

# ÍNDICE

## INTRODUCCIÓN

### CAPÍTULO 1. CIBERDELINCUENCIA

- 1.1 ¿QUÉ ES LA?
- 1.2 LA CONSTANTE EVOLUCIÓN DE LA CIBERDELINCUENCIA
- 1.3 CARACTERÍSTICAS DE LA CIBERDELINCUENCIA
- 1.4 PERFIL DEL CIBERDELINCUENTE. EL DELINCUENTE INFORMÁTICO
- 1.5 TIPOS DE CIBERATAQUES
- 1.6 PREVENCIÓN CONTRA LOS CIBERATAQUES
- 1.7 CASOS IMPORTANTES DE CIBERATAQUES
- 1.8 EVOLUCIÓN DE LOS CIBERDELITOS
- 1.9 CIBERDELINCUENTE Y CIBERVÍCTIMA
- 1.10 LA PRUEBA PERICIAL EN LOS CIBERDELITOS
- 1.11 ESTRATEGIA MUNDIAL CONTRA LA CIBERDELINCUENCIA

### CAPÍTULO 2. CIBERCRIMINALIDAD

- 2.1 CIBERCRIMEN Y CIBERCRIMINALIDAD
- 2.2 DIFERENCIA ENTRE DELITO INFORMÁTICO Y DELITO CIBERNÉTICO
- 2.3 TIPOS DE CIBERCRIMEN
  - 2.3.1 La cibercriminalidad económica
  - 2.3.2 La cibercriminalidad social
  - 2.3.3 La cibercriminalidad política
- 2.4 LA AMENAZA DEL CIBERCRIMEN EN LA SOCIEDAD: MEDIDAS PREVENTIVAS
- 2.5 LA INVESTIGACIÓN Y PERSECUCIÓN DE LA CIBERCRIMINALIDAD
- 2.6 LA IDENTIFICACIÓN Y LA PROBLEMÁTICA PROBATORIA
- 2.7 CIBERCRIMINALIDAD EN LAS PRÓXIMAS DÉCADAS

### CAPÍTULO 3. DELITOS INFORMÁTICOS

- 3.1 DEFINICIÓN DE DELITOS INFORMÁTICOS
- 3.2 LA INFORMÁTICA COMO MEDIO DEL DELITO
- 3.3 DELITO INFORMÁTICO: DELINCUENCIA INFORMÁTICA, CRIMINALIDAD INFORMÁTICA, CIBERDELINCUENCIA, CIBERCRIMEN
- 3.4 SUJETOS DE LOS DELITOS INFORMÁTICOS
- 3.5 BIENES JURÍDICOS PROTEGIDOS EN EL DELITO INFORMÁTICO
- 3.6 NUEVAS TECNOLOGÍAS PARA NUEVOS CONCEPTOS DELICTIVOS: CIBERESPACIO, CIBERDELINCUENCIA, CIBERCRIMEN
- 3.7 TIPOS DE DELITOS INFORMÁTICOS
- 3.8 DELITO DE ESTAFA O FRAUDE INFORMÁTICO
  - 3.8.1 Fraudes cometidos mediante la manipulación de computadoras
  - 3.8.2 Falsificaciones informáticas

- 3.9 FRAUDES FINANCIEROS Y ECONÓMICOS
  - 3.9.1 Fraudes con tarjetas
  - 3.9.2 Ofertas de trabajo falsas
  - 3.9.3 Robo, usurpación o suplantación de identidad
- 3.10 SABOTAJE INFORMÁTICO
- 3.11 DELITOS SEXUALES
- 3.12 DELITOS CONTRA LA INTEGRIDAD SEXUAL
  - 3.12.1 Prostitución infantil
  - 3.12.2 Pornografía infantil
  - 3.12.3 Pedofilia
  - 3.12.4 Grooming
- 3.13 DELITOS DE ACOSO ESCOLAR Y LABORAL
  - 3.13.1 El acoso escolar o bullying
  - 3.13.2 El acoso laboral o mobbing
- 3.14 ROOTKIT (LA AMENAZA INVISIBLE)

## **CAPÍTULO 4. CIBERDELINCUENCIA ORGANIZADA O SAQUEO INFORMÁTICO**

- 4.1 EL CIBERESPACIO COMO CAMPO DELICTIVO
- 4.2 CIBERCRIMEN
  - 4.2.1 Ingresos económicos de forma fraudulenta
  - 4.2.2 Fraude en comercio electrónico
  - 4.2.3 El carding
  - 4.2.4 Ventas en portales de anuncios clasificados
  - 4.2.5 Crime as a service
  - 4.2.6 La infraestructura de mulas
  - 4.2.7 Los timos en la Red
  - 4.2.8 La piratería informática
  - 4.2.9 Blanqueo de capitales
  - 4.2.10 Causas y consecuencias del blanqueo de capitales
  - 4.2.11 Técnicas de blanqueo de capitales
  - 4.2.12 Mecanismos de detección del blanqueo de capitales
- 4.3 CIBERTERRORISMO
  - 4.3.1 Comunicación y propaganda
  - 4.3.2 Financiación de los grupos terroristas
  - 4.3.3 La captación de los seguidores o súbditos
  - 4.3.4 Adoctrinamiento
  - 4.3.5 El uso de Internet y su radicalización en la Red
- 4.4 CIBERGUERRA
  - 4.4.1 ¿Qué es ciberguerra?
  - 4.4.2 El sistema informático en la ciberguerra actual
  - 4.4.3 Ciberespacio: territorio sin fronteras
  - 4.4.4 El conflicto Israel-Hamas
  - 4.4.5 El conflicto Rusia-Ucrania

## **CAPÍTULO 5. HACKERS**

- 5.1 LA APARICIÓN DEL HACKER, JÁQUER O JACKER
- 5.2 LAS HERRAMIENTAS DEL HACKER
- 5.3 LA ENSEÑANZA HACKER
- 5.4 ¿QUIENES SON LOS CRACKERS?
- 5.5 LA OCULTACIÓN DE MENSAJES: LA CRIPTOGRAFÍA
- 5.6 EL SOFTWARE LIBRE
- 5.7 CIBERSOCIEDAD Y CIBERGRUPOS DE HACKERS

- 5.8 ORIGEN Y PRECEDENTES DE LOS HACKERS
- 5.9 LA CIBERSOCIEDAD ACTUAL Y DE FUTURO
- 5.10 CRÓNICAS DE HACKERS Y CRACKERS
  - 5.10.1 El caso del Phreaker ciego
  - 5.10.2 El robo del banco
- 5.11 LA SEGURIDAD EN INTERNET Y LA AMENAZA DE LOS VIRUS INFORMÁTICOS
- 5.12 AMENAZAS Y VULNERABILIDADES DE LOS SISTEMAS INFORMÁTICOS Y DE LOS DATOS
- 5.13 LA IMPORTANCIA DE UNA DEFENSA CIBERNÉTICA PROACTIVA CONTRA LOS CIBERATAQUES
  - 5.13.1 Ataques contra la integridad
  - 5.13.2 Ataques contra la disponibilidad
  - 5.13.3 Ataques contra la privacidad
- 5.14 SEGURIDAD EN SISTEMAS
- 5.15 SEGURIDAD EN REDES
- 5.16 SEGURIDAD EN APLICACIONES WEB Y WEBSERVERS

## **CAPÍTULO 6. REDES SOCIALES**

- 6.1 ATRAPADOS EN LA TELA DE ARAÑA
- 6.2 LA TECNOCRACIA O EL MUNDO DE LA INCOMUNICACIÓN TRADICIONAL
- 6.3 EL FENÓMENO DE LAS REDES SOCIALES EN LA SOCIEDAD
- 6.4 LOS PERFILES DE LOS ADOLESCENTES EN LAS REDES SOCIALES
- 6.5 EL COMPONENTE RELACIONAL, DE ENTRETENIMIENTO Y DE OCIO DE LAS REDES SOCIALES
- 6.6 EL RIESGO DEL USO ABUSIVO DE LAS REDES SOCIALES
- 6.7 LAS REDES SOCIALES COMO MEDIO DE DIFUSIÓN
- 6.8 EL USO DE LAS REDES SOCIALES: PRIVACIDAD Y SEGURIDAD
- 6.9 TENDENCIAS EN LAS REDES SOCIALES
  - 6.9.1 Mayor personalización y algoritmos inteligentes
  - 6.9.2 Inteligencia Artificial (IA) y chatbots
  - 6.9.3 Realidad Virtual (RV) y redes sociales inmersivas
  - 6.9.4 Mayor enfoque en la autenticidad y la transparencia
  - 6.9.5 Contenido generado por los usuarios
  - 6.9.6 Redes sociales de nicho
- 6.10 EL AUGE DE LA UTILIZACIÓN Y EXPANSIÓN DEL TIKTOK
- 6.11 LAS REDES SOCIALES EN LA ACTUALIDAD Y SU IMPACTO SOCIOCULTURAL: BENEFICIOS Y PERJUICIOS DEL USO DE LAS REDES SOCIALES
- 6.12 REDES SOCIALES Y PERSPECTIVAS DE FUTURO

## **CAPÍTULO 7. LEGISLACIÓN**

- 7.1 EL CODIGO PENAL ESPAÑOL Y LA CIBERDELINCUENCIA
- 7.2 DELITOS RECOGIDOS Y TIPIFICADOS EN EL CÓDIGO PENAL ESPAÑOL
  - 7.2.1 Delitos relacionados con el contenido
  - 7.2.2 Descubrimiento y revelación de secretos
  - 7.2.3 Estafa informática
  - 7.2.4 De las defraudaciones de fluido eléctrico y análogas
  - 7.2.5 Daños informáticos
  - 7.2.6 De los delitos relativos a la propiedad intelectual
- 7.3 LA CIBERSEGURIDAD EN LA UNIÓN EUROPEA

**GLOSARIO**

**BIBLIOGRAFÍA**