA 7. IDENTIFICACIÓN DE SERVICIOS

1.Identificación de los protocolos, servicios y puertos utilizados por los sistemas de información

2.Utilización de herramientas de análisis de puertos y servicios abiertos para determinar aquellos que no son necesarios

3.Utilización de herramientas de análisis de tráfico de comunicaciones para determinar el uso real que hacen los sistemas de información de los distintos protocolos, servicios y puertos

UNIDAD DIDÁCTICA 8. ROBUSTECIMIENTO DE SISTEMAS

1.Modificación de los usuarios y contraseñas por defecto de los distintos sistemas de información

2.Configuración de las directivas de gestión de contraseñas y privilegios en el directorio de usuarios
3.Eliminación y cierre de las herramientas, utilidades, servicios y puertos prescindibles
4.Configuración de los sistemas de información para que utilicen protocolos seguros donde sea posible
5.Actualización de parches de seguridad de los sistemas informáticos
6.Protección de los sistemas de información frente a código malicioso
7.Gestión segura de comunicaciones, carpetas compartidas, impresoras y otros recursos compartidos del sistema
8.Monitorización de la seguridad y el uso adecuado de los sistemas de información

UNIDAD DIDÁCTICA 9. IMPLANTACIÓN Y CONFIGURACIÓN DE CORTAFUEGOS

1.Relación de los distintos tipos de cortafuegos por ubicación y funcionalidad
2.Criterios de seguridad para la segregación de redes en el cortafuegos mediante Zonas Desmilitarizadas / DMZ
3.Utilización de Redes Privadas Virtuales / VPN para establecer canales seguros de comunicaciones
4.Definición de reglas de corte en los cortafuegos
5.Relación de los registros de auditoría del cortafuegos necesarios para monitorizar y supervisar su correcto funcionamiento y los eventos de seguridad
6.Establecimiento de la monitorización y pruebas del cortafuegos

Terminos relacionados:

Anual, Auditor, Auditoria, Calidad, Carácter, certificado, Competencia, configuración, Cortafuegos, Datos, Departamento, Documentos, Empresas, equipos, Física, Formativo, Gestión, Implantación, Industrial, Información, Informáticos, Interna, ISO 27001, lógica, Módulo, Personal, Plan, Profesionalidad, Protección, Riesgos, Seguridad, sistemas, trabajo, Unidad, Verificación

EUROINNOVA BUSINESS SCHOOL

FICHA DE MATRICULACIÓN

Para efectuar su matrícula sólo tiene que hacernos llegar esta ficha con sus datos personales vía email a formacion@euroinnova.com.

POSTGRADO EN QUE DESEA MATRICULARSE: : .....

.....

Nombre: .....

Apellidos:.....

DNI/ID/Pasaporte:.....

Domicilio envío: .....

..... CP:.....

Localidad:.....

Provincia:..... País:.....

Teléfono:..... E-mail:.....

Horario de entrega (Mañana o tarde).....

Forma de pago .....

Observaciones:.....

Una vez recibidos los datos personales, uno de nuestros asesores pedagógicos contactará con usted para concretar la matrícula y confirmarle cuando va a recibir todos los materiales en su domicilio.

EUROINNOVA BUSINESS SCHOOL

DESDE ESPAÑA LLAMA GRATIS A:	DESDE FUERA DE ESPAÑA:
900 831 200	+ 34 958 05 02 00

EUROINNOVA FORMACIÓN
POLÍGONO INDUSTRIAL LA ERMITA.
EDIF. CENTRO DE EMPRESAS GRANADA. OFICINA 1º D • 18230 ATARFE - GRANADA
Teléfono: 958 050 200