

ÍNDICE

AGRADECIMIENTOS	11
PRÓLOGO	13
CAPÍTULO I	
INTRODUCCIÓN A LAS (CIBER)ESTAFAS EN LA ERA DIGITAL: DEFINICIONES Y TENDENCIAS GENERALES.	19
I.1. La globalización y la industrialización de las estafas.	19
I.2. ¿Qué entendemos por ciberestafa?	22
I.3. La extensión y las tendencias en las ciberestafas	28
I.3.1. Los datos oficiales	28
I.3.2. Otras fuentes de datos.	34
I.4. Conclusión y estructura del resto del libro	37
Lecturas complementarias	38
Referencias bibliográficas.	39
CAPÍTULO II	
CIBERESTAFADORES: ORGANIZACIÓN, TÉCNICAS Y MOTIVACIÓN	43
II.1. Introducción	43
II.2. <i>Crime scripts</i> de ciberestafas y <i>phishing</i>	44
II.2.1. Fase I. Preparación	45
II.2.1.1. Función de mercado de los lugares de encuentro de delincuentes en línea.	46
II.2.1.2. Función social	49
II.2.1.3. Función de aprendizaje	49

II.2.2. Fase II. La actividad: contacto y engaño.	50
II.2.2.1. <i>Phishing</i>	50
II.2.2.2. Anuncios fraudulentos	52
II.2.2.3. Páginas web fraudulentas.	52
II.2.2.4. Robo de identidad y uso fraudulento de datos	53
II.2.2.5. Las técnicas de los estafadores para engañar a sus víctimas: la ingeniería social	53
II.2.3. Fase III: Cobrar, huir y cubrir el rastro	58
II.3. Estructura y perfil de los grupos y redes criminales que cometen ciberestafas	60
II.4. Perfil de ciberestafadores individuales y sus motivaciones	63
II.5. Teorías de la criminalidad y los ciberestafadores	65
II.5.1. La teoría de la elección racional.	65
II.5.2. La teoría del aprendizaje social	67
II.5.3. Técnicas de neutralización y las ciberestafas.	68
II.6. Conclusión	71
Lecturas complementarias.	72
Referencias bibliográficas.	72
CAPÍTULO III	
LAS VÍCTIMAS DE CIBERESTAFAS	79
III.1. Introducción	79
III.2. Características de las víctimas de ciberestafas.	80
III.2.1 Características sociodemográficas	80
III.2.2. Actividades cotidianas y estilos de vida de las víctimas de ciberestafas	85
III.2.3. La teoría general del delito y la victimización por ciberfraude	88
III.2.4. Rasgos disposicionales más allá del autocontrol	90
III.2.5. Organizaciones víctimas de estafas en línea	92
III.3. El impacto económico de las ciberestafas y factores correlacionados	96
III.3.1. Factores asociados con el impacto financiero	98
III.3.2. El impacto sobre las organizaciones	100
III.3.3. Más allá del impacto económico	103
III.3.4. Factores asociados con el impacto no financiero.	105
III.4. Miedo a las estafas en internet.	106
III.5. Conclusión	108
Lecturas complementarias.	109
Referencias bibliográficas.	110
CAPÍTULO IV	
CIBERESTAFAS Y EL SISTEMA PENAL.	121
IV.1. Introducción.	121

IV.2. La denuncia del fraude informático y la cifra negra	121
IV.3. La denuncia de las ciberestafas por parte de las organizaciones.	126
IV.4. El modelo de sistema penal reactivo y las estafas en Internet	129
IV.5. Retos para las respuestas policiales al ciberfraude	132
IV.5.1. Localización de sospechosos.	133
IV.5.2. Obtención de pruebas	134
IV.5.3. Los retos de la gestión de las víctimas	135
IV.5.4. Las estafas en línea y los modelos preventivos del derecho penal	136
IV.5.5. Entonces, ¿qué se puede hacer?	137
IV.5.5.1. Cooperación policial: estudio de caso 1	139
IV.5.5.2. Cooperación policial: estudio de caso 2	139
IV.6. Respuestas pluralizadas y privatizadas al ciberfraude.	141
IV.7. Conclusiones	145
Lecturas complementarias.	146
Referencias bibliográficas.	146

CAPÍTULO V

PREVENCIÓN DE LAS CIBERESTAFAS: EL FACTOR HUMANO Y LAS RESPUESTAS TECNOLÓGICAS

V.1. Introducción	151
V.2. Prevención de las ciberestafas centrada en el factor humano.	152
V.3. Comunicación de información sobre ciberseguridad y prevención de ciberestafas	154
V.3.1. Campañas de concienciación y guías dirigidas a organizaciones	154
V.3.2. Campañas de concienciación, guías y formación dirigidas a individuos	156
V.3.2.1. Campañas de concienciación y guías	157
V.3.2.2. Formación.	159
V.3.3. Dificultades para evaluar las medidas de prevención centradas en el factor humano	161
V.4. Prevención de las ciberestafas centrada en la tecnología	163
V.4.1. Medidas tecnológicas que dificultan el contacto con la víctima	163
V.4.2. Medidas tecnológicas que reducen los beneficios.	166
V.4.3. Dificultades para evaluar la eficacia de las medidas técnicas de prevención	168
V.5. Intervenciones contra las estafas en línea y el desplazamiento del delito	170
V.6. Conclusión	173
Lecturas complementarias.	174
Referencias bibliográficas.	174

CAPÍTULO VI	
CONSIDERACIONES FINALES Y EL FUTURO DE LAS CIBERESTAFAS	181
VI.1. Introducción	181
VI.2. Medios sintéticos y ciberestafas	181
VI.3. La Comisión Europea y el papel de las empresas TIC en la lucha contra las ciberestafas	185
VI.4. El futuro de los estudios sobre las ciberestafas	187
Referencias bibliográficas	188