1. Record Nr. UNINA9911008963603321

Autore	Giménez Albacete José Francisco
Titolo	Seguridad en Equipos Informáticos. IFCT0109
Pubbl/distr/stampa	Antequera : , : IC Editorial, , 2023 ©2023
ISBN	9788411035934 841103593X
Edizione	[1st ed.]
Descrizione fisica	1 online resource (260 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	Monografia
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 seguridad de los equipos informáticos -- 1. Introducción -- 2. Modelo de seguridad orientada a la gestión del riesgo relacionado con el uso de los sistemas de información -- 3. Relación de las amenazas más frecuentes, los riesgos que implican y las salvaguardas más frecuentes -- 4. Salvaguardas y tecnologías de seguridad más habituales -- 5. La gestión de la seguridad informática como complemento a salvaguardas y medidas tecnológicas -- 6. Resumen -- Ejercicios de repaso y autoevaluación -- Capítulo 2 Análisis de impacto de negocio -- 1. Introducción -- 2. Identificación de procesos de negocio soportados por sistemas de información -- 3. Valoración de los requerimientos de confidencialidad, integridad, y disponibilidad de los procesos de negocio -- 4. Determinación de los sistemas de información que soportan los procesos de negocio y sus requerimientos de seguridad -- 5. Resumen -- Ejercicios de repaso y autoevaluación -- Capítulo 3 Gestión de riesgos -- 1. Introducción -- 2. Aplicación del proceso de gestión de riesgos y exposición de las alternativas más frecuentes -- 3. Metodologías comúnmente aceptadas de identificación y análisis de riesgos -- 4. Aplicación de controles y medidas de salvaguarda para obtener una reducción del riesgo -- 5. Resumen -- Ejercicios de repaso

y autoevaluación -- Capítulo 4 Plan de implantación de seguridad -- 1. Introducción -- 2. 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 -- 3. Selección de medidas de salvaguarda para cubrir los requerimientos de seguridad de los sistemas de información -- 4. Guía para la elaboración del plan de implantación de las salvaguardas seleccionadas.
5. Resumen -- Ejercicios de repaso y autoevaluación -- Capítulo 5 Protección de datos de carácter personal -- 1. Introducción -- 2. Principios generales de protección de datos de carácter personal -- 3. Infracciones y sanciones contempladas en la legislación vigente en materia de protección de datos de carácter personal -- 4. Identificación y registro de los ficheros con datos de carácter personal utilizados por la organización -- 5. Elaboración del documento de seguridad requerido por la legislación vigente en materia de protección de datos de carácter personal -- 6. Resumen -- Ejercicios de repaso y autoevaluación -- Capítulo 6 Seguridad física e industrial de los sistemas. Seguridad lógica de sistemas -- 1. Introducción -- 2. Determinación de los perímetros de seguridad física -- 3. 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 -- 4. Criterios de seguridad para el emplazamiento físico de los sistemas informáticos -- 5. Exposición de elementos más frecuentes para garantizar la calidad y continuidad del suministro eléctrico a los sistemas informáticos -- 6. Requerimientos de climatización y protección contra incendios aplicables a los sistemas informáticos -- 7. Elaboración de la normativa de seguridad física e industrial para la organización -- 8. Sistemas de ficheros más frecuentemente utilizados -- 9. Establecimiento del control de accesos de los sistemas informáticos a la red de comunicaciones de la organización -- 10. Configuración de políticas y directivas del directorio de usuarios -- 11. Establecimiento de las listas de control de acceso (ACL) a ficheros -- 12. Gestión de altas, bajas y modificaciones de usuarios y los privilegios que tienen asignados.
13. Requerimientos de seguridad relacionados con el control de acceso de los usuarios al sistema operativo -- 14. Sistemas de autenticación de usuarios débiles, fuertes y biométricos -- 15. Relación de los registros de auditoría del sistema operativo necesarios para monitorizar y supervisar el control de accesos -- 16. Elaboración de la normativa de control de accesos a los sistemas informáticos -- 17. Resumen -- Ejercicios de repaso y autoevaluación -- Capítulo 7 Identificación de servicios -- 1. Introducción -- 2. Identificación de los protocolos, servicios y puertos utilizados por los sistemas de información -- 3. Utilización de herramientas de análisis de puertos y servicios abiertos para determinar aquellos que no son necesarios -- 4. 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 -- 5. Resumen -- Ejercicios de repaso y autoevaluación -- Capítulo 8 Robustecimiento de sistemas -- 1. Introducción -- 2. Modificación de los usuarios y contraseñas por defecto de los distintos sistemas de información -- 3. Configuración de las directivas de gestión de contraseñas y privilegios en el directorio de usuarios -- 4. Eliminación y cierre de las herramientas, utilidades, servicios y puertos prescindibles -- 5. Configuración de los sistemas de información para que utilicen protocolos seguros donde sea posible -- 6. Actualización de parches de seguridad de los sistemas informáticos -- 7. Protección de los sistemas de información frente a código malicioso -- 8. Gestión segura de comunicaciones, carpetas

compartidas, impresoras y otros recursos compartidos del sistema -- 9. Monitorización de la seguridad y el uso adecuado de los sistemas de información -- 10. Resumen -- Ejercicios de repaso y autoevaluación. Capítulo 9 Implantación y configuración de cortafuegos -- 1. Introducción -- 2. Relación de los distintos tipos de cortafuegos por ubicación y funcionalidad -- 3. Criterios de seguridad para la segregación de redes en el cortafuegos mediante Zonas Desmilitarizadas / DMZ -- 4. Utilización de redes privadas virtuales / VPN para establecer canales seguros de comunicaciones -- 5. Definición de reglas de corte en los cortafuegos -- 6. Relación de los registros de auditoría del cortafuegos, necesarios para monitorizar y supervisar su correcto funcionamiento y los eventos de seguridad -- 7. Establecimiento de la monitorización y pruebas del cortafuegos -- 8. Resumen -- Ejercicios de repaso y autoevaluación -- Bibliografía.

Sommario/riassunto

Libro especializado que se ajusta al desarrollo de la cualificacion profesional y adquisicion del certificado de profesionalidad "IFCT0109. SEGURIDAD INFORMATICA". Manual imprescindible para la formacion y la capacitacion, que se basa en los principios de la cualificacion y dinamizacion del conocimiento, como premisas para la mejora de la empleabilidad y eficacia para el desempeno del trabajo.