Enciclopedia de la Seguridad Informática

2ª Edición actualizada

En este libro se pretende abordar desde un punto de vista global la problemática de la Seguridad Informática y la Protección de Datos, contemplando tanto los aspectos técnicos, como los factores humanos y organizativos, así como el cumplimiento del entorno legal. Para ello, el contenido de esta obra se ha estructurado en siete grandes bloques:

- La primera parte presenta los principios básicos de la Seguridad de la Información en las organizaciones y en las redes de computadoras, describiendo los elementos de las Políticas, Planes y procedimientos de Seguridad, el análisis y gestión de riesgos, así como la certificación según estándares como los de la familia ISO/IEC 27000.
- En la segunda parte se estudian las vulnerabilidades de los sistemas y redes informáticas, las amenazas y los tipos de ataques más frecuentes. También se analizan los Planes de Respuesta a Incidentes y de Continuidad del Negocio.
- Una tercera parte se dedica a los aspectos relacionados con la identificación y autenticación de los usuarios en los sistemas informáticos, incluyendo el estudio de los más novedosos sistemas biométricos.
- En la cuarta parte se describen los principales sistemas y técnicas criptográficos, así como algunas de sus aplicaciones para mejorar la seguridad de los sistemas informáticos y de los servicios de Internet, analizando las características del DNI electrónico o de la factura electrónica.
- La quinta parte se centra en los aspectos técnicos para implantar las medidas de seguridad en las redes de computadoras, analizando el papel de dispositivos como los cortafuegos (firewalls), sistemas de detección de intrusiones (IDS) o servidores proxy. Así mismo, se aborda el estudio de la seguridad en las redes privadas virtuales y en las redes inalámbricas.
- En la sexta parte del libro se presentan los aspectos relacionados con la seguridad en el uso de los principales servicios de Internet, el desarrollo de los medios de pago on-line, así como la forma de afrontar problemas como el spam, el phishing o la protección de la privacidad de los ciudadanos en Internet.
- Por último, en la séptima parte se analizan diversos aspectos relacionados con el entorno legal y normativo que afectan a la Seguridad Informática: la lucha contra los Delitos Informáticos, la protección de los Datos Personales o el Control de Contenidos, entre otros.

Álvaro Gómez Vieites es Doctor en Economía (con el Premio Extraordinario de Doctorado), Licenciado en Administración y Dirección de Empresas e Ingeniero en Informática de Gestión por la UNED, Ingeniero de Telecomunicación por la Universidad de Vigo. Su formación se ha completado con los programas de posgrado Executive MBA y Diploma in Business Administration de la Escuela de Negocios Caixanova. Catedrático, consultor e investigador en las áreas de sistemas de información, seguridad informática, e-administración y comercio electrónico.

ÍNDICE