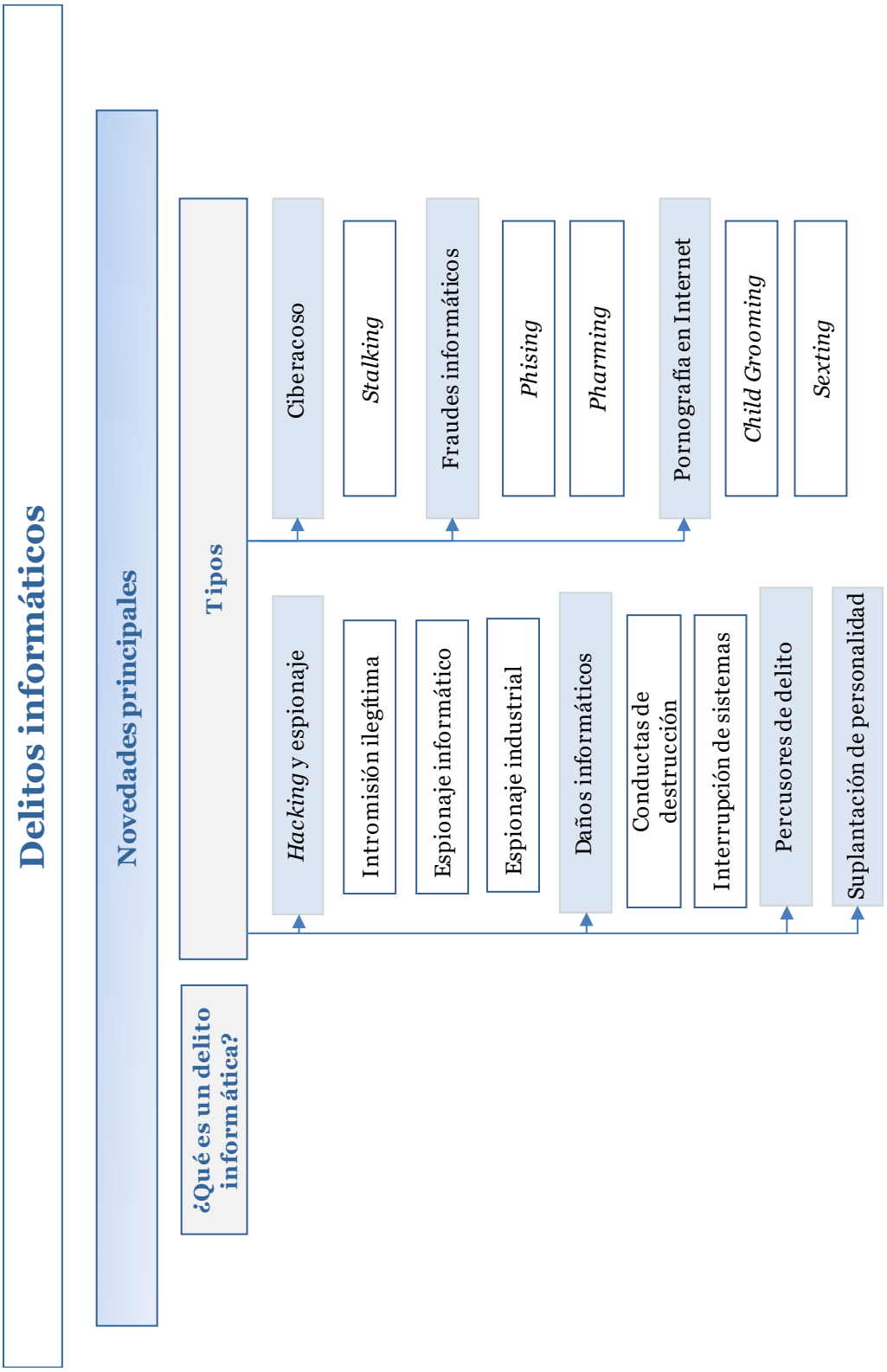
Delitos informáticos y ciberdelincuencia

TEMA 8

Esquema



Ideas clave

8.1. ¿Cómo estudiar este tema?

Para estudiar este tema deberás comprender las **Ideas clave** expuestas en este documento, que se complementan con lecturas y otros recursos para que puedas ampliar los conocimientos sobre el mismo.

En este tema realizaremos una introducción al derecho penal informático y a la ciberdelincuencia.

- Analizaremos el sentido de la aparición de los delitos informáticos y de la ciberdelincuencia.
- Comprenderemos la tipología de los ciberdelitos más importantes: *hacking* y espionaje, daños informáticos, precursores del delito, suplantación de personalidad, ciberacoso, ciberfraude y pornografía en Internet.
- Entenderemos qué son la prueba electrónica y la prueba pericial forense.

8.2. Introducción a los delitos informáticos

Tal como sostiene Lessig (2001), el ciberespacio no es un lugar, sino muchos lugares y las características de cada uno de ellos no son siempre idénticos, difiriendo entre sí en sus características más fundamentales.

Las TIC unido a Internet han potenciado los efectos de la delincuencia tradicional. De esta forma, y siguiendo a Gutiérrez Francés, el «cibercrimen se mueve en la práctica impunidad de un espacio virtual y sin fronteras, el espacio que suministra Internet, la Red de redes» (Gutiérrez Francés, 2005, p. 72).

Cuando pensamos en delitos informáticos nos vienen a la cabeza conductas como el *hacking*, fraude informático, *cyberbullying*, ciberterrorismo, usurpación de perfiles en redes sociales, piratería, virus, troyanos, pornografía infantil, *child grooming*, espionaje personal e industrial, *phishing, pharming, malware*, y muchas más conductas que describen acciones muy distintas y que atacan a priori a bienes jurídicos también distintos.

La Fiscalía General del Estado en su Instrucción 2/2011 definió al delito informático como aquel que se comete:

- Contra equipos y sistemas (por ejemplo, daños informáticos).
- A través de equipos y sistemas (por ejemplo, fraudes informáticos).
- Con la ayuda de sistemas (por ejemplo, blanqueo).

El Convenio de cibercriminalidad de Budapest proporciona una clasificación oficial. Serían delitos informáticos según dicho instrumento internacional los siguientes:

- Delitos contra la confidencialidad, integridad y disponibilidad de datos y sistemas informáticos.
- Fraudes y falsificaciones informáticas.
- Pornografía infantil.
- Infracciones de propiedad intelectual y otros derechos.

Pasemos ahora a examinar algunos supuestos de delitos informáticos.

8.3. Tipos de delitos informáticos

Hacking y espionaje

- **Intromisión ilegítima.** El delito de intromisión ilegítima, intrusión o *hacking* tiene que ver con el acceso intencional a un sistema o equipo informático sin autorización de su titular, una conducta introducida en el año 2010 en el Código Penal y trasladada al artículo 197 bis CP con la Reforma 2015. Los elementos del delito son:

  - Acceso no autorizado a datos o programas de un sistema.
  - Vulnerando medidas de seguridad.
  - O bien permanencia en el sistema informático contra la voluntad de quien tenga derecho a excluirnos.

  El hacker utiliza distintas técnicas combinadas para introducirse en sistemas informáticos ajenos: conocimientos técnicos sobre redes y comunicaciones, así como

explotación de información sobre sus usuarios. Normalmente las intromisiones se producen mediante técnicas de ingeniería social o con el uso de malware9 (normalmente *software* espía). Mediante *spyware* el cibercriminal obtiene claves de acceso y datos personales con los que perpetrar la intromisión. Pero el cibercriminal en muchas ocasiones, aunque presuma de conocimientos técnicos, actúa fundamentalmente a través de técnicas de ingeniería social.

El *hacking* o intrusismo informático, consistente en el acceso no autorizado, por lo general violando los mecanismos de seguridad allí donde los haya, a los archivos y bases de datos contenidos en los sistemas informáticos ajenos, normalmente de grandes empresas o instituciones. El problema más grave es la incardinación de la mayoría de las conductas de hacking en el derecho penal represivo.

- **Espionaje informático.** El delito del artículo 197.2 CP regula la obtención de datos personales o familiares registrados en sistemas informáticos o el acceso a cualquier tipo de dato informático de carácter personal con el fin de perjudicar al titular de los datos, siendo el supuesto más habitual de espionaje. El delito tiene que ver con la interceptación de comunicaciones, sea durante su transmisión, sea en su origen o en destino y está previsto también para el apoderamiento de mensajes impresos. Protege cualquier comunicación telemática de injerencias *inconsentidas*, incluyendo la mensajería instantánea.

- **Espionaje industrial.** Hace referencia a los *secretos de empresa* donde reside la dificultad interpretativa de determinar precisamente en qué consisten esos secretos.

Daños informáticos

Hasta el año 2010 los daños informáticos eran una modalidad agravada del delito de daños tradicional, lo que dificultaba mucho la interpretación del tipo penal porque en definitiva se remitía a una estructura típica antigua pensada para la destrucción de *cosas*, de objetos. Después de la firma del Convenio de Cibercriminalidad se tipifica en España el sabotaje informático como delito independiente (actuales artículos 264 a 264 ter CP) que recoge tres grandes casos: destrucción de datos, programas o documentos; interrupción del funcionamiento de sistemas; y precursores del delito.

- **Conductas de destrucción.** Según el artículo 264.1 CP:

  > «El que, por cualquier medio, sin autorización y de manera grave borrase, dañase, deteriorase, alterase, suprimiese o hiciese inaccesibles datos informáticos, programas informáticos o documentos electrónicos ajenos, cuando el resultado producido fuera grave, será castigado con la pena de prisión de seis meses a tres años. La redacción recoge, por tanto, conductas de destrucción de datos que nos hacen pensar en supuestos de hacking, cracking, virus, troyanos, y en la mayoría de supuestos prácticos en conductas de borrado masivo de información ajena».

  Para que exista el delito debe darse una alteración o daño que afecte a la funcionalidad de los datos informáticos pues tenemos que asumir un concepto funcional de la propiedad más allá de la indemnidad de la *cosa* ya que en materia informática la destrucción de datos siempre es relativa al poderse, por definición, restablecer cualquier tipo de dato informático ya que es de creación humana.

- **Interrupción de sistemas.** Según el vigente artículo 264 bis CP, erá castigado con la pena de prisión de seis meses a tres años el que, sin estar autorizado y de manera grave, obstaculizara o interrumpiera el funcionamiento de un sistema informático ajeno. Ello debe hacerse de los tres tipos de formas que dicho artículo regula y que son distintas modalidades de destrucción, alteración, inutilización, introducción de datos, etc.

  En 2010 se introduce expresamente como delito la interrupción de servicios informáticos, una conducta de daño no permanente relacionada con el fenómeno de los ataques de «denegación de servicio» o *Denial-of-Service attacks* (ataques DoS).

Precursores del delito

Los precursores se definen como las conductas destinadas a facilitar la comisión de otros delitos en materia informática. El delincuente informático ya no tiene porqué saber informática para cometer delitos pues existe una real oferta en Internet. El Código Penal prevé la sanción de los programas de anulación de la protección de *software* (270.3 CP) que son fórmulas preparatorias de delitos contra la propiedad intelectual (*software* de liberación de programa de prueba, destrucción de la protección anticopia). También se sanciona el *software* que permite el acceso a servicios protegidos o que sirve para la duplicación de equipos (286 CP). Se trata de conductas de facilitación del acceso a servicios condicionados concurriendo una finalidad comercial y ánimo de lucro.

Suplantación de personalidad

El derecho penal solo podrá entrar a sancionar conductas de suplantación que signifiquen una usurpación no-esporádica de los signos de identidad de alguien y vinculada a actuaciones que generen obligaciones o produzcan efectos económicos o jurídicos, por lo que normalmente irá asociado a otro tipo de delitos: falsificación de documentos informáticos, estafas, etc.

Ciberacoso

- **El *stalking*.** La Reforma 2015 ha incriminado por primera vez en el nuevo artículo 172 ter CP dicha conducta: Será castigado con la pena de prisión de tres meses a dos años o multa de seis a veinticuatro meses el que acose a una persona llevando a cabo de forma insistente y reiterada, y sin estar legítimamente autorizado, alguna de las conductas siguientes y, de este modo, altere gravemente el desarrollo de su vida cotidiana:

  1.º La vigile, la persiga o busque su cercanía física.

  2.º Establezca o intente establecer contacto con ella a través de cualquier medio de comunicación, o por medio de terceras personas.

  3.º Mediante el uso indebido de sus datos personales, adquiera productos o mercancías, o contrate servicios, o haga que terceras personas se pongan en contacto con ella.

  4.º Atente contra su libertad o contra su patrimonio, o contra la libertad o patrimonio de otra persona próxima a ella.

  5.º Realice cualquier otra conducta análoga a las anteriores.

Fraudes informáticos o ciberfraude

El ciberfraude, según los datos conocidos en España ocupa el 75 % de los hechos delictivos cometidos en la Red. Una de las características principales de la estafa informática es que estructuralmente no es exigible el engaño.

- ***Phising.*** Se conoce como *'phishing'* a la suplantación de identidad (en Internet, pero también por otras vías) que persigue apropiarse de datos confidenciales de los usuarios para, en base a ellos, conseguir menoscabar patrimonios ajenos. El delito consiste en obtener información tal como números de tarjetas de crédito, contraseñas, información de cuentas u otros datos personales por medio de engaños.

Este tipo de fraude se efectúa habitualmente a través de mensajes de correo electrónico o de ventanas emergentes.

- ***Pharming.*** *Pharming* es la explotación de una vulnerabilidad en el *software* de los servidores DNS (Domain Name System) o en el de los equipos de los propios usuarios, que permite a un atacante redirigir un nombre de dominio (*domain name*) a otro ordenador diferente. De esta forma, un usuario que introduzca un determinado nombre de dominio que haya sido redirigido, accederá en su explorador de Internet a la página web que el atacante haya especificado para ese nombre de dominio. La técnica de *pharming* se utiliza normalmente para realizar ataques de *phishing*, redirigiendo el nombre de dominio de una entidad de confianza a una página web, en apariencia idéntica, pero que en realidad ha sido creada por el atacante para obtener los datos privados del usuario, generalmente datos bancarios. La «manipulación» se corresponde con la conducta de alterar, modificar u ocultar datos informáticos de manera que se realicen operaciones de forma incorrecta o que no se lleven a cabo.

En cuanto a la conducta del «mulero» (persona que abre o «presta» su cuenta corriente para que el *phiser* haga el ingreso del dinero de las víctimas, normalmente mediante un reparto del botín, bien por una cantidad a tanto alzado o mediante una cuota o porcentaje. No es impune y se calificará, en función de los casos, o como un delito de estafa informática del art. 248.2 del CP (STS 533/ 2007, de 12 de junio) o, como un delito de blanqueo de capitales del art. 301 del CP, atendiendo a las circunstancias concurrentes, singularmente al origen del dinero.

Pornografía en Internet

El bien jurídico protegido en estos delitos no se reduce únicamente a la libertad sexual, ya que también se han de tener en cuenta los derechos inherentes a la dignidad de la persona humana y el derecho al libre desarrollo de su personalidad y la indemnidad e integridad sexual de los menores e incapaces.

- ***Child Grooming.*** Actualmente el art. 183 TER establece que:

> «1. El que a través de Internet, del teléfono, o cualquier otra tecnología de la información y la comunicación contacte con un menor de dieciséis años y proponga concertar un encuentro con el mismo a fin de cometer cualquiera de los delitos descritos en los artículos 183 y 189, siempre que tal propuesta se acompañe de actos materiales encaminados al acercamiento, será castigado con la pena de uno a tres años de prisión o

> multa de doce a veinticuatro meses, sin perjuicio de las penas correspondientes a los delitos en su caso cometidos. Las penas se impondrán en su mitad superior cuando el acercamiento se obtenga mediante coacción, intimidación o engaño».

- ***Sexting*.** La exposición de motivos lo justifica de la siguiente manera:

> «La protección de los menores frente a los abusos cometidos a través de Internet u otros medios de telecomunicación, debido a la facilidad de acceso y el anonimato que proporcionan, se completa con un nuevo apartado en el artículo 183 ter del Código Penal destinado a sancionar al que a través de medios tecnológicos contacte con un menor de dieciséis años y realice actos dirigidos a embaucarle para que le facilite material pornográfico o le muestre imágenes pornográficas».

8.4. La prueba electrónica

Algunos autores de distintos países se refieren a esta prueba como «prueba digital», algunos como «prueba informática», otro sector como «prueba tecnológica» y unos últimos como «prueba electrónica». **La peripecia y la estrategia procesal** que adopten las partes será determinante para que será imprescindible para convencer de la conveniencia e importancia de la prueba electrónica. Para ello, podrá ir acompañada con **informes periciales** que expliquen cómo fue obtenida y conservada. Hemos de tener en cuenta, que, además, en materia penal, rige **el principio de libertad probatoria.** ¿Qué tipos de pruebas electrónicas se pueden presentar en sede judicial?

Partiremos de un sistema *numerus apertus* según el profesor Bueno de Mata (2014):

- Creadas a través de la informática. No dispondrán de un formato físico. Ejemplo, *cookies*, *tags, logs*, etc.
- Proceden de reproducción o archivos electrónicos, vídeos, o fotografía digital. Ejemplo, fotografías digitales.
- Presentadas mediante un *hardware*. Es decir, a través de una CPU, disco externo, *pen drive*.
- Pruebas electrónicas mixtas. En este caso, las pruebas tradicionales entrarían en contacto con las nuevas tecnologías de la información, con lo que nos encontraríamos ante pruebas mutadas. Ejemplo, prueba pericial electrónica o prueba testifical

Validez probatoria de pantallazos de whatsApp

Si partimos de la base del principio de la libertad para presentar pruebas en el proceso penal, se puede deducir que los medios como Facebook o Twitter, o WhatsApp pueden ser válidos como prueba. Pero, se deberá ser cauto y evitar cualquier debilidad en la autenticidad de la prueba sino queremos que sea impugnada por la parte contraria. Por ello, enumero algunos consejos:

- En primer lugar, por lo que será necesario la **Intervención** de un **notario** para acreditar la validez (mediante acta) con copia escrita de los mensajes. Se recomienda en ese momento la intervención de un **perito de informática forense** y de abogados especializados en nuevas tecnologías.

- En segundo lugar, tal y como recomiendan los expertos, la prueba electrónica se puede **complementar** con **otras pruebas** como pueden ser las **testificales o documentales** (pantallazos). No obstante, tampoco resultaría excesivo aportar y entregar el **dispositivo** juzgado o fiscalía para eventuales cotejos. En estos casos la prueba es plenamente **válida**; sin perjuicio de la valoración de su eficacia probatoria por el juez o tribunal, que dependerá básicamente de la postura de las partes procesales. Si la otra parte no lo impugna, existen grandes posibilidades de que el juez o tribunal le otorgue eficacia probatoria.

- En tercer lugar, tendremos que **acreditar la autoría** del mensaje por el titular de la línea. Cabe recordar que el uso del WhatsApp exige la contratación de un servicio de Internet móvil, de tal forma que los mensajes son enviados a través de la red desde el número de teléfono del titular hasta el número de teléfono del destinatario. De esta forma, cabe preguntarse ¿cómo se puede acreditar que el titular y denunciado de la línea es quien ha enviado el mensaje de las amenazas que ha de ser probado?

  En principio, sería razonable pensar que el titular sí ha enviado el mensaje; y correspondería a la parte que niega este hecho la acreditación de aquellos elementos fácticos que lo prueben: acceso ordinario al teléfono móvil o dispositivo electrónico por otras personas y/o conocimiento de la clave de acceso por terceros; sustracción o pérdida del dispositivo, etc. Estas últimas suelen ser usadas por la defensa del acusado normalmente, por eso la intervención del escribano y del informático forense puede ser fundamental.

- En cuarto lugar, respecto el ámbito de la **privacidad y el honor**, se requiere que el dato obtenido por una intromisión estatal sea relacionado con algún aspecto de la maniobra ilícita investigada. Por ejemplo, si es necesario entrar a la cuenta de una red social del acusado, para que la limitación al derecho sea constitucionalmente legítima en la faz procesal penal, es preciso que su adopción sea dispuesta por **autoridad judicial**.

- En quinto lugar, uno de los métodos por excelencia, que se usa para respetar la **cadena de custodia,** es el **uso del *hash*** que es un algoritmo formado por números y letras que está relacionado con el archivo de la prueba digital. ¿Para qué servirá a la autoridad judicial? Para verificar si sigue intacto y no se ha modificado. En caso negativo, la cadena de custodia se habría violado, y por tanto no podría utilizarse como prueba.

8.5. La prueba pericial forense

Tipos de peritos

En primer lugar, corresponde determinar los tipos de peritos informáticos existentes:

- **Forense**. Según Wikipedia, la informática forense ayuda a detectar pistas sobre ataques informáticos, robo de información, conversaciones, pistas, etc., dentro de un entorno informático.

- **De gestión.** El peritaje de gestión o *management*, está asociado más a las auditorías informáticas, que a la Informática Forense. varios estándares establecidos para ayudar al perito de gestión a elaborar su desempeño, como son COBIT, ITIL, CMMI, o la propia normativa ISO 9001. En todos estos estándares se desarrollan todos los elementos que deben contemplarse, a la hora de hacer un Análisis de Gestión.

- **Tasador.** Es la persona que estima el valor de un activo o un pasivo de una empresa basándose bien en estándares o tablas ya definidos, o a baremos de referencias ampliamente reconocidas por la comunidad profesional.

- **Telemático.** El perito telemático, podría considerarse como una variante del perito informático forense, pero especializado en terminales móviles. La extracción de los datos de un teléfono móvil puede hacerse por hardware o *software* (herramientas forenses de *hardware*, tales como las UFED «cellebrite», o UFED «Chinex», para teléfonos chinos, son las más reconocidas internacionalmente).

El proceso probatorio pericial forense

- **Fase de actuación.** El perito, antes de empezar con los trabajos, debe tener permiso explícito para el manejo de las evidencias o de los objetos que las contienen, por parte de quien le entregue los elementos de estudio.

- **Fase de identificación.** En este punto es preciso recordar que, en muchos casos el **fedatario público** podrá dar fe.

> De haber visto tal o cual cosa, o que tal dispositivo tiene tal número de serie, pero, en más de una ocasión, sus testimonios han sido desmontados en los juzgados por abogados eficientes que, haciendo las preguntas correctas, han demostrado que el fedatario no sabe a ciencia cierta qué se ha hecho, ni cómo se ha actuado con la prueba, ni qué se ha obtenido; todo esto debido, sin duda, a la falta de conocimientos tecnológicos de muchos de estos profesionales aún tienen.

Es muy recomendable que el perito tome **fotografías del escenario**, así como de los elementos a analizar, para acompañarlas posteriormente en el informe. Una imagen vale más que mil palabras; siempre se ha dicho. De hecho, la fotografía forense es una técnica que, cada vez más, se está implantando en todas las actuaciones judiciales, periciales y forenses de cualquier tipo.

- **Fase de recopilación.** Deben observarse:

  - **Principios de autenticidad y conservación,** de tal manera que se pueda acreditar que el elemento original no ha sufrido alteraciones en el momento de la identificación y posterior catalogación.
  - **Principio de legalidad:** una prueba obtenida de forma ilegal, o una información recopilada sin permiso de su propietario no solo es una prueba inútil, sino que puede sentar al perito en el banquillo de los acusados.

- **Principio de idoneidad,** de tal forma que los elementos o la documentación obtenida contengan información que sea relevante para el caso asignado.
- **Principio de inalterabilidad:** durante el proceso de la recopilación de las evidencias físicas ha de garantizarse que estas no van a ser alteradas, generando *in situ*, si es preciso, la cadena de custodia de esa evidencia, para luego clonarla –si no es posible hacerlo sobre la marcha-, en el laboratorio. De esta forma, al *trabajar sobre las copias*, se acredita la inalterabilidad de los datos contenidos en el soporte original.
- **Documentación:** Es preciso documentar todos y cada uno de los pasos que se van realizando a lo largo de la fase de recopilación, incluyendo datos fotográficos del proceso.
- **Principio de volatilidad***:* establece el orden en que debe hacerse la recopilación de las evidencias. Ejemplo, Los registros de la caché, la tabla de enrutamiento, la tabla ARP, las tablas de procesos, información del kernel, memoria, archivos temporales del sistema. dispositivos de almacenamiento (discos, pendrives, etc.).
- **Principio de privacidad:** El perito debe ser consciente en todo momento de que la información personal es inviolable, salvo mandato judicial.

» **Fase de tratamiento.** Hay que tener en cuenta que:

- **Tiene que ser una prueba admisible;** es decir: el tratamiento de la prueba debe ajustarse al marco legal, acreditándose en todo momento los diferentes pasos que se han establecido durante el proceso, de tal forma que no haya duda posible de que las evidencias obtenidas pertenecen al dispositivo sobre el que se ha trabajado.
- **Tiene que ser auténtica:** tiene que poder vincularse de forma fácil la prueba material, con el escenario en que se produjo el incidente
- **Tiene que ser completa:** reproduciendo toda la historia de esta, desde que se localizó, hasta que se presentaron las evidencias obtenidas.
- **Tiene que ser fiable:** no puede generarse ninguna duda acerca de cómo la prueba fue obtenida y cómo se hizo el análisis de las evidencias, y finalmente
- **Tiene que ser entendible**: pues de nada sirve hacer un informe exhaustivo y sobre la prueba, si esta no se sabe explicar, o si no es comprensible por el tribunal.

Siempre que sea posible ha de procederse a una **clonación idéntica, fidedigna**, de los elementos originales, para trabajar después con las copias, sin miedo a que las

posibles alteraciones debidas a la manipulación de esta puedan destruir evidencias que podrían ser relevantes para el caso que se trate.

Como medida que garantice la fidelidad y exactitud de los datos existentes en ambos dispositivos –el original y el clonado-, habrá que emplear **funciones *hash*** que acrediten (mediante la igualdad numérica arrojada por el algoritmo) que ambas copias o imágenes son idénticas.

8.6. Referencias bibliográficas

Bueno de Mata, F. (2014). *Prueba electrónica y proceso 2.0*. Madrid: Tirant lo Blanch.

Gutiérrez Francés, M. L. (2005). Reflexiones sobre la ciberdelincuencia hoy (en torno a la Ley penal en el espacio virtual. *Revista elecrtónica del Departamento de Derecho de la Universidad de La Rioja, 3*. Recuperado de: https://dialnet.unirioja.es/servlet/articulo?codigo=1396379

Lessig, L. (2001). *El código y otras leyes del ciberespacio*. Madrid: Taurus.

Lo + recomendado

No dejes de leer…

Código penal

Ley Orgánica 10/1995, de 23 de noviembre, del Código Penal.

Se recomienda que leas la siguiente ley.

Accede al documento a través del aula virtual o desde la siguiente dirección web:
http://noticias.juridicas.com/base_datos/Penal/lo10-1995.html

No dejes de ver…

Derechos fundamentales en la era digital

Eloy Velasco, juez magistrado de la Audiencia Nacional, Doctor en Derecho con una tesis pionera en la investigación de los delitos informáticos es uno de los mayores expertos en cibercrimen de España. En este vídeo nos habla sobre la irrupción de las nuevas tecnologías obliga a reformular los mecanismos jurídicos de protección de los derechos fundamentales de las personas.

Accede al vídeo a través del aula virtual o desde la siguiente dirección web:
https://www.youtube.com/watch?v=d_cuFAmp5ws

Ciberdelincuencia organizada, caso práctico: Inteligencia económica… (UCO, guardia civil)

En la siguiente conferencia nos hablan sobre la ciberdelincuencia organizada.

Accede al vídeo a través del aula virtual o desde la siguiente dirección web:
https://www.youtube.com/watch?v=NThbCnhG8AA

Ciberdelincuencia

En la siguiente *Openclass* de UNIR con Jorge Ramiro hablaremos de la cibercriminología.

Accede al vídeo a través del aula virtual o desde la siguiente dirección web:
https://www.youtube.com/watch?v=3vRW3ZpMxdo

+ Información

A fondo

Cibercrimen. Ciberguerra. Ciberespionaje. Nadie está a salvo en Internet

Reportaje de El País Semanal sobre las ciberamenazas que vivimos hoy en día.

Accede al documento a través del aula virtual o desde la siguiente dirección web:
https://elpais.com/elpais/2018/01/22/eps/1516637253_754345.html

Bibliografía

Barrio, M. (2012). El régimen jurídico de los delitos cometidos en internet en el derecho español tras la reforma penal de 2010. *Revista de derecho y nuevas tecnologías*, *27,* p. 35.

Miró F. (2013). *El cibercrimen: fenomenología y criminología de la delincuencia en el ciberespacio*. Madrid: Marcial Pons.

Velasco, E. (2010). *Delitos cometidos a través de internet: cuestiones procesales*. Madrid: La Ley.

Test

1. ¿Cuál es el objeto del delito de espionaje industrial? Selecciona una:

A. Información que tenga el carácter de secreto de empresa.

B. Cualquier tipo de dato económico.

C. Datos informáticos de cualquier tipo.

D. Datos personales de trabajadores.

2. El delito que tiene que ver con el acceso intencional a un sistema o equipo informático sin autorización de su titular es:

A. Ciberacoso.

B. Ciberfraude.

C. Intromisión ilegítima.

D. Espionaje.

3. El sabotaje informático como delito informático se recoge en los siguientes tres casos:

A. Destrucción de datos, programas o documentos; interrupción del funcionamiento de sistemas; y precursores del delito.

B. Destrucción de datos, programas o documentos; interrupción del funcionamiento de sistemas; y espionaje.

C. Destrucción de datos, programas o documentos; interrupción del funcionamiento de sistemas; y ciberfraude.

D. Espionaje, intromisión y cibefraude.

4. Las conductas destinadas a facilitar la comisión de otros delitos en materia informática:

A. Los facilitadores del delito.

B. Los impulsadores del delito.

C. Los precursores del delito.

D. Ninguna de las anteriores es correcta.

5. La suplantación de identidad en Internet que persigue apropiarse de datos confidenciales de los usuarios para menoscabar patrimonios ajenos se denomina:

A. *Phising*.

B. Suplantación de identidad.

C. *Pharming*.

D. Ninguna de las anteriores es correcta.

6. La explotación de una vulnerabilidad en el software de los servidores DNS o en el de los equipos de los usuarios que permite a un atacante redirigir uno nombre de dominio a otro ordenador diferentes se denomina:

A. *Phising*.

B. Suplantación de identidad.

C. *Pharming*.

D. Ninguna de las anteriores es correcta.

7. Los pantallazos de WhatsApp:

A. Se admitirán como prueba electrónica en sede judicial si es auténtica y no se impugna por la parte contraria.

B. Se aconseja que vayan acompañados de acta notarial, de otras pruebas documentales o testificales y del propio dispositivo móvil.

C. Se aconseja acreditar la autoría, respetar el ámbito de la privacidad y la cadena de custodia (*hash*).

D. Las tres respuestas anteriores son correctas.

8. El perito especializado en la extracción de datos terminales móviles por *hardware* o *software* se denomina:

A. De gestión.

B. Tasador.

C. Telemático.

D. Forense.

9. El principio que establece que durante el proceso de la recopilación de las evidencias físicas ha de garantizarse que estas no sean alteradas, generando *in situ*, si es preciso, la cadena de custodia de esa evidencia es:

A. el principio de idoneidad.

B. el principio de proporcionalidad.

C. el principio de privacidad.

D. El principio de inalterabilidad.

10. La prueba pericial ha de ser:

A. Admisible, auténtica, inalterable, fiable y accesible.

B. Admisible, auténtica, completa, fiable y entendible.

C. Admisible, auténtica, completa, fiable y privada.

D. Ninguna de las anteriores es correcta.