

1. Record Nr.	UNINA9911008962903321
Autore	Chicano Tejada Ester
Titolo	Auditoría de Seguridad Informática. IFCT0109
Pubbl/distr/stampa	Antequera : , : IC Editorial, , 2023 ©2023
ISBN	9788411035286 841103528X
Edizione	[1st ed.]
Descrizione fisica	1 online resource (125 pages)
Collana	Certificado de Profesionalidad ; IFCT0109-Seguridad Informatica
Disciplina	005
Soggetti	Seguridad informatica Libros electronicos.
Lingua di pubblicazione	Spagnolo
Formato	Materiale a stampa
Livello bibliografico	Monografía
Note generali	Incluye indice.
Nota di bibliografia	Incluye bibliografia.
Nota di contenuto	Intro -- Título -- Copyright -- Presentación del manual -- Índice -- Capítulo 1 Criterios generales comúnmente aceptados sobre auditoría informática -- 1. Introducción -- 2. Código deontológico de la función de auditoría -- 3. Relación de los distintos tipos de auditoría en el marco de los sistemas de la información -- 4. Criterios a seguir para la composición del equipo auditor -- 5. Tipos de pruebas a realizar en el marco de la auditoría. Pruebas sustantivas y pruebas de cumplimiento -- 6. Tipos de muestreo a aplicar durante el proceso de auditoría -- 7. Utilización de herramientas tipo CAAT (Computer Assisted Audit Tools) -- 8. Explicación de los requerimientos que deben cumplir los hallazgos de auditoría -- 9. Aplicación de criterios comunes para categorizar los hallazgos como observaciones o no conformidades -- 10. Relación de las normativas y metodologías relacionadas con la auditoría de sistemas de información comúnmente aceptadas -- 11. Resumen -- Ejercicios de repaso y autoevaluación -- Capítulo 2 Aplicación de la normativa de protección de datos de carácter personal -- 1. Introducción -- 2. Principios de protección de datos de carácter personal -- 3. Normativa europea recogida en la directiva 95/46/CE (Reglamento Europeo de Protección de Datos) -- 4. Normativa nacional recogida en el Código penal, Ley Orgánica para el Tratamiento Automatizado de Datos (LORTAD), Ley orgánica de Protección de Datos

(LOPD)/Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos y Garantía de Derechos Digitales (LOPDGDD) y Reglamento de desarrollo de la Ley Orgánica de Protección de Datos (R. D. 1720/2007)

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

6. Explicación de las medidas de seguridad para la protección de los datos de carácter personal recogidas en el Real Decreto 1720/2007 (RGPD y LOPDGDD)

-- 7. Guía para la realización de la auditoría bienal obligatoria de la Ley Orgánica 15/1999 de Protección de Datos de Carácter Personal (LOPD)/Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales (LOPDGDD)

-- 8. Resumen -- Ejercicios de repaso y autoevaluación -- Capítulo 3 Análisis de riesgos de los sistemas de información -- 1. Introducción -- 2. Introducción al análisis de riesgos -- 3. Principales tipos de vulnerabilidades, fallos de programa, programas maliciosos y su actualización permanente, así como criterios de programación segura -- 4. Particularidades de los distintos tipos de código malicioso (malware) -- 5. Principales elementos del análisis de riesgos y sus modelos de relaciones -- 6. Metodologías cualitativas y cuantitativas de análisis de riesgos -- 7. Identificación de los activos involucrados en el análisis de riesgos y su valoración -- 8. Identificación de las amenazas que pueden afectar a los activos identificados previamente -- 9. Análisis e identificación de las vulnerabilidades existentes en los sistemas de información que permitirían la materialización de amenazas, incluyendo análisis local, análisis remoto de caja blanca y de caja negra -- 10. Optimización del proceso de auditoría y contraste de vulnerabilidades e informe de auditoría -- 11. Identificación de las medidas de salvaguarda existentes en el momento de la realización del análisis de riesgos y su efecto sobre las vulnerabilidades y amenazas -- 12. Establecimiento de los escenarios de riesgo entendidos como pares activo-amenaza susceptibles de materializarse -- 13. Determinación de la probabilidad e impacto de materialización de los escenarios.

14. Establecimiento del nivel de riesgo para los distintos pares de activo y amenaza -- 15. Determinación por parte de la organización de los criterios de evaluación del riesgo, en función de los cuales se determina si un riesgo es aceptable o no -- 16. Relación de las distintas alternativas de gestión de riesgos -- 17. Guía para la elaboración del plan de gestión de riesgos -- 18. Exposición de la metodología NIST SP 800-30 -- 19. Exposición de la metodología Magerit versión 2 -- 20. Resumen -- Ejercicios de repaso y autoevaluación -- Capítulo 4 Uso de herramientas para la auditoría de sistemas -- 1. Introducción -- 2. Herramientas del sistema operativo tipo Ping, Traceroute, etc. -- 3. Herramientas de análisis de red, puertos y servicios tipo Nmap, Netcat, NBTScan, etc. -- 4. Herramientas de análisis de vulnerabilidades tipo Nessus -- 5. Analizadores de protocolos tipo Wireshark, DSniff, Cain & Abel, etc. -- 6. Analizadores de páginas web tipo Acunetix, Dirb, Parosproxy, etc. -- 7. Ataques de diccionario y fuerza bruta tipo Brutus, John the Ripper, etc. -- 8. Resumen -- Ejercicios de repaso y autoevaluación -- Capítulo 5 Descripción de los aspectos sobre cortafuegos en auditorías de sistemas informáticos -- 1. Introducción -- 2. Principios generales de cortafuegos -- 3. Componentes de un cortafuegos de red -- 4. Relación de los distintos tipos de cortafuegos por ubicación y funcionalidad -- 5. Arquitecturas de cortafuegos de red -- 6. Otras arquitecturas de cortafuegos de red -- 7. Resumen -- Ejercicios de repaso y autoevaluación -- Capítulo 6 Guías para la ejecución de las distintas fases de la auditoría de sistema de información -- 1. Introducción -- 2. Guía para la auditoría de la documentación y

normativa de seguridad existente en la organización auditada -- 3.
Guía para la elaboración del plan de auditoría.
4. Guía para las pruebas de auditoría -- 5. Guía para la elaboración del informe de auditoría -- 6. Resumen -- Ejercicios de repaso y autoevaluación -- Bibliografía.
