

## ÍNDICE

---

<i>Abstract</i> .....	17
<i>Subtítulos</i> .....	17
<i>Prólogo</i> .....	19
<i>Introducción</i> .....	23

### CAPÍTULO I

## LA SEGURIDAD INFORMÁTICA Y OTROS CONCEPTOS RELACIONADOS

1. Introducción .....	27
2. Evolución de la seguridad informática: desde los albores de la informática, las primeras vulnerabilidades, hasta los “zero day” .....	29
2.1. La evolución del concepto de seguridad .....	29
2.2. La seguridad informática en la informática moderna .....	31
2.3. Los albores del hacking y la ruptura del equilibrio en seguridad informática .....	33
2.4. Hacia la comprensión de las violaciones de seguridad informática .....	36
2.5. Descifrando el universo de los “exploits”, los “zero day” y las vulnerabilidades .....	37
2.6. El panorama vigente en seguridad informática y la explosión en ciberincidentes .....	42

2.7. Reflexiones finales . . . . .	43
3. La información: extensión y aristas de su significado . .	44
4. Conceptos. . . . .	48
4.1. Seguridad de la información / infosecurity / infosec / information security / infoseguridad. . . . .	51
4.2. Seguridad informática / information technology se- curity/ IT security / Ciberseguridad / Cybersecurity / Cybersec / Computer security. . . . .	55
4.2.1. Uso de “Ciberseguridad” como campo dife- renciado . . . . .	66
4.3. Ciberdefensa . . . . .	66
5. El deber de seguridad. . . . .	79
6. Atribución de la responsabilidad en materia de seguri- dad. . . . .	83
7. La importancia de la seguridad informática en términos jurídicos . . . . .	89
8. Seguridad informática y seguridad jurídica . . . . .	91
9. Conclusiones . . . . .	95

## CAPÍTULO II

### ARISTAS TÉCNICAS Y LEGALES DE LA SEGURIDAD INFORMÁTICA

1. Introducción. . . . .	99
2. La seguridad informática desde el hardware . . . . .	100
3. La seguridad física y lógica. . . . .	103
3.1. Medidas de seguridad física y lógica. . . . .	104
4. Seguridad activa y pasiva . . . . .	105
4.1. Medidas de seguridad activa y pasiva. . . . .	106
5. Seguridad defensiva y ofensiva . . . . .	107
6. Normas, Estándares y Prácticas . . . . .	108

6.1. Mejores Prácticas y Buenas Prácticas . . . . .	108
6.2. Normas y Estándares . . . . .	109
6.3. Organizaciones estandarizadoras . . . . .	110
6.3.1. IRAM . . . . .	110
6.3.2. ISO . . . . .	110
6.3.3. IEC . . . . .	111
6.3.4. ANSI . . . . .	111
6.3.5. NIST . . . . .	112
6.3.6. ANSI / NIST . . . . .	113
6.3.7. CEN . . . . .	114
6.3.8. DIN . . . . .	114
6.3.9. AENOR / UNE . . . . .	114
6.3.10. AMN . . . . .	115
6.3.11. COPANT . . . . .	115
6.3.12. Otros . . . . .	115
6.3.13. Comités Técnicos de Normalización . . . . .	116
6.4. Proceso de estandarización . . . . .	117
6.5. Certificados ISO . . . . .	118
6.6. Requisitos para cotizar en Bolsa, exigencias en tecnología. Ley Sarbanes-Oxley / SOX / SOx / SarbOx / SOA y sus equivalentes. . . . .	120
6.7. La guerra de las estandarizaciones . . . . .	121
6.8. Las normas ISO/IEC en tecnología de la información y seguridad informática . . . . .	127
7. Metodologías, Técnicas, Procedimientos, Procesos y Reportes . . . . .	128
7.1. Metodologías y marcos de trabajo en tecnología de la información . . . . .	129
7.1.1. COBIT . . . . .	129
7.1.2. ITIL . . . . .	130
7.1.3. IT4IT . . . . .	130
7.1.4. TOGAF . . . . .	130
7.2. Marcos de trabajo en seguridad informática. . . . .	130

7.2.1.	NIST CSF - EE.UU. - Marco de Ciberseguridad del NIST (NIST Cybersecurity Framework) . . . . .	131
7.2.2.	UE - Marco de Ciberseguridad de la UE (NIS - Network and Information Security) - NIS 2 . . . . .	132
7.3.	Reportes SOC 1 / SOC 2 / SOC 3 . . . . .	133
7.3.1.	Complementariedad en el uso de normas y metodologías . . . . .	133
8.	Seguridad informática y respuesta a incidentes . . . . .	134
8.1.	CERT . . . . .	135
8.1.1.	CERT-EU . . . . .	137
8.1.2.	CERT de nuestra región latinoamericana . . . . .	139
8.1.3.	ArCERT - Antecedente / Derogado . . . . .	140
8.1.3.a.	Informe del ArCERT . . . . .	142
8.1.4.	CERT.ar . . . . .	143
8.1.4.a.	El Informe 2021 del CERT.ar . . . . .	146
8.1.4.b.	El Informe 2022 del CERT.ar . . . . .	150
8.2.	CSIRT . . . . .	159
8.2.1.	CSIRT-MINSEG . . . . .	160
8.2.2.	BA-CSIRT . . . . .	164
8.2.3.	CSIRT-PBA . . . . .	165
8.2.4.	CERTUNLP . . . . .	167
8.3.	Otras conformaciones . . . . .	170
8.3.1.	CGIP . . . . .	170
8.4.	Tipos de CERT/CSIRT . . . . .	172
8.5.	SOC . . . . .	172
8.6.	Asociaciones y Centros . . . . .	173
8.6.1.	EGC Group: European Government CERTs . . . . .	173
8.6.2.	FIRST: Forum of Incident Response and Security Teams . . . . .	174
8.6.3.	TF-CSIRT/TI: Task Force on Computer Security Incident Response Teams / Trusted Introducer . . . . .	174

8.6.4. NCIRC: Nato Computer Incident Response Capability Technical Centre . . . . .	175
8.7. Agencias . . . . .	175
8.7.1. ENISA . . . . .	175
8.7.2. CISA . . . . .	176
9. Seguridad informática vs. la Ciberseguridad . . . . .	176
10. La Ciberseguridad y su regulación en Argentina . . . . .	178
10.1. Comité de Ciberseguridad . . . . .	178
10.2. Primera Estrategia Nacional de Ciberseguridad . . . . .	179
10.3. La Dirección Nacional de Ciberseguridad . . . . .	185
10.4. Informe de Gestión Febrero 2020-Agosto 2022 de la Dirección Nacional de Ciberseguridad . . . . .	186
10.5. La Segunda Estrategia Nacional de Ciberseguridad . . . . .	193
10.6. Los Informes de la Dirección Nacional de Ciberseguridad . . . . .	204
10.6.1. Botnets. Una guía y un glosario para entender su funcionamiento . . . . .	205
10.6.2. Guía de recomendaciones para compras seguras por internet . . . . .	206
10.6.3. Phishing. Una guía y un glosario para conocer sus modalidades y prevenirlas . . . . .	206
10.6.4. El ransomware, el software malicioso usado para atacar a las organizaciones . . . . .	207
10.6.5. Informe 2021 del CERT.ar . . . . .	208
10.6.6. Delitos informáticos en Argentina: Modalidades detectadas durante la pandemia del covid-19 . . . . .	209
11. La política de protección de infraestructuras críticas . . . . .	210
12. Ciberseguridad y Ciberresiliencia de las Infraestructuras críticas del Mercado de Capitales . . . . .	217
13. Los lineamientos para la respuesta y recuperación ante ciberincidentes del Banco Central de la República Argentina . . . . .	223

14. Los Requisitos mínimos para la gestión y control de los riesgos de tecnología y seguridad de la información del Banco Central de la República Argentina . . . . .	224
15. La Política de Seguridad de la Información y los Requisitos de Seguridad de la Información para Organismos . . . . .	225
16. El Plan de Seguridad del Ministerio de Ciencia, Tecnología e Innovación . . . . .	235
17. Las Normas de Control Interno para Tecnología de la Información de la SIGEN . . . . .	235
18. Las Políticas de Seguridad de la Información de la Autoridad Regulatoria Nuclear . . . . .	237
19. La Política de Seguridad de la Información de la Superintendencia de Servicios de Salud . . . . .	238
20. El Registro de Puntos Focales en Ciberseguridad del Sector Público Nacional . . . . .	239
21. El Comité Asesor para el Desarrollo e Implementación de Aplicaciones Seguras. . . . .	240
22. La Guía introductoria a la Seguridad para el Desarrollo de Aplicaciones WEB . . . . .	242
23. Seguridad informática y delitos informáticos . . . . .	245
23.1. Ley de Delitos Informáticos . . . . .	245
23.2. Convenio de Budapest . . . . .	248
24. Denuncia de ciberdelitos . . . . .	249
25. El Plan Federal de Prevención de Delitos Tecnológicos y Ciberdelitos (2021-2024) . . . . .	250
26. El Programa de Fortalecimiento en Ciberseguridad y en Investigación del Ciberdelito (ForCIC). . . . .	258
27. El Centro de Investigaciones del Ciberdelito de Alta Tecnología (CICAT). . . . .	260
28. Necesidad de marco regulatorio específico en seguridad informática . . . . .	264
29. El estado de la ciberseguridad en Argentina en los últimos años. Incidentes de seguridad más salientes. . . . .	265

30. La mirada internacional sobre nuestro modelo de madurez de la capacidad de ciberseguridad .....	282
31. Conclusiones .....	284

**CAPÍTULO III**

**ROLES Y FUNCIONES  
EN LA SEGURIDAD INFORMÁTICA**

1. Introducción .....	287
1.1. Chief Executive Officer / CEO .....	288
1.2. Chief Information Security Officer / CISO .....	288
1.3. Chief Security Officer / CSO .....	290
1.4. Jefe de Seguridad Informática .....	291
1.5. Chief Information Officer / CIO .....	291
1.6. Chief Technology Officer / CTO .....	292
1.7. Auditor en Seguridad / CISA .....	292
1.8. Certificados y certificaciones .....	294
1.9. Pentester .....	295
1.10. Incident Responder .....	296
1.11. Especialista en Informática Forense .....	298
1.12. Responsable de Tratamiento .....	299
1.13. Encargado de Tratamiento .....	308
1.14. Data Compliance Officer .....	313
1.15. DPO / Data Protection Officer / Delegado de Protección de Datos .....	316
2. Conclusiones .....	332

**CAPÍTULO IV**

**LA SEGURIDAD DE DATOS Y LOS INCIDENTES  
DE SEGURIDAD EN TRATAMIENTO DE DATOS**

1. Introducción .....	335
2. La seguridad de datos .....	337

3. El tratamiento de datos como actividad riesgosa . . . . .	364
4. Responsabilidad por daños en seguridad de datos . . . . .	387
5. Marco regulatorio en seguridad de datos . . . . .	388
6. Medidas de seguridad en el tratamiento de datos personales. . . . .	408
7. Los incidentes de seguridad . . . . .	422
8. Las fugas de información / security breach . . . . .	431
9. El deber de notificación y comunicación de los incidentes de seguridad. . . . .	438
10. El valor de los principios de prevención y precautorio en la seguridad de datos . . . . .	442
11. Conclusiones . . . . .	445

**CAPÍTULO V**  
**HACKING**

1. Introducción . . . . .	451
2. Hackers y Hacking . . . . .	452
3. Breve racconto de la historia del Hacking. . . . .	455
4. Tipos de Hacking . . . . .	462
4.1. White Hat Hackers / Hackers de sombrero blanco	462
4.2. Black Hat Hackers / Hackers de sombrero negro / Crackers / Piratas informáticos . . . . .	463
4.3. Grey Hat Hackers / Hackers de sombrero gris . . . . .	464
4.4. Red Hat Hackers / Hackers de sombrero rojo . . . . .	466
4.5. Blue Hat Hackers / Hackers de sombrero azul . . . . .	466
4.6. Green Hat Hackers / Hackers de sombrero verde / Newbies / Noobs . . . . .	467
4.7. Script Kiddies . . . . .	467
4.8. Suicide Hackers / Hackers suicidas . . . . .	468
4.9. Hacktivistas . . . . .	468



5. El sesgo negativo respecto del hacking y su imaginario	468
6. El hacking ético y su falacia	475
7. Responsable & Irresponsable disclosure	478
8. Interpretaciones recientes relativas a los “Hackers de buena fe” / “Good-faith security research”	482
9. La importancia del hacking desde la perspectiva del derecho al consumidor	484
10. El hacking como un mecanismo de mejora de calidad	491
11. El hacking y la ingeniería inversa. La prohibición de la ingeniería inversa como cláusula abusiva.	493
12. Resignificación y revalorización del hacking a través de los programas de “bug bounty”	500
13. La ética hacker	502
14. El hacking, su casuística y persecución y nuestra codificación penal	504
14.1. Iniciativas internacionales de relevancia e impacto en la temática.	511
14.1.1. “Hacking is NOT a Crime”	511
14.1.2. “Protecting Security Researchers’ Rights in the Americas” de la Electronic Frontier Foundation	514
14.1.3. “Statement for the Protection of Digital Rights Defenders” de Access Now	515
15. Líneas de defensa ortodoxas, inexploradas y nuevos planteos de la actividad de hacking	517
16. Conclusiones	521

**CAPÍTULO VI**

**MANIFIESTO LEGAL EN SEGURIDAD INFORMÁTICA,  
INFOSECURITY & HACKING**

1. Introducción	523
-----------------	-----

2. TO HACK AND NOT TO JAIL: Legal guidance for staying  
in front of the bars ..... 529

– “Manifiesto legal en seguridad informática para Hackers  
y especialistas en infosecurity” ..... 530

**CONCLUSIÓN**

**EL FUTURO DISTÓPICO  
DE LA SEGURIDAD INFORMÁTICA Y EL HACKING  
Y LAS ACCIONES CONCRETAS PARA HACKEAR  
LAS CONCEPCIONES LEGALES ERRADAS  
DE NUESTRO PRESENTE**

..... 535

*Bibliografía* ..... 543

*Artículos / Noticias / Documentos Web* ..... 551