



Prólogo	15
Introducción	21

Capítulo I. LA INFORMÁTICA	
1. Civilización, evolución y tecnología	29
2. Una nueva tecnología	31
3. Desde sus orígenes hasta hoy	36
4. Componentes del sistema informático	46
A. Componentes pesados {Hardware}	46
B. Software (Componentes Manos)	48
5. El quark informático	50
6. Beneficios e importancia de la informática en el mundo actual	55

Capítulo II. REVOLUCIÓN - INFORMACIÓN DIGITAL	
1. La información como cuestión fundamental de la informática	67
2. La información digital: ¿es privada?	74
3. Las fuentes de almacenamiento de la información	86
4. Los sistemas informáticos. Su importancia como fuente de comunicación. El correo electrónico	90
5. El funcionamiento del correo electrónico	98
6. Otras formas de comunicación y transferencia de datos en forma electrónica	101

Capítulo III. EL SISTEMA SE RESFRÍA	
1. Problemas generales de la informática	107
a. Conductas que afectan la privacidad informática	109
b. Piratería informática	115
c. Servicios de comunicación	120
d. Honor	123
e. Pornografía infantil	125
f. Fraudes electrónicos y delitos contra la propiedad	126
g. Cuestiones colectivas	129
h. Organizaciones criminales	130
i. Seguridad de la información	130
2. Virus informáticos. Denominaciones, conceptos y clases	133
a. Denominaciones	133
b. Conceptos	135
c. Funcionamiento y clases de los virus informáticos de acuerdo a sus particularidades	142
d. Formas de actuar de los virus y las restantes amenazas lógico informáticas	146
e. Capacidad de la amenaza	148
f. Seguridad contra los virus y las amenazas lógico informáticas	151
3. Las consecuencias de las amenazas lógico informáticas	153
4. Creadores de virus	157
5. Enfermos por los virus	163
a. Ataques informáticos detectados	165
b. Las pérdidas por estos ataques son las siguientes	166

Capítulo IV. EL IMPACTO DE LA INFORMÁTICA	
1. El derecho mira a las nuevas tecnologías	171
2. La explosión digital en Argentina y la imprevisión legislativa	173
3. Informática y Derecho Penal	176
4. El delito informático. Problemática conceptual. Clasificación	178

Capítulo V. PROBLEMAS INFORMÁTICOS Y ANALOGÍA	
1. El principio de legalidad. Origen y características	189
2. La prohibición de analogía	192
3. Objetos de protección: las cosas	195
4. Consecuencias para la legislación	200
Capítulo VI. LEGISLACIÓN CONVENCIONAL	
1. Legislación Nacional	205
a. El delito de daño (Artículos 183 y siguientes del Código Penal)	205
b. Aplicación del delito de daño a las amenazas lógico informáticas	209
2. Otra legislación en conexión a las amenazas lógico informáticas	213
a. Art. 157 bis del Código Penal	214
b. Interrupción de las comunicaciones	216
3. Legislación internacional	218
Convenio sobre la ciberdelincuencia del Consejo de Europa	218
España	221
Alemania	227
Austria	229
Chile	229
Francia	231
Estados Unidos	239
Italia	241
Venezuela	244
México	250
Suiza	253
Bolivia	254
Costa Rica	255
Perú	256
Ecuador	257
Gran Bretaña	259
Brasil	262
Portugal	263
Japón	265
4. Jurisprudencia relativa a los delitos informáticos	274
Capítulo VII CONCLUSIONES	
1. La utilización de amenazas lógico informáticas como conducta atípica	285
Privacidad informática	286
Interrupción de las comunicaciones	287
2. Justificación del delito	291
3. Propuestas de reforma	296
a. Daño informático	296
b. Acceso indebido a sistemas informáticos o comunicaciones electrónicas	300
c. Interrupción o entorpecimiento de las comunicaciones electrónicas	303
4. Análisis y crítica a la reforma proyectada	303
a. Daño informático	303
La figura básica	305
Acciones típicas	305
Consecuencias de las acciones	307
Consumación, tentativa y subsidiariedad	308
Aspecto subjetivo	308
Comentarios y casos abarcados	308
Daño informático agravado	309
El daño informático y la imprudencia. Otras conductas no previstas	310

b. Acceso indebido a sistemas informáticos o comunicaciones	312
Las acciones típicas	315
Objetos protegidos	316
Sujeto activo y pasivo	316
Otras particularidades	316
Comentarios finales	317
c. Interrupción de las comunicaciones electrónicas	318
5. El problema de la aplicación espacial. La necesidad de contar con recursos humanos y tecnológicos capaces de hacer frente al delito informático	320
 Bibliografía	 325