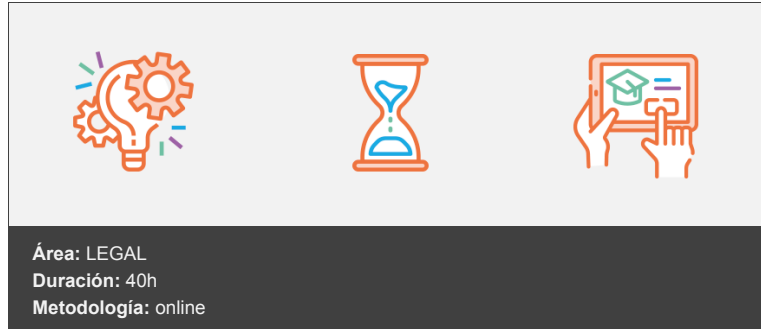


## Auditoría de seguridad informática y de protección de datos personales



### Objetivos

Con la realización del presente curso el alumnado adquirirá los conocimientos necesarios para auditar redes de comunicación y sistemas informáticos.

Más concretamente, será capaz de:

- Analizar y seleccionar las herramientas de auditoría y detección de vulnerabilidades del sistema informático implantando aquellas que se adecuen a las especificaciones de seguridad informática de la organización.
- Planificar y aplicar medidas de seguridad para garantizar la integridad del sistema informático y de los puntos de entrada y salida de la red departamental.
- Llevar a cabo auditorías de sistemas y de la información para la obtención de certificaciones, siguiendo una metodología específica.
- Llevar a cabo Auditorías de Datos para validar si una empresa u organización cumple con la actual normativa de protección de datos personales.

### Contenidos y estructura del curso

#### 1 - Criterios generales sobre Auditoría Informática

- Criterios generales sobre Auditoría Informática
- Introducción
- Concepto de Auditoría
- Código deontológico de la función de auditoría
- Normas profesionales y código de ética
- Principios Deontológicos Aplicables a los Auditores Informáticos
- Relación de los distintos tipos de auditoría en el marco de los sistemas de información
- Criterios a seguir para la composición del equipo auditor
- Aspectos a considerar en la composición del equipo auditor
- Funciones generales del equipo auditor
- Conocimientos y destrezas del equipo auditor
- Responsabilidad Profesional
- Tipos de pruebas a realizar en el marco de la auditoría, pruebas sustantivas y pruebas de cumplimiento
- Pruebas de cumplimiento
- Pruebas sustantivas
- Ejemplo de Pruebas de Cumplimiento y Sustantivas
- Tipos de muestreo a aplicar durante el proceso de auditoría
- Métodos de muestreo representativo o estadístico
- Técnicas de selección para el muestreo en la auditoría

- Utilización de herramientas tipo CAAT (Computer Assisted Audit Tools)
- Software de Auditoría
- Datos de prueba
- Otros componentes de las CAAT
- Utilización de CAATs
- Explicación de los requerimientos que deben cumplir los hallazgos de auditoría
- Requisitos de un hallazgo de auditoría
- Elementos de un hallazgo de auditoría
- Comunicación de los hallazgos de auditoría
- Aplicación de criterios comunes para categorizar los hallazgos como observaciones o no conformidades
- Relación de las normativas y metodologías relacionadas con la auditoría de sistemas de información comúnmente aceptadas
- Normas de Auditoría Generalmente Aceptadas (NAGAS)
- Metodologías relacionadas con la Auditoría de Sistemas de Información
- Resumen de la Unidad

## **2 - Análisis de Riesgos en los Sistemas de Información: Identificación de Vulnerabilidades y Amenazas**

- Análisis de Riesgos en los Sistemas de Información: Identificación de Vulnerabilidades y Amenazas
- Introducción
- Objetivos de la unidad
- Introducción a los contenidos
- Términos relacionados con la seguridad informática
- Introducción al análisis de riesgos
- Análisis de riesgos
- Reducción del Riesgo: Mecanismos de Seguridad (Controles)
- Vulnerabilidades del sistema
- Tipos de Vulnerabilidades
- Criterios de programación segura
- Particularidades de los distintos tipos de código malicioso
- Principales elementos del análisis de riesgos y sus modelos de relaciones
- Metodologías cualitativas y cuantitativas de análisis de riesgos
- Métodos Cualitativos
- Métodos Cuantitativos
- Identificación y valoración de los activos involucrados en el análisis de riesgos
- El inventario de activos
- Valoración de los activos
- Identificación de las amenazas que pueden afectar a los activos
- Naturaleza de las amenazas
- Amenazas Físicas
- Descripción de algunas amenazas físicas
- Amenazas Lógicas
- Algunas amenazas lógicas
- Análisis e identificación de las vulnerabilidades existentes
- Pensando como el enemigo
- Pruebas de Penetración
- Evaluación de vulnerabilidad
- Establecimiento de una metodología
- Herramientas de evaluación de vulnerabilidades
- Resumen

## **3 - Análisis de Riesgos en los Sistemas de Información: Plan de Gestión de Riesgos**

- Análisis de Riesgos en los Sistemas de Información: Plan de Gestión de Riesgos
- Introducción
- Objetivos de la unidad
- Introducción a los contenidos
- El Informe de Auditoría
- Mecanismo de salvaguarda vs Funciones de salvaguarda
- Funciones de Salvaguarda en sistemas de información
- Establecimiento de los escenarios de riesgo
- Determinación de la probabilidad e impacto de materialización de los escenarios
- Establecimiento del nivel de riesgo para los distintos pares de activo y amenaza
- ¿Cómo valorar la probabilidad de una amenaza?
- ¿Cómo valorar la magnitud del daño?
- Criterios de Evaluación de Riesgo
- Relación de las distintas alternativas de gestión de riesgos
- Guía para la elaboración del Plan de Gestión de Riesgos

- Exposición de la metodología NIST SP 800-30
- Exposición de la metodología Magerit versión 3
- Método MAGERIT
- Catálogo de elementos MAGERIT
- Guía de Técnicas MAGERIT
- Resumen

#### **4 - Herramientas de Análisis de Red y de Vulnerabilidades en la Auditoría de Sistemas de Información**

- Uso de Herramientas para la Auditoría de Sistemas
- Introducción
- Objetivos de la unidad
- Introducción a los contenidos
- Instrucciones de instalación de los laboratorios virtuales
- Herramientas del sistema operativo
- Ping
- Traceroute
- DNS lookup
- ssh
- netstat
- ipconfig/ifconfig
- Herramientas de análisis de red, puertos y servicios
- Nmap
- Escaneo de Puertos
- NBTScan
- Netcat
- Herramientas de análisis de vulnerabilidades
- Manejo de usuarios en Nessus
- Configuración del análisis
- Proceso de análisis de vulnerabilidades
- Plugins
- Plugins en C
- Plugins en NASL
- Informes Nessus y análisis de resultados
- Resumen

#### **5 - Herramientas de Análisis de Web y de Protocolos en la Auditoría de Sistemas de Información**

- Herramientas de Análisis de Web y de Protocolos en la Auditoría de Sistemas de Información
- Introducción
- Objetivos de la unidad
- Introducción a los contenidos
- Instrucciones de instalación de los laboratorios virtuales
- Analizadores de protocolos
- WireShark
- Manual Básico de Wireshark
- DSniff
- Cain & Abel
- Analizadores de páginas web
- Acunetix
- Dirb
- Proxy Paros
- Ataques de diccionario y fuerza bruta
- John the Ripper
- Aircrack-ng: Auditoría inalámbrica
- Resumen

#### **6 - La función de los firewalls en Auditorías de Sistemas de Información**

- Firewalls en la Auditorías de Sistemas Informáticos
- Introducción
- Objetivos de la unidad
- Introducción a los contenidos
- Principios generales de firewalls
- Componentes de un firewall de red
- Filtrado de paquetes
- Especificación de las Reglas (ACL)

- Características: Pros y Contras
- El proxy de aplicación
- Ventajas e inconvenientes
- Pasarelas de nivel de circuito
- Monitorización y Detección de Actividad sospechosa
- SMLI
- Clasificación de los firewalls por ubicación y funcionalidad
- Arquitecturas de Firewalls de red
- Otras arquitecturas de firewalls de red
- Gestión Unificada de Amenazas: Firewalls UTM
- Resumen

## 7 - Guías para la ejecución de las distintas fases de la Auditoría de Sistemas de Información

- Guías para la ejecución de las distintas fases de la Auditoría en Sistemas de Información
- Introducción
- Objetivos de la unidad
- Introducción a los contenidos
- Guía para la auditoría de la documentación y normativa de seguridad existente en la organización auditada
- Investigación preliminar
- Guía para la elaboración del plan de auditoría
- Guía para las pruebas de auditoría
- Guía para la elaboración del informe de auditoría
- Formato del informe de auditoría
- Resumen

## 8 - Auditoría de la Protección de Datos

- Auditoría de la Protección de Datos
- Introducción
- Objetivos de la unidad
- Marco Jurídico de la Protección de Datos en España
- Principios Generales de la Protección de Datos
- La protección de datos en el Código Penal
- Normativa europea recogida en el Reglamento 2016/679
- Aplicación de la norma
- Síntesis
- Derechos del interesado o interesada
- Ley Orgánica de Protección de Datos Personales y garantía de los derechos digitales (LOPDGDD)
- Síntesis
- Autoridad de Control : La Agencia Española de Protección de Datos
- Funciones
- Poderes
- De investigación
- Correctivos
- De autorización y consultivos
- Medidas de cumplimiento
- Principios
- Responsable del tratamiento y encargado/a del tratamiento
- Delegado de protección de datos
- Registro de actividades de tratamiento
- Medidas de protección de datos desde el diseño y por defecto
- Análisis de riesgos y adopción de medidas de seguridad
- Notificación de quebras de seguridad
- Evaluaciones de impacto sobre la protección de datos
- Mecanismos de certificación y códigos de conducta
- Transferencias internacionales y normas corporativas vinculantes
- Herramientas de Auditoría de Protección de Datos
- Herramienta "Facilita\_RGPD" para datos de escaso riesgo
- Listado de cumplimiento
- Resumen

### Metodología

En Criteria creemos que para que la formación e-Learning sea realmente exitosa, tiene que estar basada en contenidos 100% multimedia (imágenes, sonidos, vídeos, etc.) diseñados con criterio pedagógico y soportados en una plataforma que ofrezca recursos de comunicación como chats, foros y conferencias...Esto se

logra gracias al trabajo coordinado de nuestro equipo e-Learning integrado por profesionales en pedagogía, diseño multimedia y docentes con mucha experiencia en las diferentes áreas temáticas de nuestro catálogo.

### Perfil persona formadora

Esta acción formativa será impartida por un/a experto/a en el área homologado/a por Critería, en cumplimiento con los procedimientos de calidad, con experiencia y formación pedagógica.

*En Critería queremos estar bien cerca de ti, ayúdanos a hacerlo posible:  
¡Suscríbete a nuestro blog y síguenos en redes sociales!*

Blog de Critería

