

DIPLOMADO "GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN Y AUDITORÍA DE SISTEMAS"

Horas Totales 140

(104 horas teoría interactiva + 36 de laboratorio)

MÓDULO I - SEGURIDAD INFORMÁTICA EMPRESARIAL 20 HORAS (20 horas teoría interactiva)

1. Curso : **Seguridad Empresarial I** (20 horas)
 - a. Este módulo permitirá al participante conocer las normas Estándares de seguridad de información, así como su metodología de implantación en las empresas.
 - b. Contenido del Curso
 - Norma BS 7799
 - Norma NTP/ISO 17799
 - Metodología de implantación
 - Fases en la Implantación
 - Sistema de Gestión de Seguridad de la Información
 - Identificación de procesos críticos

MÓDULO II - DISEÑO DE POLÍTICAS DE SEGURIDAD y GESTION DE RIESGOS 30 horas (18 horas teoría + 12 LAB)

1. Curso : **Seguridad Empresarial II** (18 horas)
 - a. Permitirá al participante el diseño de políticas de seguridad y gestión de riesgos dentro de entornos de Informática y TI.
 - b. Marco de los temas del módulo.
 - Políticas y procedimientos de seguridad empresariales
 - Diseño de políticas de acuerdo al entorno tecnológico
 - Diseño de políticas de acuerdo a la necesidad de protección de datos
 - Diseño de políticas de acuerdo a estándares internacionales
 - Normas y metodologías estándares para el diseño de políticas de seguridad.
 - Evaluación de riesgos:
 - Operativos de la empresa
 - En operaciones y servicios de informática
 - En proyectos de sistemas
 - En las aplicaciones críticas
 - En el procedimiento de información
 - En las redes de datos
 - En el desarrollo de aplicaciones y programas producto Gestión de los riesgos de las TI
 - Evaluación de los diversos tipos de riesgos informáticos y su relación con las políticas empresariales
 - Procesos y marco de acción para delimitar los riesgos tecnológicos y de información.

1. Laboratorio
Herramientas. Uso de herramientas para:
 - Analizar paquetes TCP/IP
 - Detector de sniffers
 - Análisis ARP
 - Generador de auditorías de software y hardware
 - Eliminador de cookies
 - Redireccionamiento de puertos
 - Analizador de puertos TCP y UDP
 - Comprobador de proxies
 - Escáner de vulnerabilidades

MÓDULO III - SISTEMAS DE SEGURIDAD – 30 horas (18 horas teoría + 12 LAB.)

2. Curso : **Sistemas de seguridad**
 - a. Este módulo proporcionará al participante los conocimientos de las herramientas y tecnologías existentes para los entornos informáticos y de TI relacionados a su aplicación en la seguridad.
 - b. Marco de los temas del módulo
Tecnología de seguridad de información
 - Criptografía
 - PKI – Certificados y firma digital
 - Tools: Firewalls, IDS, VPN, Smart cards

- Remote access servers
 - Dispositivos biométricos
 - Plataformas comerciales: SSL, SET y 3D – Secure
 - Seguridad en redes Inalámbricas
 - Tendencias de seguridad en las TI
2. Laboratorio
Firewalls & Detección de Intrusos
1. Protocolos y Puertos: Herramientas TCP/IP
 2. Panorámica de los FW y las herramientas IDS
 3. Identificación de los FW y las herramientas IDS
 4. Descubrimiento avanzado de los FW y las herramientas IDS
 5. Exploración a través de los FW
 6. Filtrado de paquetes
 7. Vulnerabilidades de los proxy de aplicación
 8. Prácticas con ISA Server y otras herramientas FW y de Detección de intrusos

MÓDULO IV – AUDITORÍA de SISTEMAS DE INFORMACIÓN – 36 horas (24 horas teoría + 12 LAB.)

1. Curso : **COBIT I Directrices de Auditoria de tecnologías de la Información**
(24 horas)
 - a. Permitirá al participante conocer los principios de la auditoria de sistemas y la aplicación del marco de trabajo, dominios del COBIT, en los procesos de auditoria de sistemas de información.
 - b. Marco de los temas del módulo

Introducción a la Auditoria de Sistemas

- Concepto de Auditoria.
- Definición de Auditoria de TI
- Objetivos de la Auditoria de TI
- Planeación de la Auditoria
- Investigación Preliminar
- El Equipo de Auditoria
- Herramientas de Auditoria
- El proceso de la Auditoria
- La Comunicaciones de los resultados
- El Seguimiento de las Recomendaciones

"Aplicación de las Directrices de Auditoria por Proceso y Dominio".

Planeación y Organización.

- Plan estratégico de Tecnología de Información.
- Arquitectura de información.
- Determinación de la dirección tecnológica.
- Determinación de la organización y de las funciones de TI.
- Manejo de la inversión en tecnología de Información.
- Administración de los recursos humanos.
- Aseguramiento del cumplimiento de requerimientos externos.
- Evaluación de riesgos.
- Administración de proyectos y Administración de la calidad.

Adquisición e implementación.

- Administración e identificación de soluciones.
- Adquisición y mantenimiento de software e aplicación.
- Adquisición y mantenimiento de arquitectura tecnológica.
- Desarrollo y mantenimiento de Procedimientos en Tecnologías de la Información.
- Instalación y acreditación de sistemas.
- Administración de Cambios.

Entrega y Soporte.

- Niveles del servicio.

- Administración de los servicios.
 - Administración de los servicios prestados por terceros.
 - Administración de Desempeño y capacidades.
 - Aseguramiento del servicio continuo.
 - Garantizar la seguridad de los sistemas.
 - Identificación y asignación de costo.
 - Educación y entrenamiento de usuarios.
 - Apoyo y asistencia para los clientes de Tecnología de Información.
 - Administración de la configuración.
 - Manejo de problemas e incidentes.
 - Administración de datos.
 - Administración de las instalaciones.
 - Manejo de las Operaciones.
 - Directrices de Auditoria - Monitoreo
 - Monitorear los procesos.
 - Evaluar la suficiencia del control interno.
 - Obtener el aseguramiento independiente.
 - Preparar auditorias independientes.
2. Laboratorio
ACL (12 horas)
- 1) Uso y aplicaciones del ACL

MÓDULO V – AUDITORÍA de SISTEMAS DE INFORMACIÓN PARTE II – 24 horas (24 horas teórico - Práctico)

1. Curso : **COBIT II (Implementación de Objetivos de Control para TI)** (24 horas)
 - c. Permitirá al participante complementar los conocimientos adquiridos acerca de los dominios de los dominios del COBIT, y su aplicación en los procesos de gestión de tecnologías de la información.
 - d. Marco de los temas del módulo
 - El proceso de Implementación
 - Aplicación del CSA para TI
 - Configuración de parámetros.- Dominios y Procesos de Tecnología a evaluar.
 - Factores de Riesgo
 - Determinación de los objetivos de control
 - Evaluación del Control Interno de TI
 - Análisis de riesgo de TI
 - Balance Score Card (BSC) de Tecnologías de Información.
 - Indicadores clave de objetivo.
 - Indicadores clave de desempeño.
 - Factores críticos de éxito.
 - Modelo de madurez genérico.
 - Resultados por Dominio
 - Generación Informe Final.