

Seguridad informática BÁSICO



ECO E
EDICIONES



Álvaro Gómez Vieites

Seguridad informática **BÁSICO**



Álvaro Gómez Vieites

Seguridad Informática. Básico
© Álvaro Gómez Vieites
© De la edición StarBook 2010

MARCAS COMERCIALES. Las designaciones utilizadas por las empresas para distinguir sus productos suelen ser marcas registradas. StarBook ha intentado a lo largo de este libro distinguir las marcas comerciales de los términos descriptivos, siguiendo el estilo que utiliza el fabricante, sin intención de infringir la marca y sólo en beneficio del propietario de la misma. Los datos de los ejemplos y pantallas son ficticios a no ser que se especifique lo contrario.

StarBook es marca comercial registrada.

Se ha puesto el máximo empeño en ofrecer al lector una información completa y precisa. Sin embargo, StarBook Editorial no asume ninguna responsabilidad derivada de su uso ni tampoco de cualquier violación de patentes ni otros derechos de terceras partes que pudieran ocurrir. Esta publicación tiene por objeto proporcionar unos conocimientos precisos y acreditados sobre el tema tratado. Su venta no supone para el editor ninguna forma de asistencia legal, administrativa o de ningún otro tipo. En caso de precisarse asesoría legal u otra forma de ayuda experta, deben buscarse los servicios de un profesional competente.

Reservados todos los derechos de publicación en cualquier idioma.

Según lo dispuesto en el Código Penal vigente ninguna parte de este libro puede ser reproducida, grabada en sistema de almacenamiento o transmitida en forma alguna ni por cualquier procedimiento, ya sea electrónico, mecánico, reprográfico, magnético o cualquier otro sin autorización previa y por escrito de StarBook; su contenido está protegido por la Ley vigente que establece penas de prisión y/o multas a quienes, intencionadamente, reprodujeren o plagiaran, en todo o en parte, una obra literaria, artística o científica.

Editado por:

StarBook Editorial

Calle Jarama, 3A, Polígono Industrial Igarsa

28860 PARACUELLOS DE JARAMA, Madrid

Teléfono: 91 658 16 98

Fax: 91 658 16 98

Correo electrónico: edicion@starbook.es

Internet: www.starbook.es

ISBN: 978-84-92650-36-1

Depósito Legal: M-XXXXX-2010

Autoedición: Autores

Diseño Portada: Antonio García Tomé

Impresión: Closas-Orcoyen, S.L.

Impreso en España en marzo de 2011



*A mi familia y,
muy especialmente,
a mi mujer Elena y a
nuestra hija Irene.*

El Autor



Álvaro Gómez Vieites es Doctor en Economía y Administraciones de Empresas por la UNED, Ingeniero de Telecomunicación por la Universidad de Vigo (con el Premio Extraordinario Fin de Carrera) e Ingeniero en Informática de Gestión por la UNED. Su formación se ha completado con varios cursos en programas de postgrado, entre ellos el Executive MBA y el Diploma in Business Administration de la Escuela de Negocios Caixanova. Ha sido Director de Sistemas de Información y Control de Gestión en la Escuela de Negocios Caixanova. En la actualidad, es profesor colaborador de esta entidad, actividad que compagina con el asesoramiento a la Xunta de Galicia en proyectos de innovación tecnológica (gestor TIC del Plan Gallego de I+D+i), cuenta además con una amplia experiencia en las áreas de sistemas de información, seguridad informática, e-administración y comercio electrónico.

Contenido

Capítulo 1.

¿Qué es la Seguridad Informática?	3
1.1 Introducción	5
1.2 Servicios de seguridad de la información	8
1.3 Consecuencias de la falta de seguridad	14

Capítulo 2.

Gestión de la seguridad de la información	21
--	-----------

Capítulo 3.

Análisis y gestión de riesgos	31
1. Recursos del sistema	33
2. Amenazas	34
3. Vulnerabilidades	35
4. Incidentes de seguridad	35
5. Impactos	35
6. Riesgos	36
7. Defensas, salvaguardas o medidas de seguridad	37

Capítulo 4.

Políticas, planes y procedimientos de seguridad	43
4.1 Introducción	45
4.2 Conceptos básicos	46
4.3	Elementos de un plan de seguridad
	49
4.3.1 Seguridad física de las instalaciones	50
4.3.2 Copias de Seguridad (back-ups)	51

4.3.3	Identificación de los usuarios del sistema	51
4.3.4	Control de los accesos a los recursos informáticos	52
4.3.5	Auditoría de la Seguridad	53
4.3.6	Actualización de las Aplicaciones Informáticas	54
4.3.7	Protección frente a virus informáticos	54
4.3.8	Cifrado de los datos	55
4.3.9	Planes de Contingencia	55
4.3.10	Formación de los usuarios sobre seguridad	57
Capítulo 5.		
	Seguridad en la conexión de la empresa a internet	59
Capítulo 6.		
	Tipos de amenazas a la seguridad en las redes de ordenadores	69
Capítulo 7.		
	Criptografía y firma electrónica	81
7.1	Funcionamiento de un sistema criptográfico	83
7.2	Sistemas criptográficos simétricos	87
7.3	Sistemas criptográficos asimétricos	88
7.4	El concepto de firma digital o firma electrónica	93
7.5	Certificados digitales y autoridades de certificación	98
7.6	limitaciones de los sistemas criptográficos	104
Capítulo 8.		
	El problema del fraude en internet y los casos de phishing	107

Capítulo 9.	
La protección de los datos de carácter personal	115
9.1 ¿Cómo garantizar la protección de datos personales?	117
9.2 El marco normativo en España	120
9.2.1 Responsable del fichero	122
9.2.2 Principios de la protección de los datos	123
9.2.3 La problemática de la adaptación a la LOPD	129
Índice Alfabético	135
Bibliografía	141

Introducción

La mayoría de las actividades que se realizan de forma cotidiana en los países desarrollados dependen en mayor o menor medida de sistemas y de redes informáticas. El espectacular crecimiento de Internet y de los servicios telemáticos (comercio electrónico, servicios multimedia de banda ancha, administración electrónica, herramientas de comunicación como el correo electrónico o la videoconferencia...) han contribuido a popularizar aún más, si cabe, el uso de la informática y de las redes de ordenadores, hasta el punto de que en la actualidad no se circunscriben al ámbito laboral y profesional, sino que incluso se han convertido en un elemento cotidiano en muchos hogares, con un creciente impacto en las propias actividades de comunicación y de ocio de los ciudadanos.

Por otra parte, servicios críticos para una sociedad moderna, como podrían ser los servicios financieros, el control de la producción y suministro eléctrico (centrales eléctricas, redes de distribución y transformación), los medios de transporte (control de tráfico aéreo, control de vías terrestres y marítimas), la sanidad (historial clínico informatizado, telemedicina), las redes de abastecimiento (agua, gas y saneamiento) o la propia Administración Pública están soportados en su práctica totalidad por sistemas y redes informáticas, hasta el punto de que en muchos de ellos se han eliminado o reducido de forma drástica los papeles y los procesos manuales.

En las propias empresas, la creciente complejidad de las relaciones con el entorno y el elevado número de transacciones realizadas como parte de su actividad han propiciado el soporte automatizado e informatizado de muchos de sus procesos, situación que se ha acelerado con la implantación de los ERP, o

paquetes software de gestión integral.

Por todo ello, en la actualidad las actividades cotidianas de las empresas y de las distintas Administraciones Públicas e, incluso, las de muchas otras instituciones y organismos, así como las de los propios ciudadanos, requieren del correcto funcionamiento de los sistemas y redes informáticas que las soportan y, en especial, de su seguridad.

De ahí la gran importancia que se debería conceder a todos los aspectos relacionados con la seguridad informática en una organización. La proliferación de los virus y códigos malignos y su rápida distribución a través de redes como Internet, así como los miles de ataques e incidentes de seguridad que se producen todos los años han contribuido a despertar un mayor interés por esta cuestión.