



CIBERSEGURIDAD PARA DIRECTIVOS

Victor Eduardo Deutsch

ISBN: 9788411311595

Editorial: LID Editorial

Colección: Acción Empresarial

Idioma: Español

Páginas: 210

Formato: digital

PVP: 21,95 euros

e-book: 9,99 euros

#CiberseguridadDirectivos

La obra

Cada vez son más las empresas víctimas de ciberataques que generan grandes daños para el negocio y ponen en tela de juicio la confianza en ellas y su reputación. Ser vulnerable o tener una brecha de seguridad es algo que ninguna empresa de cualquier tamaño se puede permitir, en cuestión de minutos su actividad se puede ver bloqueada afectando a los diferentes stakeholders. Por ello, la ciberseguridad o la seguridad de la información es una de las mayores preocupaciones de los directivos de empresa.

La adaptación a las necesidades del mercado pasa por la transformación digital de las empresas transformando los activos físicos en activos digitales e intangibles que hay que proteger. Para ello, con el fin de ayudar a aquellos directivos que se enfrentan a este reto, nace *Ciberseguridad para directivos*, un libro que ofrece las herramientas necesarias para conocer, valorar y tomar decisiones acerca de los riesgos de ciberseguridad a los que se enfrentan las compañías a día de hoy sin imponer la necesidad de contar con formación en IT.

A lo largo de la obra, Victor Eduardo Deutsch sugiere un modelo que permite afrontar el problema de forma estructurada abordando los tres pilares fundamentales de la ciberseguridad:

Riesgos: Se realiza un análisis de las amenazas más directas al patrimonio y a la cuenta de resultados de la empresa, detallando una serie de situaciones de riesgo previsible cuando la compañía se integra en la economía digital.

Control: Se estudian los controles de seguridad informática en las empresas teniendo en cuenta que el ámbito de actuación se amplía al ámbito de las aplicaciones en la nube y otros dispositivos conectados a Internet.

Eficiencia: Se incluyen recomendaciones para diseñar procesos de negocios seguros y una organización de ciberseguridad adecuada a las estructuras y prácticas del paradigma de la transformación digital proporcionando herramientas para mejorar la eficiencia de los procesos de ciberseguridad.

El carácter más práctico del libro deriva de los casos reales y vivencias con los que se ilustran las diferentes alternativas.

Ciberseguridad para directivos es un libro de lectura obligada para aquellos profesionales que no se dedican a la ciberseguridad pero que son responsables de organizaciones y de su continuidad, siendo la seguridad de la empresa, de su información y de sus sistemas elementos clave para ello.

El autor



Victor Eduardo Deutsch es analista de computación de la Universidad de Buenos Aires. Con más de 25 años de experiencia en tecnologías de la información (IT) y ciberseguridad, ha ocupado cargos gerenciales en diferentes unidades de negocio del Grupo Telefónica en España y a nivel global. Previamente fue senior manager de la consultora KPMG en Latinoamérica. Es investigador en inteligencia artificial, profesor universitario y formador de programas in company. Ha participado en numerosos congresos y conferencias internacionales en materia de IT y es coautor del libro *Líderes del tercer milenio. Manual para el desarrollo empresario* y colaborador habitual del blog de tendencias en tecnología *Think Big Empresas*.

Índice

Agradecimientos Introducción

PRIMERA PARTE: RIESGOS

1. El marketing del miedo

1. «Algunos ya no estarán con nosotros»
2. El caso Wakefield y los bulos que matan

2. Las amenazas al patrimonio: los activos

1. Los activos en la era de Internet
2. Proteger los activos físicos
3. Proteger la información confidencial

3. Las amenazas al patrimonio: las estafas

1. Delitos informáticos
2. El fraude corporativo

4. Las amenazas a la cuenta de resultados

1. Riesgos que alteran la capacidad operativa de la empresa
2. Gastos extraordinarios y lucro cesante
3. Mayores costes

5. Gestión de crisis

1. Consecuencias de una mala gestión
2. Perjuicios económicos de una mala gestión de crisis
3. Daños a la reputación

SEGUNDA PARTE: CONTROL

6. Una breve historia de la seguridad de la información

1. Las primeras redes de comunicaciones
2. La tecnología de la información se extiende
3. Del PC a Internet
4. La noción de perímetro
5. La era de la cloud computing
6. Presente y futuro

7. La seguridad en las redes de comunicación

1. El cifrado de información en las redes públicas
2. Complejidad frente a velocidad de cálculo
3. El caso de las comunicaciones móviles

8. Defendiendo las murallas de la ciudad

1. El perímetro se desvanece: la ciudad crece extramuros
2. La nueva ciberseguridad en la empresa

3. Descomponiendo los puntos de control
4. Nuestros productos se transforman en información
5. El acceso único a la red
6. La concienciación es la clave
7. Pruebas, gestión de crisis e inteligencia
8. Un modelo de gestión de la ciberseguridad

9. La paradoja de las pymes

1. Evolución de la ciberseguridad en las pymes
2. La nueva batalla del Atlántico
3. La ciberseguridad como factor clave para la supervivencia de las pymes
4. La seguridad en las pymes de España
5. Una demanda insatisfecha.
6. Los mitos de seguridad en las pymes

10. Ciberseguridad en la industria 4.0

1. Los otros sistemas de información
2. Ciberseguridad IoT
3. Ciberseguridad en los robots industriales
4. Seguridad en el borde de la red: la cuestión moral

TERCERA PARTE: EFICIENCIA

11. Las funciones de ciberseguridad

1. Las operaciones básicas de ciberseguridad: SOC
2. Las operaciones avanzadas: el SOC ampliado
3. La cuestión del código
4. Construyendo una cultura de ciberseguridad
5. La gestión de vulnerabilidades como proceso continuo
6. Transferir el riesgo restante: los ciberseguro

12. La organización de ciberseguridad

1. Un nuevo modelo de organización de la tecnología de la información en la empresa
2. El nuevo rol del Chief Information Security Officer
3. La convergencia con el mundo físico
4. El problema de la identidad en la era digital
5. La protección de la marca y la reputación online
6. Un nuevo modelo de organización en ciberseguridad

Conclusiones

Anexos

Para más información:
laura.diez@lidbusinessmedia.com

