

I. CARACTERÍSTICAS DE LA OFERTA:

A. GUÍA RÁPIDA CIBERSEGURIDAD PARA DESPACHOS Y PROFESIONALES

Título:	Guía Rápida Ciberseguridad para despachos y profesionales.
Modo de edición	Novedad Editorial
Fecha de publicación:	3 de diciembre de 2018
Colección:	Guías Rápidas
ISBN:	978-84-17544-34-8
ISSN:	En tramitación
Páginas:	350 aprox.
Formato:	15 X 24 Cm
Encuadernación:	Rústica, tapas de cartón
Actualización:	No contemplada

II. IMAGEN DEL PRODUCTO

GUÍA RÁPIDA FRANCIS
LEFEBVRE



III. PRECIO

Precio		
Precio Base	IVA	Total
18 €	0,72 €	18,72 €

A. GUÍA RÁPIDA CIBERSEGURIDAD PARA DESPACHOS Y PROFESIONALES

ARGUMENTOS DE LA OBRA

Hoy en día proliferan medios informáticos ilegales que ponen en peligro la seguridad de nuestros datos y la confidencialidad de nuestras actuaciones, especialmente en sectores como el de los abogados y asesores en el que manejamos información muy sensible.

Por ello se edita esta guía rápida en la que se pretende mostrar **de forma práctica, clara y sencilla**, cuáles son los principales peligros a los que se enfrenta un despacho, revisando las medidas de seguridad para evitar poner en peligro nuestra información.

En ella se explican **cuestiones básicas que afectan a cualquier despacho** (el acceso a servidores, la seguridad en una red de ordenadores, la de nuestros propios equipos, la del correo electrónico, dispositivos móviles y smartphones, etc.), pero también prácticas informáticas menos conocidas pero **cada vez más frecuentes**: la seguridad en la nube, la imagen y reputación en internet, redes sociales, “Phising”, “Malware”, la firma y certificado electrónicos, etc.

Como no puede ser de otra forma, en ella se exponen también los **estándares y normativas** más relevantes acerca de la ciberseguridad. Las **novedades** de la legislación vigente para proteger los datos, para la gestión de riesgos, para la gestión de la ciberseguridad en la administración pública, etc.

SUMARIO

1. Introducción al funcionamiento de internet y a la ciberseguridad
2. Seguridad de redes: seguridad perimetral
3. Malware: prevención y detección
4. Phising e ingeniería social
5. Introducción a la continuidad de negocio
6. Seguridad en sistemas, programas y aplicaciones
7. Seguridad y buenas prácticas con el correo electrónico
8. Seguridad en los dispositivos móviles y smartphones
9. Posicionamiento, imagen y reputación en internet
10. Seguridad en la nube: cloud computing
11. Introducción a estándares y normativas acerca de la ciberseguridad
12. Servicios de confianza y firma electrónica
13. Criptomonedas y blockchain
14. Nuevas tendencias