

RENATO JIJENA LEIVA

CIBERSEGURIDAD Y DERECHO

DATOS PERSONALES Y DELITOS

Leyes N° 21.663, 19.628 y 21.459

La Ley N° 17.336 sobre Propiedad Intelectual prohíbe el uso no exceptuado de obras protegidas sin la autorización expresa de los titulares de los derechos de autor. No se permite la reproducción total o parcial de esta obra, ni su incorporación a un sistema informático, ni su transmisión en cualquier forma o por cualquier medio (electrónico, mecánico, fotocopia, grabación u otros) sin autorización previa y por escrito de los titulares del copyright. La infracción de dichos derechos puede constituir un delito contra la propiedad intelectual.. Usos infractores pueden constituir delito.



Más información sobre el libro y su autor escanee el código QR o en nuestra página web www.editorialhammurabi.com o nuestra Librería ubicada en Huerfanos 1055, local 12 (332) Santiago, Chile (Galería Agustín Edwards)

CURSOS Y MANUALES HAMMURABI



EditorialHammurabi



HammurabiEditor



HammurabiEditor



EditorialHammurabi

CIBERSEGURIDAD Y DERECHO DATOS PERSONALES Y DELITOS

© Es propiedad de Renato Jijena Leiva
Abogado, Licenciado en Ciencias Jurídicas y Sociales PUCV
Magíster en Derecho Público PUCV
Magíster en Gobierno Electrónico UTEM
Máster en Protección de Datos Personales UNIR
Diplomado en Derecho Informático Universidad de Zaragoza

ISBN: 978-956-6396-95-6
Tiraje 500 ejemplares
1ª Edición, octubre 2025

Editorial Hammurabi®

Editor: Manuel Álvarez Cabello
Teléfono: +56955258948
Correo electrónico: manuel.alvarez@editorialhammurabi.com
Sitio web: www.editorialhammurabi.com
Sala de ventas: Huerfanos 1055, local 12 (332) Santiago, Chile
(Galería Agustín Edwards)
Portada y diagramación: Editorial Hammurabi
Impresión: Impreso en Grafica LOM

IMPRESO EN CHILE / PRINTED IN CHILE

*A mis amigos ingenieros, ciberdetectives y abogados empresarios
TICs de toda la vida, en especial informáticos, de cuyas enseñanzas
soy heredero y depositario desde aquellos días del EDI aduanero, de
Transbank, de la certificadora ONCE de la CNC, del SII y de la
Estrategia Digital del Gobierno. Su respeto intelectual y profesional,
además de recíproco, ha sido un estímulo y una herramienta de ruta
esencial para navegar en el mar de los avatares de las TIC...*

INDICE GENERAL

TÉRMINOS DE USO FRECUENTE	13
INTRODUCCIÓN	15

CAPÍTULO PRIMERO

CIBERSEGURIDAD, ACTIVOS DE INFORMACIÓN, ESTÁNDARES ISO Y OTROS TÓPICOS

A. Sobre la ciberseguridad y la seguridad de la información. La ciberseguridad holística.	27
B. El rol esencial de Internet, tanto para la comisión de ciberataques como para el desarrollo de la ciberseguridad.	50
C. Los Activos de Información (AI).	54
D. Los estándares ISO 27001 y ss. Un referente ineludible.	57
E. Del análisis y la gestión de riesgos en general.	63
F. Vulnerabilidades, ataques informáticos o ciberataques e incidentes de ciberseguridad.	69
G. Inteligencia artificial versus ciberseguridad.	76
H. Ciberseguridad y blockchain.	87
I. Ciberseguridad en la nube del cloud computing.	93
J. Los Marcos de Ciberseguridad, de Privacidad y las directrices de autenticación de identidades digitales del NIST	105
K. ENISA, la European Union Agency for Cybersecurity o Agencia de la Unión Europea para la Ciberseguridad	111
L. La importancia de las auditorías de sistemas.	113
M. La importancia de la gestión y la gobernanza de datos para la ciberseguridad.	117

CAPÍTULO SEGUNDO

CIBERSEGURIDAD Y DERECHO. VISIÓN DE CONTEXTO

A. Generalidades. La Ley N° 21.663 (referencia)	121
B. El marco jurídico para la ciberseguridad en la Administración del Estado. Referencia	126

C. Marco regulatorio (i) para las Instituciones Financieras y (ii) para las empresas fintec. Las normas de la CMF y las Leyes N° 20.009, N° 21.521 y N° 21.663 (referencias)	149
D. Directrices de la CMF sobre gestión de riesgo operacional y ciberseguridad en materia de seguros. NCG N° 454	158
E. Ley N° 19.799. Criptografía, firma electrónica avanzada y autenticación de documentos electrónicos	159
E.1 Falta de seguridad y no adecuación al Derecho Público en el uso de certificados de PKI en el SRC.	178
E.2 Falta de seguridad y no adecuación al Derecho Público del sistema www.firmagob.cl	178
E.3 Falta de seguridad y no adecuación al Derecho Público de la FEA en línea - Decreto N° 24 del 2019.	182
E.4 Uso válido de certificados digitales para la emisión y firma de DTE (facturas) en el Portal MiPyme del SII.	186
F. Bloque de posibles responsabilidades legales asociadas a la ciberseguridad. Sobre la responsabilidad civil en general y particular	187
G. Derecho Comparado. La Ley de Gestión de la Seguridad de la Información y Ciberseguridad (FISMA) de EEUU y los Reglamentos de Ciberseguridad de la UE	197

CAPÍTULO TERCERO

EL MARCO JURÍDICO GENERAL DE LA LEY N° 21.663

A. Generalidades y Políticas Nacionales	201
B. El caso del Banco Santander. Acceso indebido a credenciales y datos personales	208
C. El antecedente previo de la Ley N° 21.663: el NIS 2 de la Unión Europea	210
D. Contexto, objeto y estructura del articulado de la Ley N° 21.663 de abril del 2024	217
E. Los Principios fundantes de la Ley N° 21.663	218
F. Roles esenciales de la norma. Operadores de Importancia Vital y Prestadores de Servicios Esenciales (artículos 4°, 5° y 6°)	220
G. Obligaciones de ciberseguridad. Deberes generales y específicos de los OIV (artículos 7° y 8°)	223
H. Clasificación administrativa de los incidentes de ciberseguridad	225
I. Marco jurídico (referencia). Ley, Reglamento e Instrucción General sobre reportes de brechas o de incidentes de ciberseguridad (artículos 9° y 27°)	226
J. Los incidentes de efecto significativo, el tratamiento de DP y las direcciones IP	229
K. De la reserva de información en el sector público en materia de ciberseguridad	231
L. Incumplimientos, infracciones y sanciones	232

CAPÍTULO CUARTO

CIBERSEGURIDAD Y PROTECCIÓN DE DATOS PERSONALES. EL MARCO JURÍDICO ESPECIAL DE LAS LEYES N° 19.628 Y N° 21.663

A. Generalidades	235
B. Sobre el tratamiento de DP y las obligaciones de los responsables y encargados. La importancia del deber de secreto, confidencialidad o reserva en materia de SGSI y tratamiento de DP	240
C. Derecho de supresión de DP ejercido mediante el concatenamiento de información en los bloques del blockchain	265
D. Análisis y gestión de riesgos en materia de PDP en particular. Las específicas evaluaciones de impacto o PIAS.	266
E. Normas ISO 27701, especialmente referida a “privacidad” y a “protección de DP”	283
F. El RGPD del 2016 y su influencia directa en la Ley N° 19.628	285
G. Acceso ilícito a las credenciales de autenticación en el iter criminis del delito de phishing (referencia)	287
H. Especiales cuestionamientos jurídicos a las definiciones contractuales y bancarias acerca de la responsabilidad por el uso y la confidencialidad de una password o clave de acceso	298
I. Tratamiento de DP sensibles y biométricos con fines de autenticación de ID. Ley N° 21.734 y facultades de la PDI	301
J. Normas jurídicas expresas y particulares aplicables a los RDP en calidad de prestadores de servicios esenciales y operadores de importancia vital. Ley N° 21.663	304
K. Derecho Comparado: ciberseguridad para los sistemas de IA aplicados al tratamiento de DP en Colombia	307
L. Derecho Comparado: estándares de ciberseguridad y privacidad sugeridos por el MINTIC (Colombia)	309
M. Derecho Comparado: estándares o medidas de ciberseguridad de los ficheros automatizados que contengan datos personales, contenidos en los Reglamento o Real Decreto 994/1999 y el Real Decreto 1720/2007 (España)	310
N. Derecho Comparado: el Habeas Data como mecanismo procesal para auditar e instar por el cumplimiento de los deberes de seguridad en el tratamiento de DP (Argentina)	312

CAPÍTULO QUINTO

RESPONSABILIDAD PENAL DERIVADA DE LA COMISIÓN DE DELITOS INFORMÁTICOS. *HACKING Y PHISHING*

A. Sanciones jurídico-penales a los ciberataques	315
B. De los delitos informáticos en general	320

C. Los delitos informáticos, el Convenio de Budapest y la cibercriminalidad en la Ley N°
21.459. Referencia 328

D. El específico delito de hacking. El delito blanco no sancionable penalmente 339

E. El Ransomware 347

F. Robo de Identidad digital y phishing, desde la perspectiva del Derecho Penal 349

BIBLIOGRAFÍA 353