

Frank Almanza

Cibercriminalidad y nuevas modalidades delictivas

- INTRODUCCIÓN A LA CIBERCRIMINALIDAD • DELITOS INFORMÁTICOS
 - TRASCENDENCIA DEL DELITO DE LAVADO DE ACTIVOS VIRTUALES
 - DIVISIONES DE INVESTIGACIÓN • PROCESO DE ANÁLISIS FORENSE
- EN DELITOS INFORMÁTICOS • PRUEBA ELECTRÓNICA Y PRUEBA DIGITAL
 - JURISPRUDENCIA • REFERENCIAS BIBLIOGRÁFICAS

LEGALÍA
JURÍDICA

CIENCIAS
PENALES

Director: *Frank Almanza A.*



SAN BERNARDO

FRANK ALMANZA ALTAMIRANO

*Magíster de Derecho Penal
Universidad de Medellín (Colombia)
Magíster de Derecho
Universidad de Jaén (España)
Profesor de la Universidad de San Martín de Porres
Profesor principal de la Academia de la Magistratura*

CIBERCRIMINALIDAD Y NUEVAS MODALIDADES DELICTIVAS

Con la colaboración de
Fiorella María Almanza Chávez y
Josef José Campos Ravichagua

LEGALÍA
JURÍDICA


SAN BERNARDO



986 864 354



ventas@legaliajuridica.com

ÍNDICE

Prólogo.....	13
--------------	----

1.

INTRODUCCIÓN A LA CIBERCRIMINALIDAD

1.1. Definición de cibercriminalidad y algunos alcances	35
1.2. Impacto y alcance de la cibercriminalidad	37
1.3. Evolución de la cibercriminalidad.....	40

2.

DELITOS INFORMÁTICOS

2.1. Definición de delitos informáticos.....	45
2.1.1. Categorías	46
2.1.2. Bienes jurídicos vulnerados.....	47
2.2. Tipos de delitos informáticos y tratamiento normativo.....	62
2.2.1. Delitos contra datos y sistemas informáticos.....	62
2.2.2. Delitos informáticos contra la indemnidad y libertad sexuales.....	68
2.2.3. Delitos informáticos contra la intimidad y el secreto de las comunicaciones	72

FRANK ALMANZA ALTAMIRANO

2.2.4. Delitos informáticos contra el patrimonio	76
2.2.5. Delitos informáticos contra la fe pública.....	84
2.2.6. Interferencia Telefónica.....	89
2.2.7. Pornografía Infantil	92
2.3. Aspectos de delitos reconocidos a nivel internacional.....	95
2.3.1. Grooming	95
2.3.2. Stalking	97
2.3.3. Phishing	100
2.3.4. Fraudes en línea.....	103
2.3.5. Bullying Cibernético	108
2.3.6. Sexting	109
2.3.7. Ciberodio.....	110
2.3.8. Vishing.....	113
2.3.9. Ciberterrorismo.....	116
2.4. La violencia de género digital contra las mujeres.....	123
2.4.1. Comercio a través del material que sexualiza a la mujer ...	123
2.4.2. Violencia de género digital en la relación de pareja	125
2.4.3. Sextorsión.....	128
2.5. Casos prácticos de delitos informáticos en Perú.....	129

3.

TRASCENDENCIA DEL DELITO DE LAVADO DE ACTIVOS VIRTUALES

3.1. Características del delito	141
3.2. La influencia del Covid-19 en el lavado de activos.....	147
3.3. Riesgo emergente de activos virtuales	150



CIBERCRIMINALIDAD Y NUEVAS MODALIDADES DELICTIVAS

3.4. Delitos de lavado de activos en el Decreto Legislativo N° 1106 ..	153
3.5. Naturaleza jurídica del Bitcoin	157
3.6. El uso de bitcoins como instrumento para el lavado de activos	161
3.7. Los actos de lavado de activos virtuales son típicos y punibles	165

4.

DIVISIONES DE INVESTIGACIÓN

4.1. División de Investigación Delitos Alta Tecnología	169
4.1.1. Funciones y aspectos generales.....	172
4.2. El Ministerio Público	183
4.2.1. Desafíos.....	186
4.2.2. La Oficina de Peritajes.....	187
4.3. Procedimientos generales.....	190
4.4. Procedimientos específicos.....	193
4.5. Anexos de denuncias	196

5.

PROCESO DE ANÁLISIS FORENSE EN DELITOS INFORMÁTICOS

5.1. Informática forense	197
5.1.1. Fases del análisis forense:	199
5.2. La evidencia	203
5.3. Peritaje Informático.....	207



FRANK ALMANZA ALTAMIRANO

5.4.	Normas internacionales aplicadas a la informática forense	210
5.5.	Modelos de análisis o interpretación forense.....	213
5.5.1.	Modelo Digital Forensic Research Workshop (DFRWS)..	214
5.5.2.	Modelo Casey (2000)	215
5.5.3.	Modelo Casey (2004)	216
5.5.4.	Modelo Forense del Departamento de Justicia de EEUU...	217
5.5.5.	Manual para el tratamiento de evidencia digital.....	218
5.6.	Proceso en el campo de acción.....	219
5.6.1.	Protección de la escena	219
5.6.2.	Identificar evidencias	222
5.6.3.	Recolección de evidencias	225
5.6.4.	Preservación de las evidencias	228
5.6.5.	Análisis de las evidencias.....	231
5.6.6.	Redacción de informes	232
5.6.7.	Aspectos ulteriores.....	235

6.

PRUEBA ELECTRÓNICA Y PRUEBA DIGITAL

6.1.	Definición de prueba electrónica y prueba digital.....	237
6.2.	Diferencias entre prueba electrónica y prueba digital	240
6.2.1.	Pruebas en el entorno digital	241
6.2.2.	Pruebas en el entorno electrónico	243
6.3.	Reglas en la prueba de evidencias digitales que sean idealmente hechos jurídicos.....	244
6.4.	Controversias	245



CIBERCRIMINALIDAD Y NUEVAS MODALIDADES DELICTIVAS

6.4.1. La validez probatoria	245
6.4.2. Prestadores de servicios de comunicaciones sobre certificar el contenido de una comunicación.....	250
6.4.3. Teoría del árbol envenenado y saneado	252

7.

JURISPRUDENCIA

7.1. Jurisprudencia nacional	255
7.2. Jurisprudencia Internacional.....	265

8.

REFERENCIAS BIBLIOGRÁFICAS

.....	267
-------	-----

