ANEXO DE LECTURAS OBLIGATORIAS

CURSO: “DELITOS INFORMATICOS”

UNIDAD I: CONOCIMIENTOS TECNICOS

1. EL SECRETO DE LAS COMUNICACIONES CON EL ABOGADO DEFENSOR EN LA NUEVA SOCIEDAD DE LA INFORMACIÓN- INMACULADA LÓPEZ-BARAJAS PEREA.

EL SECRETO DE LAS COMUNICACIONES CON EL ABOGADO DEFENSOR EN LA NUEVA SOCIEDAD DE LA INFORMACIÓN

INMACULADA LÓPEZ-BARAJAS PEREA
Profesora Contratada Doctora de Derecho Procesal
UNED

I. El derecho al secreto de las comunicaciones y su virtualidad expansiva

La expansión de las redes de telecomunicaciones y, en especial, de Internet como vehículo de comunicación, transmisión e intercambio de todo tipo de información a gran velocidad, ha originado una auténtica "revolución tecnológica digital", de forma semejante a lo que sucedió en la Revolución Industrial del siglo XIX.

Los profundos cambios y transformaciones sociales que se han producido han dado paso a la denominada "sociedad de la información"[1] en la que los modelos de negocio, de ocio e, incluso, la estrategia militar se diseñan con base en la red[2]. Hoy, el factor tecno-comunicativo constituye una herramienta esencial.

Hasta hace pocas décadas el teléfono fijo era la única vía de telecomunicación al alcance real de la ciudadanía. Hoy se puede afirmar que las comunicaciones telefónicas clásicas han quedado superadas o, mejor dicho absorbidas, por las telemáticas o electrónicas. Existen hoy centrales digitales de conmutación automática, totalmente electrónicas y controladas por ordenador, permiten además multitud de servicios complementarios al propio establecimiento de la comunicación como por ejemplo los denominados servicios de valor añadido.

Aunque el derecho al secreto de las comunicaciones se reconoce como garantía en todas las Constituciones, así como en las normas internacionales, el Tribunal Europeo de Derechos Humanos ha puesto de manifiesto que la vida privada es un término abierto no susceptible de una definición exhaustiva, que

---

[1] CORRIPIO GIL-DELGADO y MARROIG POL, *El tratamiento de los datos de carácter personal y la protección de la intimidad en el sector de las telecomunicaciones,* Agencia de Protección de Datos, Madrid, 2001, pág. 55.

[2] Vid. Exposición de Motivos de la Ley de Servicios de la Sociedad de la Información y Comercio Electrónico 34/2002; SALOM CLONET, "Incidencia de la nueva regulación en la investigación de los delitos cometidos a través de medios informáticos", en AA.VV, *La protección de datos en la cooperación policial y judicial,* Thomson-Aranzadi, 2008, pág.152.

deber ser interpretado a la luz de las condiciones actuales de vida propias de la Sociedad de la información en la que estamos inmersos para proteger al individuo de forma real y efectiva en aquellos ámbitos a los que se refiere[3].

Como ha señalado nuestro Tribunal Constitucional, los avances tecnológicos que en los últimos tiempos se han producido en el ámbito de las telecomunicaciones, especialmente en conexión con el uso de la informática, hacen necesario un nuevo entendimiento del concepto de comunicación y del objeto del derecho fundamental, que extienda la protección a esos nuevos ámbitos, como se deriva necesariamente del tenor literal del art. 18.3 CE[4].

La doctrina[5] ha destacado la enorme virtualidad expansiva del derecho a la vida privada y al secreto de las comunicaciones en un contexto en el que existe una gran capacidad tecnológica de control social en manos del Estado. Podemos afirmar que la garantía del derecho a la esfera privada es uno de los grandes desafíos de los ordenamientos jurídicos en la actualidad toda vez que los ciudadanos se sienten cada vez más amenazados en su ámbito de libertad personal.

II. El derecho a la asistencia de abogado como instrumento del derecho de defensa

La asistencia letrada dentro del proceso judicial forma parte inescindible del mas amplio derecho de defensa, que ha sido calificado como el más elemental de los derechos del imputado[6]. El Pacto Internacional de Derechos Civiles y Políticos de 1966 establece que toda persona acusada de un delito, durante el proceso tendrá derecho a unas garantías mínimas, entre las cuales, se encuentra la de disponer del tiempo y de los medios adecuados para la preparación de su defensa y a comunicarse con un defensor de su elección (art. 14).

Con objeto de salvaguardar mejor el mencionado derecho de defensa, nuestro legislador además de reconocer el derecho del imputado a ser asistido por un Abogado, dispone que la defensa técnica es obligatoria en el proceso por delitos[7]. De conformidad con lo dispuesto por el art. 767 de la LECrim, en su redacción dada por la Ley 38/2002, obligatoriamente ha de designarse Abogado defensor desde que en las diligencias practicadas por cualquiera de los órganos públicos encargados de la persecución penal resulte una imputación

---

[3] Caso Raninen c. Finlandia, Sentencia de 16 de diciembre de 1997; Caso Burghartz c. Suiza, Sentencia de 22 de febrero de 1994.

[4] STC 70/2002.

[5] AROZ SANTISTEBAN, "Derecho al respeto de la vida privada y familiar" en *Convenio Europeo de Derechos Humanos. Comentario sistemático,* Thomson-Civitas, 2004, pág. 260.

[6] Vid. STEDH de 20 de junio de 1988 -asunto Schönenberger y Durmaz-.

[7] Vid. GIMENO SENDRA, *Los Procesos Penales. Comentarios a la Ley de Enjuiciamiento Criminal*, 2000, Bosch, pág. 171.

contra persona determinada. La Policía Judicial, el Ministerio Fiscal o la autoridad judicial recabarán de inmediato del Colegio de Abogados la designación de un abogado de oficio, si no lo hubiere nombrado ya el interesado. Este derecho es exigible, pues, desde la misma puesta en marcha del procedimiento penal[8], desde el instante en que exista una imputación contra una persona determinada.

Ha señalado el Tribunal Constitucional que en los supuestos en que la intervención del Letrado sea preceptiva, esta garantía constitucional se convierte en una exigencia estructural del proceso tendente a asegurar su correcto desenvolvimiento, cuyo sentido es satisfacer el fin común a toda asistencia letrada que es el de lograr el adecuado desarrollo del proceso como mecanismo instrumental introducido por el legislador con miras a una dialéctica procesal efectiva que facilita al órgano judicial la búsqueda de una sentencia ajustada a Derecho. La conexión existente entre el derecho a la asistencia letrada y la institución misma del proceso determina, incluso, que la pasividad del titular del derecho deba ser suplida por el órgano judicial para cuya propia actuación, y no sólo para el mejor servicio de los derechos e intereses del defendido, es necesaria la asistencia del Letrado (STC 174/2009).

De lo expuesto se deduce que el derecho de defensa formal en el proceso penal no es un derecho que lo pueda o no ejercitar el imputado sino que constituye un requisito legal en el juicio oral por lo que deberá ejercitarse incluso con oposición del propio imputado. Dado que el acusador público –el Ministerio Fiscal– es un técnico en Derecho, el principio de igualdad de armas exige que el acusado sea defendido también por un técnico, el Letrado. Por esta razón se ha establecido la obligatoriedad de la defensa técnica del acusado (STC 29/1995).

La doctrina constitucional también ha proclamado la extensión del derecho a la asistencia de Abogado incluso en los procedimientos en que no resulta obligatoria, considerando que "el hecho de que la intervención de Letrado no sea preceptiva en un proceso determinado, con arreglo a las normas procesales, no priva al justiciable del derecho a la defensa y asistencia letrada que le reconoce el art. 24.2 CE, pues el carácter no preceptivo o necesario de la intervención del Abogado en ciertos procedimientos no obliga a las partes a actuar personalmente, sino que les faculta para elegir entre la autodefensa o la defensa técnica, pero permaneciendo, en consecuencia, el derecho de asistencia letrada incólume en tales casos, cuyo ejercicio queda a la disponibilidad de las partes, lo cual conlleva, en principio, el derecho del litigante que carece de recursos económicos para sufragar un Letrado de su elección a que se le provea de Abogado de oficio, si así lo considera conveniente a la mejor defensa de sus

[8] RAMOS MÉNDEZ, *Enjuiciamiento Criminal. Novena Lectura Constitucional,* Atelier, 2010, pág. 280.

derechos, siendo procedente el nombramiento de oficio cuando se solicite y resulte necesario" (SSTC 212/1998, 152/2000).

Pero el nombramiento de un Abogado no asegura, por sí mismo, la efectividad de la asistencia que puede proporcionar al acusado (STEDH de 24 de noviembre de 1993 -caso Imbrioscia-). La presencia obligada de los letrados no puede considerarse defensa, siendo en este sentido muy significativa la expresión del art. 6.3 c) del Convenio de Roma que habla de "asistencia letrada" y no de presencia letrada[9]. Por ello, las autoridades estatales han de adoptar las medidas necesarias para que esta asistencia sea concreta y efectiva (STEDH de 21 de abril de 1998 -caso Daud-).

También, el Tribunal Constitucional ha establecido que la asistencia de Abogado no se puede reducir a una mera designación formal sino que es preciso extremar las cautelas para que la defensa sea real y efectiva. Los órganos judiciales han de velar por evitar la indefensión del justiciable en el proceso penal, especialmente en los casos en que la dirección y representación se realiza mediante la designación de oficio (STC 47/2003).

III. La confidencialidad de las comunicaciones con el abogado defensor

De conformidad con lo expuesto, la efectividad del derecho de defensa no sólo depende del reconocimiento del derecho a recibir los servicios de un abogado, sino también de que este profesional goce de los medios y prerrogativas necesarias para el libre ejercicio de su función[10].

Entre las obligaciones de los Abogados figura el de secreto profesional[11] –lo que legitima la intervención del Decano en las diligencias de registro de los despachos profesionales–, de celo y de diligencia en la defensa que le sea encomendada[12]. Asimismo, les asiste el derecho a ejercer la defensa con libertad e independencia y con pleno respeto a su función[13], lo cual implica el reconocimiento de una serie de garantías entre las que figura necesariamente la confidencialidad de las comunicaciones entre Abogado y cliente.

---

[9] STS de 21 de noviembre de 2008.

[10] Vid. JIMÉNEZ CAMPO, "La garantía constitucional del secreto de las comunicaciones", en *Comentarios a la legislación penal,* Madrid, 1986, vid.VII, pág.18.

[11] Art. 5 Código Deontológico de la Abogacía Española –CDAE–.

[12] Art. 32.1 y 42 del RD 658/2001, de 22 de junio, por el que se aprueba el Estatuto General de la Abogacía Española –EGAE–.

[13] Arts. 2 y 3 CDAE y art. 33 EGAE.

1. Reconocimiento y bienes jurídicos protegidos

La Ley de Enjuiciamiento Criminal reconoce a los imputados en una causa criminal, el derecho a mantener comunicaciones y entrevistas reservadas con los Letrados encargados de su defensa. En concreto, el artículo 263 establece que la obligación de presentar denuncia no comprenderá a los Abogados ni a los Procuradores respecto de las instrucciones o explicaciones que recibieron de sus clientes. Asimismo, los artículos 416 y 707 de la LECrim, dispensan al Abogado del deber general de declarar, tanto en el sumario como en el juicio oral, sobre los hechos que el procesado le hubiere confiado en su calidad de defensor. En la misma línea, el art. 542.3 LOPJ dispone que los Abogados deberán guardar secreto de todos los hechos o noticias de que conozcan por razón de cualquiera de las modalidades de su actuación profesional, no pudiendo ser obligados a declarar sobre los mismos[14].

Por su parte, el Tribunal de Justicia de la Unión Europea ha reconocido sin reservas el derecho al secreto de la correspondencia profesional, en especial, aquéllas entre Abogados y sus clientes[15]. También el Tribunal Europeo de Derechos Humanos se ha preocupado de garantizar la confidencialidad de las relaciones profesionales de un Abogado y sus clientes configurándola como una manifestación básica del derecho de defensa[16]. En su sentencia de 2 noviembre 1991 -asunto S contra Suiza-, establece que el derecho del acusado de comunicarse con su Abogado fuera del alcance del oído de un tercero, figura entre las exigencias elementales de un proceso equitativo en una sociedad democrática y deriva del artículo 6.3 c) del Convenio. El acusado tiene, como mínimo, derecho a disponer de las facilidades necesarias para la preparación de su defensa y, a estos efectos, a ser asistido por un abogado de libre elección[17]. Ahora bien, difícilmente puede el inculpado recibir asistencia de su Abogado sin un previo y reservado contacto entre ambos (STEDH de 28 de junio de 1984 -asunto Campbell y Fell-).

La STEDH de 25 de marzo de 1998 -caso Koop-, entiende que la confidencialidad de las relaciones entre un Abogado y sus clientes afecta directamente a los derechos de la defensa y también declara protegidas por el art. 8 del Convenio las llamadas telefónicas al Despacho de Abogados. Este último artículo dispone que toda persona tiene derecho al respeto de su vida privada y familiar, de su domicilio y de su correspondencia. Mas recientemente, la STEDH de 1 de octubre de 2009 -Caso Tsonyo Tsonev contra Bulgaria- recuer-

---

[14] Una disposición idéntica se recoge en el art. 42.1 del Estatuto General de la Abogacía Española.

[15] STJCE de 18 de mayo de 1982.

[16] STEDH 15 de noviembre de 1996 -caso Domenichini- afirma que el derecho a entrevistarse libremente con el abogado constituye una esencial manifestación del derecho de defensa.

[17] Art. 6.3 b) del CEDH.

da que la correspondencia con un Abogado, cualquiera que sea su finalidad, goza de un estatus privilegiado al amparo del artículo 8 del Convenio[18].

La confidencialidad de estas comunicaciones también resulta esencial para garantizar la efectividad real del derecho a no declarar contra sí mismo y a no confesarse culpable, reconocido constitucionalmente (art. 24.2 CE). No cabe duda que el contenido de la conversación mantenida entre el Abogado y su cliente es susceptible de abarcar, incluso, en algunos casos el reconocimiento de su culpa por el imputado o la aportación a su defensor de datos sustanciales sobre la comisión del delito con cuyo conocimiento el letrado puede articular su defensa.

De lo hasta aquí expuesto se deduce que, en el caso de las comunicaciones con el Abogado defensor, como pone de relieve la doctrina[19], junto al secreto formal de las comunicaciones reconocido en el art. 18.3 CE, concurre otro secreto de naturaleza material, el secreto profesional, por lo que no es lícito intervenir el teléfono del Abogado del sospechoso, salvo en los supuestos en los que este profesional deba ser considerado también imputado como autor principal o partícipe. En este caso, ya no se trataría de una relación profesional Abogado-cliente, sino de amparar una actividad delictiva[20].

De esta manera, junto al deber formal de secreto de las comunicaciones coexiste un deber de reserva del contenido material, en razón de lo que efectivamente se comunica dada la especial relación que une a los interlocutores. En congruencia con lo expuesto, la doctrina[21] ha considerado temas prohibidos de investigación las conversaciones entre esposos, familiares, médicos, sacerdotes, abogados etc., ante las cuales, una vez identificado el comunicante, debería interrumpirse la captación y no ser aprehendida.

La legitimidad de la intervención de las comunicaciones del Abogado con su cliente, no debe analizarse desde la exclusiva órbita del art.18.3 de la CE, sino también a la luz del derecho de defensa que reconoce el art. 24 CE y, desde esa perspectiva, ponderar la constitucionalidad de esta medida restrictiva[22].

---

[18] El TEDH ha interpretado la noción de "domicilio" del artículo 8.1 del Convenio en un sentido amplio, de tal manera que abarca no solamente el domicilio privado de una persona, sino también su despacho profesional y, por tanto, un despacho de Abogados (Sentencia Petri Sallinen y otros contra Finlandia de 27 de septiembre de 2005; Sentencia Chappell contra el Reino Unido de 30 marzo 1989; Sentencia Niemietz contra Alemania de 16 diciembre 1992).

[19] RODRÍGUEZ RAMOS, "Las intervenciones telefónicas", en *La prueba en el Proceso Penal,* op.cit., pág. 456.

[20] FERNÁNDEZ ESPINAR, "El levantamiento del secreto de las comunicaciones telefónicas en el marco de las diligencias de investigación y aseguramiento en el proceso penal", Poder Judicial, núm. 32, diciembre, 1993, pág. 27.

[21] ASENCIO MELLADO, *Prueba prohibida y prueba preconstituida,* op. cit., pág. 133.

[22] Vid. LÓPEZ YAGÜES, *La inviolabilidad de las comunicaciones con el Abogado defensor,* Tirant lo blanch, Valencia, 2003, pág. 26.

Así, podríamos distinguir entre comunicaciones generales y especiales, perteneciendo a esta última categoría las que se llevan a cabo entre los imputados y sus Abogados. Si la medida consistente en la intervención de las comunicaciones debe tener siempre un carácter excepcional, en cuanto suspende el ejercicio del derecho fundamental a mantenerlas en secreto, cuando además concurra otro derecho fundamental como el derecho de defensa, parece claro que las garantías que deben rodear la injerencia deben ser extremadas. Se exigiría, por así decirlo, una "súper-excepcionalidad". A juicio del Auto del Tribunal Supremo de 19 octubre 2010, los supuestos en que se autorice la intervención de las comunicaciones de un interno con su letrado han de ser sumamente extraordinarios.

2. La dimensión pública del secreto profesional del abogado

La colaboración y la confianza son los factores fundamentales del eficaz ejercicio de la defensa técnica, de modo tal que, como señala la doctrina[23], en ningún caso se puede hablar de defensa si entre el imputado y el defensor no existe confianza y colaboración. El deber de secreto profesional se funda en la necesidad de salvaguardar la confianza del cliente en el Abogado como única forma de hacer posible que éste disponga de la información necesaria para llevar a cabo su defensa con la eficacia que la Constitución, en el ámbito del proceso, considera nota característica del derecho a la tutela judicial (STS de 17 de febrero de 1998).

El deber de secreto profesional de los letrados adquiere, así, una dimensión pública. No sólo tutela la intimidad de los clientes, sino que constituye un instrumento para salvaguardar la confianza en la profesión de Abogado y, en consecuencia, encarna una garantía del derecho de defensa de todos los ciudadanos[24]. El TEDH consideró una cuestión de interés público el que la persona que desea consultar a un abogado, pueda hacerlo en condiciones propicias para una plena y libre discusión (STEDH 15 de noviembre de 1996 -caso Domenichini-).

Nuestro Tribunal de Defensa de la Competencia, en su resolución de 22 de julio de 2002, destaca también la trascendencia pública del secreto profesional declarando que garantiza la justa y adecuada administración de justicia, de manera que sirve no solo a un interés privado sino que también atañe al interés general que el proceso sea decidido rectamente. Por ello, las comunicaciones con el Abogado deben protegerse frente a cualquier intento de revelación, provenga de quien provenga y cualquiera que sean las circunstancias que se produzcan.

---

[23] MORENO CATENA, *El secreto en la prueba de testigos en el proceso penal,* 1980, pág. 209.
[24] Declaración del Consejo General de la Abogacía sobre el caso *Gürtel.*

En este mismo principio se apoya la doctrina penal[25] para criticar la deficiente cobertura que el Código Penal vigente otorga al secreto profesional del Abogado, que en la actualidad se regula dentro de los delitos contra la intimidad cuando, a la vista del bien jurídico protegido, se aproxima más a los delitos contra la Administración de Justicia regulados en el Título XX de dicho texto legal.

3. Límites

Las consideraciones expuestas determinan que las comunicaciones con el Abogado sólo puedan ser intervenidas en circunstancias muy excepcionales y rodeándose de las mayores garantías.

Señala el Tribunal Constitucional que es competencia del legislador ponderar la proporcionalidad de la exclusión o inclusión y, en su caso, bajo qué requisitos, de círculos determinados de personas en atención a la eventual afectación de otros derechos fundamentales o bienes constitucionales concurrentes al intervenirse sus comunicaciones, o las de otros con quienes se comunica, citando el caso de los Abogados o profesionales de la información, Diputados o Senadores (STC 184/2003).

Dada la incuestionable gravedad que supone de la injerencia en las comunicaciones con el Abogado, ésta tiene que ponderarse cuidadosamente por el legislador y por el órgano jurisdiccional que la acuerda y, únicamente puede fundarse en la necesidad de tutelar otros intereses fundamentales de orden público prevalentes.

Estos intereses no pueden consistir en la genérica obligación de perseguir la comisión de un delito y de obtener datos relevantes en la investigación de los mismos. Probablemente, el Abogado conocerá la verdad de lo acontecido y en transcurso de sus comunicaciones con la persona a la que defiende ésta le revelará datos de interés para el éxito de la investigación. Ahora bien, hoy es un principio comúnmente admitido que la verdad no puede alcanzarse a cualquier precio [26] . El proceso penal se funda en los principios recogidos en la Constitución, la cual reconoce, entre otros, el derecho a la prueba obtenida y practicada de acuerdo con las normas de garantía legalmente establecidas[27].

Conviene recordar que el Tribunal Constitucional en su sentencia 114/1984 proclamó, por primera vez, la prohibición de utilizar pruebas cuando en el momento de su obtención se hubieran infringido los mencionados derechos.

---

[25] CORTÉS BECHIARELLI, "Secreto profesional del abogado y ejercicio del derecho de defensa a la luz de la Directiva 2001/97/CE del Parlamento Europeo y del Consejo", *Anuario de la Facultad de Derecho*, vol. XXI, 2003.

[26] Así lo declaró el Tribunal Supremo Federal alemán en su Sentencia de 14 de junio de 1960, BGHSt, 14, 358, 365.

[27] Vid. SSTC 49/1999, 141/2.001, 167/2.002.

Así, recogiendo el sentir de una parte de la doctrina, se apartó del criterio que había mantenido la jurisprudencia anterior, según la cual en el proceso penal debía prevalecer el interés público en la búsqueda de la verdad.

Por imperativo constitucional, el derecho a un proceso con todas las garantías y a la presunción de inocencia, es el marco dentro del cual pueden realizarse los fines de averiguación de la verdad en el proceso penal.

El acceso por parte del órgano jurisdiccional a las conversaciones con el Abogado, puede permitir a éste conocer las estrategias de defensa del imputado[28], lo que afecta a uno de los principios básicos de la estructura del proceso: el de igualdad de las partes. Asimismo, queda en cuestión la posición "supra partes" que debe ostentar el Juez dentro del proceso y, por tanto, en última instancia, su independencia o imparcialidad. Sea suficiente recordar que la independencia judicial constituye una nota esencial de la Jurisdicción sin la cual no podrían los Juzgados y Tribunales aplicar correctamente el Derecho a los casos concretos, ya que la Ley, en tanto que manifestación de la voluntad general, precisa que la actividad judicial de individualización normativa no pueda efectuarse tomando en consideración situaciones hegemónicas de las partes o privilegio material alguno[29].

Por tanto, la intervención de las comunicaciones con el Abogado debe limitarse a aquellos supuestos en los que existe una constancia, suficientemente contrastada, de que el Abogado ha podido extralimitarse en sus obligaciones y responsabilidades profesionales integrándose en la actividad delictiva como uno de sus elementos componentes (STS de 28 de noviembre de 2001). Cuando haya razones objetivas para pensar que los Abogados defensores pueden contribuir a ocultar pruebas o a colaborar en la comisión de delitos, el derecho de defensa se estaría utilizando como cauce abusivo para actividades que exceden de la finalidad de esta garantía procesal.

En este caso, la participación directa e indiciaria que en la investigación se le atribuya es totalmente ajena a su condición de Letrado, la cual no puede servir en ningún caso de amparo, protección o favorecimiento de la comisión de delitos (ATS de 24 de enero de 2003*).* El Abogado ya no actúa como defensor, sino como un mero partícipe en el delito. Por tanto, no se trata de la defensa de un imputado en prisión, sino de la presunta actividad delictiva del Abogado no amparada por el derecho de defensa.

La STEDH de 25 de marzo de 1998 (caso KOPP), reconoce como única excepción al secreto de las comunicaciones telefónicas con el Abogado la existencia de razones bastantes para considerar como sospechoso de participación en la actividad delictiva al propio defensor. Por su parte, la STEDH de 1 de octubre de 2009, declara que la lectura de la correspondencia de un interno

---

[28] Así lo subraya la STEDH de 28 de junio de 1985 -caso *Campbell y Fell contra el Reino Unido*-.
[29] Cfr. GIMENO SENDRA, *Introducción al Derecho Procesal,* Colex, Madrid, 2010.

con su Letrado, sólo puede autorizarse en casos excepcionales, si las autoridades tienen razones para creer que existe un abuso de privilegio por cuanto el contenido de la carta amenaza la seguridad del establecimiento o a terceros o reviste un carácter delictivo.

Por tanto, como afirma Velasco Núñez[30], existen secretos funcionalmente inviolables que han de quedar excluidos de toda injerencia, incluso judicial, a no ser que el Letrado reúna al propio tiempo la condición de sospechoso de participación en un hecho delictivo.

En este caso, debe dictarse por el órgano jurisdiccional una resolución que autorice expresamente la intervención de las comunicaciones de dicho Abogado como sujeto pasivo de la medida misma. Ésta es la manera de comprobar la existencia de un efectivo control judicial donde concurra el necesario juicio de excepcionalidad y de proporcionalidad, en los términos exigidos por Constitución Española, que permita verificar la legalidad de las intervenciones practicadas. Cuando en el marco de una investigación criminal, se conozcan nuevos hechos delictivos o nuevos sujetos implicados diferentes de los originariamente investigados y que, por tanto, no están comprendidos en el ámbito de la autorización judicial inicial, resulta obligado recabar la pertinente solicitud de la autoridad judicial, sin cuya autorización no podrá el Tribunal extender su conocimiento a las conversaciones de tales sujetos o a los nuevos hechos. Se debe dictar una autorización judicial expresa de ampliación subjetiva del objeto de la investigación[31]. Un Abogado sospechoso de un delito grave no puede ser tratado de manera diferente a los otros sospechosos.

4. Excepciones: la proporcionalidad y legalidad de la excepción

Si bien es cierto que los derechos a no padecer indefensión y a ser defendido por un Abogado pueden ceder ante la necesidad de preservar otros derechos o bienes constitucionalmente protegidos, resulta necesario determinar si la medida restrictiva de estos derechos fundamentales supera las exigencias del juicio de proporcionalidad. Para ello, debe comprobarse si dicha medida contribuye a conseguir el objetivo propuesto (juicio de idoneidad); si además es necesaria, en el sentido de que no exista otra medida más moderada para la consecución del tal propósito (juicio de necesidad); y, finalmente, si la misma es ponderada o equilibrada, por derivarse de ella más ventajas o beneficios para el interés general que perjuicios sobre otros bienes o valores en conflicto, lo que constituye el juicio de proporcionalidad en sentido estricto (STC 198/2003).

---

[30] VELASCO NÚÑEZ, "Presencias y ausencias -aspectos aclarados y discutidos- en materia de intervenciones telefónicas, en espera de una regulación parlamentaria del tema", en *Actualidad Penal*, núm. 18, mayo de 1993.

[31] Vid. STS de 18 de julio de 2000.

Nuestro legislador sólo ha previsto expresamente la intervención de las comunicaciones entre el Abogado y el cliente en el caso del delito de terrorismo. Ello no obstante, se ha suscitado un amplio debate sobre la interpretación que deba darse al art. 51 de la Ley Orgánica 1/1979 General Penitenciaria (en adelante LOGP) que regula las comunicaciones con el exterior de quienes se encuentran internados en establecimientos penitenciarios. El párrafo segundo de dicho precepto dispone que "las comunicaciones de los internos con el Abogado defensor o con el Abogado expresamente llamado en relación con asuntos penales y con los Procuradores que los representen, se celebrarán en departamentos apropiados y no podrán ser suspendidas o intervenidas salvo orden de la autoridad judicial y en los supuestos de terrorismo".

Según la interpretación que realiza el Auto del Tribunal Superior de Justicia de Madrid 28/2010 de 25 marzo (que resuelve la escuchas del caso *gürtel*) cuando se trate de personas privadas de libertad, constreñidas por tanto a realizar las imprescindibles comunicaciones con su Letrado en un entorno controlado por la Administración Pública, el legislador dispuso que sólo podrían intervenirse estas comunicaciones, necesarias para el ejercicio efectivo del derecho de defensa, cuando concurrieran dos condiciones conjuntamente: que se tratara de presos o penados por delitos de terrorismo y que esa restricción fuera ponderada adecuadamente en una resolución judicial. Entiende que el legislador fue consciente de que dejar abierta la posibilidad de restricción de esas comunicaciones en cualquier clase de delito podría dar a traste con el derecho de defensa. Por eso, sólo la autorizó en casos de terrorismo que constituyen un ataque máximo a la convivencia social y, aun en estos casos, se condicionó dicha medida restrictiva a que una autoridad judicial evaluara su conveniencia, utilidad y proporcionalidad, al objeto de preservar los derechos individuales de los penados, imputados o acusados, aunque lo fueran por terrorismo.

Nuestro máximo garante de la Constitución también se ha pronunciado sobre el alcance del art. 51 de la LOGP (aunque referido a un supuesto distinto), declarando que los dos requisitos que recoge deben concurrir de forma acumulativa y no como requisitos alternativos. La STC 183/1994, al analizar este precepto, distingue entre las comunicaciones, que califica de generales, entre el interno con determinada clase de personas -art. 51.1 - y las comunicaciones específicas, que aquél tenga con su Abogado defensor o con el Abogado expresamente llamado en relación con asuntos penales (art. 51.2). La primera clase de comunicaciones viene sometida al régimen general del art. 51.5, que autoriza al Director del Centro a suspenderlas o intervenirlas "por razones de seguridad, de interés del tratamiento y del buen orden del establecimiento", según precisa el art. 51.1, mientras que las segundas son sometidas al régimen especial del art. 51.2, cuya justificación es necesario encontrar en las exigencias y necesidades de la instrucción penal, a las cuales es totalmente ajena la Administración Penitenciaria que no tiene posibilidad alguna

de ponderar circunstancias procesales que se producen al margen del ámbito penitenciario. Culmina el razonamiento esta sentencia diciendo que esta diferenciación esencial que existe entre el art. 51.5 -régimen general cuya única remisión válida es al art. 51.1- y el art. 51.2, pone de manifiesto la imposibilidad constitucional de interpretar este último precepto en el sentido de considerar alternativas las dos condiciones de "orden de la autoridad judicial" y "supuestos de terrorismo", que en el mismo se contienen, así como derivar de ello la legitimidad constitucional de una intervención administrativa que es totalmente incompatible con el más intenso grado de protección que la norma legal confiere al derecho de defensa en los procesos penales. Dichas condiciones habilitantes deben, por tanto, considerarse acumulativas. Esta doctrina se reitera en la STC 58/1998.

Ahora bien, una parte de la doctrina [32] ha entendido que el carácter acumulativo de las condiciones habilitantes del art.51.2 LOGP defendido por la referida jurisprudencia del Tribunal Constitucional no implica que los dos requisitos deban concurrir en todo caso, sino que lo que este Tribunal pretendía destacar en los supuestos concretos analizados es que aún en los casos de terrorismo, resulta necesaria también la orden judicial, siendo precisamente en este punto en lo que las SSTC 183/1994 y 58/1998 corrigieron la doctrina primeramente establecida en la STC 73/1983. Por ello, concluye este sector doctrinal que los fundamentos del Tribunal Constitucional al interpretar el mencionado artículo no iban encaminados a limitar la posibilidad de que la autoridad judicial acuerde la intervención de las comunicaciones de un interno con su Abogado, sino a impedir que pudiera hacerlo la administración penitenciaria.

Sin embargo, la sentencia del Tribunal Supremo 538/1997 de 23 de abril llega a conclusiones diferentes. Entiende que las razones de seguridad, de interés del tratamiento y del buen orden del establecimiento, que pueden justificar estas limitaciones, no son aplicables a las comunicaciones incardinadas en el ejercicio del derecho de defensa del interno (art. 24 CE), derecho que no se ve legalmente limitado por su privación de libertad, y que debe ser especialmente tutelado, garantizando la igualdad real y efectiva de posibilidades de defensa de los acusados en un proceso penal, tanto a quienes la ejercitan desde la libertad como a quienes tienen que ejercitarla desde la prisión (art. 9.2 de la Constitución Española). Más adelante añade que la regla general debe ser la de garantizar, en todo caso, la confidencialidad de las comunicaciones de los internos enmarcadas dentro del ejercicio de su derecho de defensa en un procedimiento penal, sin posibilidad de intervención ni administrativa ni judicial. Ello no obstante, la máxima tutela de los derechos individuales en un Estado de Derecho Social y Democrático no es incompatible con la admisión

[32] JIMÉNEZ VILLAREJO, "Intervención de comunicaciones entre internos y sus letrados", en *El Cronista*, Iustel, núm. 14, junio, 2010, págs. 70 y 71.

de reacciones proporcionadas frente a la constatada posibilidad de abusos en supuestos muy específicos y excepcionales. Concretamente, en el ámbito de las actividades de delincuencia organizada en grupos permanentes y estables, de carácter armado, cuya finalidad o efecto es producir el terror en la colectividad, se ha constatado la utilización de las garantías que el sistema democrático proporciona al derecho de defensa como cauce abusivo para actividades que exceden de la finalidad de defensa e inciden en la colaboración con las actividades terroristas. Es por ello por lo que, excepcionalmente y sin que dicha excepción pueda contagiarse al resto del sistema, en el ámbito personal exclusivo de los supuestos de terrorismo, y en todo caso con la especial garantía de la orden judicial previa, naturalmente ponderadora de la necesidad, proporcionalidad y razonabilidad de la medida en cada caso concreto, el art. 51.2 LOGP faculta para la intervención de este tipo de comunicaciones singulares.

De conformidad con lo expuesto, el terrorismo constituye una excepción al principio de confidencialidad de las comunicaciones personales con el Abogado siempre que concurra la correspondiente autorización judicial previa donde se pondere la necesidad, proporcionalidad y razonabilidad de la medida restrictiva en cada caso concreto (STS 23 de abril 1997). Pero no sólo constituye una excepción sino la única excepción prevista en nuestro Derecho positivo vigente. Nuestra LECrim no establece ninguna otra excepción expresa al respecto.

Ahora bien, si se considera que el terrorismo no es el único delito del que debe defenderse la sociedad con medios extraordinarios es al legislador al que le corresponde prever las demás excepciones pues tal y como se indicó mas arriba, la actuación del Juez se refiere al caso concreto, lo que implica la necesidad de que, con carácter previo, el poder legislativo haya establecido, en abstracto, la procedencia de la intervención de acuerdo con el principio de legalidad que inspira la actuación jurisdiccional. No podemos olvidar que el principio de proporcionalidad debe inspirar tanto la actuación del legislador al prever la posible limitación en abstracto, como la actuación del Juez en el caso concreto.

Por mandato expreso de la Constitución, toda injerencia estatal en el ámbito de los derechos fundamentales y las libertades públicas que incida directamente sobre su desarrollo o limite o condicione su ejercicio, precisa una habilitación legal (STC 49/1999). Por ello, es competencia del legislador autorizar a los órganos jurisdiccionales para poder disponer de tales medios de investigación. La Constitución Española exige una triple condición sobre la previsión legal de las medidas limitativas de los derechos fundamentales. En primer lugar, la existencia de una disposición jurídica que habilite a la autoridad judicial para la imposición de la medida en el caso concreto. En segundo lugar, el rango legal que ha de tener dicha disposición. Finalmente, la calidad de la Ley como garantía de seguridad (STC 169/2001).

De esta manera, no sólo se exige que la injerencia estatal en dicho secreto esté presidida por el principio de legalidad, sino que se especifica que el respeto

a dicho principio requiere, en este caso, "una ley de singular precisión"[33] . Según el Tribunal Europeo de Derechos Humanos entre las exigencias integrantes de la "calidad de la Ley" se encuentran la accesibilidad y la previsibilidad. El Derecho interno debe usar términos suficientemente claros para indicar en qué circunstancias y bajo qué condiciones se habilita a los poderes públicos a autorizar medidas consistentes en la interceptación de las comunicaciones. En la Sentencia de 30 de julio de 1998 -caso *Valenzuela Contreras c. España*-, el Tribunal de Estrasburgo hizo una enumeración minuciosa de los requisitos imprescindibles que deben figurar en la Ley, extrayéndolos directamente de casos significativos. Así, como garantías mínimas, las Sentencias Kruslin y Huvig, de 24 y 26 de Abril de 1990, mencionaron, entre otras, la definición de las categorías de personas susceptibles de interceptación judicial. La célebre STC 49/1999, también enumeró de forma concreta cada una de las exigencias derivadas de nuestra Constitución[34].

Por ello, el art. 579 LECrim no puede considerase un marco legal suficiente que habilite la intervención de este tipo especial de comunicaciones, pues como nuestro Tribunal Constitucional ha declarado, de forma reiterada, adolece de vaguedad e indeterminación en estos aspectos esenciales (SSTC 26/2006, 184/2000). De hecho, ningún autor que haya abordado el estudio de esta medida restrictiva ha dejado de denunciar la falta de concreción e inseguridad de nuestra normativa vigente[35], calificándola de norma en blanco.

Resulta urgente una regulación específica y detallada de la intervención de las comunicaciones electrónicas que, garantizando los derechos constitucionales, y sobre todo la intimidad y el derecho de defensa, proporcione unas pautas legales a las que deba ajustarse esta diligencia, fuera de las escasas disposiciones que establece el mencionado art. 579 de la Ley de Enjuiciamiento Criminal[36].

---

[33] SSTC 49/1999, 123/1997, 54/1996, 49/1996, 85/1994.

[34] La STC 49/1999 se refirió a la necesidad de definir en la Ley "las categorías de personas susceptibles de ser sometidas a escucha judicial; la naturaleza de las infracciones susceptibles de poder dar lugar a ella; la fijación de un límite a la duración de la ejecución de la medida; el procedimiento de trascripción de las conversaciones interceptadas; las precauciones a observar, para comunicar, intactas y completas, las grabaciones realizadas a los fines de control eventual por el Juez y por la defensa; las circunstancias en las cuales puede o debe procederse a borrar o destruir las cintas, especialmente en caso de sobreseimiento o puesta en libertad".

[35] Vid. DÍAZ CABIALE, *La admisión y práctica de la prueba en el proceso penal,* Consejo General del Poder Judicial, 1991.

[36] STC 34/2003 de 22 de enero.

UNIDAD II: CONOCIMIENTOS LEGALES

1.- Convenio sobre la Cibercriminalidad de Budapest.

COUNCIL OF EUROPE CONSEIL DE L'EUROPE

Serie de Tratados Europeos- nº185

CONVENIO
SOBRE LA CIBERDELINCUENCIA

Budapest, 23.XI.2001

Preámbulo

Los Estados miembros del Consejo de Europa y los demás Estados signatarios del presente Convenio,

Considerando que el objetivo del Consejo de Europa es lograr una unión más estrecha entre sus miembros;

Reconociendo el interés de intensificar la cooperación con los otros Estados Partes en el presente Convenio;

Convencidos de la necesidad de aplicar, con carácter prioritario, una política penal común con objeto de proteger a la sociedad frente a la ciberdelincuencia, en particular mediante la adopción de una legislación adecuada y la mejora de la cooperación internacional;

Conscientes de los profundos cambios provocados por la digitalización, la convergencia y la globalización continuas de las redes informáticas;

Preocupados por el riesgo de que las redes informáticas y la información electrónica sean utilizadas igualmente para cometer delitos y de que las pruebas relativas a dichos delitos sean almacenadas y transmitidas por medio de dichas redes;

Reconociendo la necesidad de cooperación entre los Estados y el sector privado en la lucha contra la ciberdelincuencia, así como la necesidad de proteger los intereses legítimos en la utilización y el desarrollo de las tecnologías de la información;

Estimando que la lucha efectiva contra la ciberdelincuencia requiere una cooperación internacional reforzada, rápida y eficaz en materia penal;

Convencidos de que el presente Convenio es necesario para prevenir los actos que pongan en peligro la confidencialidad, la integridad y la disponibilidad de los sistemas, redes y datos informáticos, así como el abuso de dichos sistemas, redes y datos, garantizando la tipificación como delito de dichos actos, tal como se definen en el presente Convenio, y la asunción de poderes suficientes para luchar eficazmente contra dichos delitos, facilitando su detección, investigación y sanción, tanto a nivel nacional como internacional, y estableciendo disposiciones materiales que permitan una cooperación internacional rápida y fiable;

Teniendo presente la necesidad de garantizar el debido equilibrio entre los intereses de la acción penal y el respeto de los derechos humanos fundamentales consagrados en el Convenio del Consejo de Europa para la Protección de los Derechos Humanos y de las Libertades Fundamentales (1950), el Pacto Internacional de Derechos Civiles y Políticos de las Naciones Unidas (1966) y otros tratados internacionales aplicables en materia de derechos humanos, que reafirman el derecho a defender la propia opinión sin interferencia, el derecho a la libertad de expresión, incluida la libertad de buscar, obtener y comunicar información e ideas de toda índole, sin consideración de fronteras, así como el respeto de la vida privada;

Conscientes igualmente del derecho a la protección de los datos personales, tal como se define, por ejemplo, en el Convenio de 1981 del Consejo de Europa para la protección de las personas con respecto al tratamiento informatizado de datos personales;

Teniendo presentes la Convención sobre los Derechos del Niño de las Naciones Unidas (1989) y el Convenio sobre las peores formas de trabajo infantil de la Organización Internacional del Trabajo (1999);

Teniendo en cuenta los convenios existentes del Consejo de Europa sobre cooperación en materia penal, así como otros tratados similares celebrados entre los Estados miembros del Consejo de Europa y otros Estados, y subrayando que el objeto del presente Convenio es completar dichos Convenios con el fin de incrementar la eficacia de las investigaciones y procedimientos penales relativos a los delitos relacionados con sistemas y datos informáticos, así como permitir la obtención de pruebas electrónicas de los delitos;

Congratulándose de las recientes iniciativas destinadas a mejorar el entendimiento y la cooperación internacionales en la lucha contra la delincuencia cibernética, y en particular las acciones organizadas por las Naciones Unidas, la OCDE, la Unión Europea y el G8;

Recordando las Recomendaciones del Comité de Ministros nº R (85) 10 relativa a la aplicación práctica del Convenio Europeo de Asistencia Judicial en Materia Penal en relación con las comisiones rogatorias para la vigilancia de las telecomunicaciones, nº R (88) 2 sobre medidas encaminadas a luchar contra la piratería en materia de propiedad intelectual y derechos afines, nº R (87) 15 relativa a la regulación de la utilización de datos de personales por la policía, nº R (95) 4 sobre la protección de los datos personales en el ámbito de los servicios de telecomunicaciones, con especial referencia a los servicios telefónicos, nº R (89) 9 sobre la delincuencia relacionada con la informática, que ofrece a los legisladores nacionales directrices para definir ciertos delitos informáticos, y nº R (95) 13 relativa a los problemas de procedimiento penal vinculados a la tecnología de la información;

Teniendo presente la Resolución nº 1, adoptada por los Ministros de Justicia europeos, en su XXI Conferencia (Praga, 10 y 11 de junio de 1997), que recomendaba al Comité de Ministros apoyar las actividades en relación con la ciberdelincuencia organizadas por el Comité Europeo para Problemas Criminales (CDPC) con el fin de aproximar las legislaciones penales nacionales y permitir la utilización de medios de investigación eficaces en materia de delitos informáticos, así como la Resolución nº 3, adoptada en la XXIII Conferencia de Ministros de Justicia europeos (Londres, 8 y 9 de junio de 2000), que exhortaba a las partes negociadoras a persistir en sus esfuerzos por encontrar soluciones que permitan al mayor número posible de Estados ser partes en el Convenio, y reconocía la necesidad de disponer de un mecanismo rápido y eficaz de cooperación internacional que tenga debidamente en cuenta las exigencias específicas de la lucha contra la ciberdelincuencia;

Teniendo asimismo en cuenta el plan de acción adoptado por los Jefes de Estado y de Gobierno del Consejo de Europa, con ocasión de su segunda Cumbre (Estrasburgo, 10 y 11 de octubre de 1997) con objeto de encontrar respuestas comunes ante el desarrollo de las nuevas tecnologías de la información, basadas en las normas y los valores del Consejo de Europa,

Han convenido en lo siguiente:

Capítulo I – Terminología

Artículo 1 – Definiciones

A los efectos del presente Convenio:

a. por "sistema informático" se entenderá todo dispositivo aislado o conjunto de dispositivos interconectados o relacionados entre sí, cuya función, o la de alguno de sus elementos, sea el tratamiento automatizado de datos en ejecución de un programa;
b. por "datos informáticos" se entenderá toda representación de hechos, información o conceptos expresados de cualquier forma que se preste a tratamiento informático, incluidos los programas diseñados para que un sistema informático ejecute una función;
c. por "proveedor de servicios" se entenderá:

    i. toda entidad pública o privada que ofrezca a los usuarios de sus servicios la posibilidad de comunicar a través de un sistema informático, y
    ii. cualquier otra entidad que procese o almacene datos informáticos para dicho servicio de comunicación o para los usuarios del mismo;

d. por "datos relativos al tráfico" se entenderá todos los datos relativos a una comunicación realizada por medio de un sistema informático, generados por este último en tanto que elemento de la cadena de comunicación, y que indiquen el origen, el destino, la ruta, la hora, la fecha, el tamaño y la duración de la comunicación o el tipo de servicio subyacente.

Capítulo II – Medidas que deberán adoptarse a nivel nacional

Sección 1 – Derecho penal sustantivo

Título 1 – Delitos contra la confidencialidad, la integridad y la disponibilidad de los datos y sistemas informáticos

Artículo 2 – Acceso ilícito

Cada Parte adoptará las medidas legislativas y de otro tipo que resulten necesarias para tipificar como delito en su derecho interno el acceso deliberado e ilegítimo a todo o parte de un sistema informático. Las Partes podrán exigir que el delito se cometa infringiendo medidas de seguridad, con la intención de obtener datos informáticos u otra intención delictiva, o en relación con un sistema informático conectado a otro sistema informático.

Artículo 3 – Interceptación ilícita

Cada Parte adoptará las medidas legislativas y de otro tipo que resulten necesarias para tipificar como delito en su derecho interno la interceptación deliberada e ilegítima por medios técnicos de datos informáticos en transmisiones no públicas dirigidas a un sistema informático, originadas en un sistema informático o efectuadas dentro del

mismo, incluidas las emisiones electromagnéticas provenientes de un sistema informático que transporte dichos datos informáticos. Las Partes podrán exigir que el delito se cometa con intención delictiva o en relación con un sistema informático conectado a otro sistema informático.

Artículo 4 – Ataques a la integridad de los datos

1. Cada Parte adoptará las medidas legislativas y de otro tipo que resulten necesarias para tipificar como delito en su derecho interno todo acto deliberado e ilegítimo que dañe, borre, deteriore, altere o suprima datos informáticos.

2. Las Partes podrán reservarse el derecho a exigir que los actos definidos en el párrafo 1 comporten daños graves.

Artículo 5 – Ataques a la integridad del sistema

Cada Parte adoptará las medidas legislativas y de otro tipo que resulten necesarias para tipificar como delito en su derecho interno la obstaculización grave, deliberada e ilegítima del funcionamiento de un sistema informático mediante la introducción, transmisión, daño, borrado, deterioro, alteración o supresión de datos informáticos.

Artículo 6 – Abuso de los dispositivos

1. Cada Parte adoptará las medidas legislativas y de otro tipo que resulten necesarias para tipificar como delito en su derecho interno la comisión deliberada e ilegítima de los siguientes actos:

a. la producción, venta, obtención para su utilización, importación, difusión u otra forma de puesta a disposición de:
    i. cualquier dispositivo, incluido un programa informático, concebido o adaptado principalmente para la comisión de cualquiera de los delitos previstos en los artículos 2 a 5 del presente Convenio;
    ii. una contraseña, código de acceso o datos informáticos similares que permitan acceder a todo o parte de un sistema informático,

    con intención de que sean utilizados para cometer cualquiera de los delitos contemplados en los artículos 2 a 5; y

b. la posesión de alguno de los elementos contemplados en los incisos i) o ii) del apartado a) del presente artículo con intención de que sean utilizados para cometer cualquiera de los delitos previstos en los artículos 2 a 5. Las Partes podrán exigir en su derecho interno la posesión de un número determinado de dichos elementos para que se considere que existe responsabilidad penal.

2. No se interpretará que el presente artículo impone responsabilidad penal cuando la producción, venta, obtención para la utilización, importación, difusión o cualquier otra forma de puesta a disposición mencionada en el párrafo 1 del presente artículo no tenga por objeto la comisión de uno de los delitos previstos de conformidad con los artículos 2 a 5 del presente Convenio, como en el caso de las pruebas autorizadas o de la protección de un sistema informático.

3. Las Partes podrán reservarse el derecho a no aplicar el párrafo 1 del presente artículo, siempre que dicha reserva no afecte a la venta, distribución o cualesquiera otras formas de puesta a disposición de los elementos mencionados en el inciso 1 a) ii) del presente artículo.

Título 2 – delitos informáticos

Artículo 7 – Falsificación informática

Cada Parte adoptará las medidas legislativas y de otro tipo que resulten necesarias para tipificar como delito en su derecho interno la introducción, alteración, borrado o supresión deliberados e ilegítimos de datos informáticos que genere datos no auténticos con la intención de que sean tomados o utilizados a efectos legales como auténticos, con independencia de que los datos sean legibles e inteligibles directamente. Las Partes podrán exigir que exista una intención dolosa o delictiva similar para que se considere que existe responsabilidad penal.

Artículo 8 – Fraude informático

Las Partes adoptarán las medidas legislativas o de otro tipo que resulten necesarias para tipificar como delito en su derecho interno los actos deliberados e ilegítimos que causen perjuicio patrimonial a otra persona mediante:

a. la introducción, alteración, borrado o supresión de datos informáticos;
b. cualquier interferencia en el funcionamiento de un sistema informático,

con la intención, dolosa o delictiva, de obtener de forma ilegítima un beneficio económico para uno mismo o para otra persona.

Título 3 – Delitos relacionados con el contenido

Artículo 9 – Delitos relacionados con la pornografía infantil

1. Cada Parte adoptará las medidas legislativas y de otro tipo que resulten necesarias para tipificar como delito en su derecho interno la comisión deliberada e ilegítima de los siguientes actos:

   a. la producción de pornografía infantil con la intención de difundirla a través de un sistema informático;
   b. la oferta o la puesta a disposición de pornografía infantil a través de un sistema informático;
   c. la difusión o la transmisión de pornografía infantil a través de un sistema informático;
   d. la adquisición, para uno mismo o para otros, de pornografía infantil a través de un sistema informático;
   e. la posesión de pornografía infantil en un sistema informático o en un dispositivo de almacenamiento de datos informáticos.

2. A los efectos del párrafo 1 anterior, se entenderá por «pornografía infantil» todo material pornográfico que contenga la representación visual de:

a. un menor adoptando un comportamiento sexualmente explícito;
b. una persona que parezca un menor adoptando un comportamiento sexualmente explícito;
c. imágenes realistas que representen a un menor adoptando un comportamiento sexualmente explícito.

3. A los efectos del párrafo 2 anterior, se entenderá por «menor» toda persona menor de 18 años. Las Partes podrán, no obstante, exigir un límite de edad inferior, que deberá ser como mínimo de 16 años.

4. Las Partes podrán reservarse el derecho a no aplicar, en todo o en parte, los apartados d) y e) del párrafo 1 y los apartados b) y c) del párrafo 2.

Título 4 – Delitos relacionados con infracciones de la propiedad intelectual y de los derechos afines

Artículo 10 – Delitos relacionados con infracciones de la propiedad intelectual y de los derechos afines

1. Cada Parte adoptará las medidas legislativas y de otro tipo que resulten necesarias para tipificar como delito en su derecho interno las infracciones de la propiedad intelectual que defina su legislación, de conformidad con las obligaciones que haya contraído en aplicación del Acta de París de 24 de julio de 1971, por la cual se revisó el Convenio de Berna para la protección de las obras literarias y artísticas, del Acuerdo sobre los aspectos de los derechos de propiedad intelectual relacionados con el comercio y del Tratado de la OMPI sobre Derecho de Autor, a excepción de cualquier derecho moral otorgado por dichos Convenios, cuando tales actos se cometan deliberadamente, a escala comercial y por medio de un sistema informático.

2. Cada Parte adoptará las medidas legislativas y de otro tipo que resulten necesarias para tipificar como delito en su derecho interno las infracciones de los derechos afines definidas en su legislación, de conformidad con las obligaciones que haya asumido en aplicación de la Convención Internacional sobre la Protección de los Artistas Intérpretes o Ejecutantes, los Productores de Fonogramas y los Organismos de Radiodifusión (Convención de Roma), del Acuerdo sobre los aspectos de los derechos de propiedad intelectual relacionados con el comercio y del Tratado de la OMPI sobre Interpretación o Ejecución y Fonogramas, a excepción de cualquier derecho moral conferido por dichos Convenios, cuando tales actos se cometan deliberadamente, a escala comercial y por medio de un sistema informático.

3. En circunstancias bien delimitadas, toda Parte podrá reservarse el derecho de no imponer responsabilidad penal en virtud de los párrafos 1 y 2 del presente artículo, siempre que se disponga de otros recursos efectivos y que dicha reserva no vulnere las obligaciones internacionales que incumban a dicha Parte en aplicación de los instrumentos internacionales mencionados en los párrafos 1 y 2 del presente artículo.

Título 5 – Otras formas de responsabilidad y de sanción

Artículo 11 – Tentativa y complicidad

1. Cada Parte adoptará las medidas legislativas y de otro tipo que resulten necesarias para tipificar como delito en su derecho interno cualquier complicidad deliberada con vistas a la comisión de alguno de los delitos previstos en aplicación de los artículos 2 a 10 del presente Convenio, con la intención de que dicho delito sea cometido.

2. Cada Parte adoptará las medidas legislativas y de otro tipo que resulten necesarias para tipificar como delito en su derecho interno toda tentativa deliberada de cometer alguno de los delitos previstos en aplicación de los artículos 3 a 5, 7, 8, 9.1.a) y 9.1.c) del presente Convenio.

3. Las Partes podrán reservarse el derecho a no aplicar, en todo o en parte, el párrafo 2 del presente artículo.

Artículo 12 – Responsabilidad de las personas jurídicas

1. Cada Parte adoptará las medidas legislativas y de otro tipo que resulten necesarias para que pueda exigirse responsabilidad a las personas jurídicas por los delitos previstos en aplicación del presente Convenio, cuando éstos sean cometidos por cuenta de las mismas por una persona física, ya sea a título individual o como miembro de un órgano de dicha persona jurídica, que ejerza funciones directivas en su seno, en virtud de:

a. un poder de representación de la persona jurídica;
b. una autorización para tomar decisiones en nombre de la persona jurídica;
c. una autorización para ejercer funciones de control en el seno de la persona jurídica.

2. Además de los casos previstos en el párrafo 1 del presente artículo, Cada Parte adoptará las medidas necesarias para garantizar que pueda exigirse responsabilidad a una persona jurídica cuando la ausencia de vigilancia o de control por parte de cualquier persona física mencionada en el párrafo 1 haya permitido la comisión de un delito previsto en aplicación del presente Convenio por una persona física que actúe por cuenta de dicha persona jurídica y bajo su autoridad.

3. Dependiendo de los principios jurídicos de cada Parte, la responsabilidad de una persona jurídica podrá ser penal, civil o administrativa.

4. Dicha responsabilidad se entenderá sin perjuicio de la responsabilidad penal de las personas físicas que hayan cometido el delito.

Artículo 13 – Sanciones y medidas

1. Cada Parte adoptará las medidas legislativas y de otro tipo que resulten necesarias para que los delitos previstos en aplicación de los artículos 2 a 11 estén sujetos a sanciones efectivas, proporcionadas y disuasorias, incluidas penas privativas de libertad.

2. Las Partes garantizarán la imposición de sanciones o medidas penales o no penales efectivas, proporcionadas y disuasorias, incluidas sanciones pecuniarias, a las personas jurídicas consideradas responsables de conformidad con el artículo 12.

Sección 2 – Derecho procesal

Título 1 – Disposiciones comunes

Artículo 14 – Ámbito de aplicación de las disposiciones de procedimiento

1. Cada Parte adoptará las medidas legislativas y de otro tipo que resulten necesarias para establecer los poderes y procedimientos previstos en la presente Sección a los efectos de investigación o de procedimientos penales específicos.

2. Salvo que se establezca lo contrario en el artículo 21, cada Parte aplicará los poderes y procedimientos mencionados en el párrafo 1 del presente artículo:

a. a los delitos previstos en aplicación de los artículos 2 a 11 del presente Convenio;
b. a cualquier otro delito cometido por medio de un sistema informático; y
c. a la obtención de pruebas electrónicas de cualquier delito.

3. a. Las Partes podrán reservarse el derecho a aplicar las medidas mencionadas en el artículo 20 únicamente a los delitos o categorías de delitos especificados en su reserva, siempre que el repertorio de dichos delitos o categorías de delitos no sea más reducido que el de los delitos a los que dicha Parte aplique las medidas mencionadas en el artículo 21. Las Partes tratarán de limitar tal reserva de modo que sea posible la más amplia aplicación de la medida mencionada en el artículo 20.

b. Cuando, a causa de las restricciones que imponga su legislación vigente en el momento de la adopción del presente Convenio, una Parte no pueda aplicar las medidas previstas en los artículos 20 y 21 a las comunicaciones transmitidas dentro de un sistema informático de un proveedor de servicios:

i. que se haya puesto en funcionamiento para un grupo restringido de usuarios, y
ii. que no emplee las redes públicas de telecomunicación y no esté conectado a otro sistema informático, ya sea público o privado,

dicha Parte podrá reservarse el derecho a no aplicar dichas medidas a esas comunicaciones. Las Partes tratarán de limitar este tipo de reservas de modo que de modo que sea posible la más amplia aplicación de las medidas previstas en los artículos 20 y 21.

Artículo 15 – Condiciones y salvaguardias

1. Cada Parte se asegurará de que la instauración, ejecución y aplicación de los poderes y procedimientos previstos en la presente Sección se sometan a las condiciones y salvaguardias previstas en su derecho interno, que deberá garantizar una protección adecuada de los derechos humanos y de las libertades, y en particular de los derechos

derivados de las obligaciones que haya asumido cada Parte en virtud del Convenio del Consejo de Europa para la Protección de los Derechos Humanos y de las Libertades Fundamentales (1950), el Pacto Internacional de Derechos Civiles y Políticos de las Naciones Unidas (1966) u otros instrumentos internacionales aplicables en materia de derechos humanos, y que deberá integrar el principio de proporcionalidad.

2. Cuando proceda, teniendo en cuenta la naturaleza del procedimiento o del poder de que se trate, dichas condiciones y salvaguardias incluirán una supervisión judicial u otra forma de supervisión independiente, los motivos que justifiquen su aplicación, así como la limitación del ámbito de aplicación y de la duración de dicho poder o procedimiento.

3. Siempre que sea conforme con el interés público, y en particular con la buena administración de la justicia, cada Parte examinará los efectos de los poderes y procedimientos mencionados en la presente Sección sobre los derechos, responsabilidades e intereses legítimos de terceros.

Título 2 – Conservación rápida de datos informáticos almacenados

Artículo 16 – Conservación rápida de datos informáticos almacenados

1. Cada Parte adoptará las medidas legislativas y de otro tipo que resulten necesarias para permitir a sus autoridades competentes ordenar o imponer de otro modo la conservación rápida de datos electrónicos específicos, incluidos los datos relativos al tráfico, almacenados por medio de un sistema informático, en particular cuando existan motivos para creer que dichos datos son particularmente susceptibles de pérdida o de modificación.

2. Cuando una Parte aplique lo dispuesto en el párrafo 1 anterior por medio de una orden impartida a una persona de que conserve determinados datos almacenados que se encuentren en poder o bajo el control de esa persona, la Parte adoptará las medidas legislativas y de otro tipo que resulten necesarias para obligar a dicha persona a conservar y a proteger la integridad de los datos durante el tiempo necesario, hasta un máximo de noventa días, con el fin de que las autoridades competentes puedan obtener su revelación. Las Partes podrán prever la renovación de dicha orden.

3. Cada Parte adoptará las medidas legislativas y de otro tipo que resulten necesarias para obligar a la persona que custodia los datos o a otra persona encargada de su conservación a mantener en secreto la ejecución de dichos procedimientos durante el tiempo previsto en su derecho interno.

4. Los poderes y procedimientos mencionados en el presente artículo estarán sujetos a lo dispuesto en los artículos 14 y 15.

Artículo 17 – Conservación y revelación parcial rápidas de los datos relativos al tráfico

1. Con el fin de garantizar la conservación de los datos relativos al tráfico, en aplicación del artículo 16, cada Parte adoptará las medidas legislativas y de otro tipo que resulten necesarias para:

a. garantizar la conservación rápida de los datos relativos al tráfico, ya sean uno o varios los proveedores de servicios que hayan participado en la transmisión de dicha comunicación; y
b. asegurar la revelación rápida a la autoridad competente de la Parte, o a una persona designada por dicha autoridad, de un volumen suficiente de datos relativos al tráfico para que dicha Parte pueda identificar tanto a los proveedores de servicios como la vía por la que la comunicación se ha transmitido.

2. Los poderes y procedimientos mencionados en el presente artículo estarán sujetos a lo dispuesto en los artículos 14 y 15.

Título 3 – Orden de presentación

Artículo 18 – Orden de presentación

1. Cada Parte adoptará las medidas legislativas y de otro tipo que resulten necesarias para facultar a sus autoridades competentes a ordenar:

a. a una persona presente en su territorio que comunique determinados datos informáticos que obren en su poder o bajo su control, almacenados en un sistema informático o en un dispositivo de almacenamiento informático; y
b. a un proveedor que ofrezca sus servicios en el territorio de dicha Parte, que comunique los datos que obren en su poder o bajo su control relativos a los abonados en relación con dichos servicios;

2. Los poderes y procedimientos mencionados en el presente artículo estarán sujetos a lo dispuesto en los artículos 14 y 15.

3. A los efectos del presente artículo, se entenderá por «datos relativos a los abonados» cualquier información, en forma de datos informáticos o de cualquier otro modo, que posea un proveedor de servicios y que se refiera a los abonados de sus servicios, diferentes de los datos relativos al tráfico o al contenido, y que permitan determinar:

a. el tipo de servicio de comunicación utilizado, las disposiciones técnicas adoptadas al respecto y el periodo de servicio;
b. la identidad, la dirección postal o situación geográfica y el número de teléfono del abonado, así como cualquier otro número de acceso y los datos relativos a la facturación y al pago, disponibles en virtud de un contrato o de un acuerdo de prestación de servicio;
c. cualquier otra información relativa al lugar en que se encuentren los equipos de comunicación, disponible en virtud de un contrato o de un acuerdo de prestación de servicio.

Título 4 – Registro y confiscación de datos informáticos almacenados

Artículo 19 – Registro y confiscación de datos informáticos almacenados

1. Cada Parte adoptará las medidas legislativas y de otro tipo que resulten necesarias para facultar a sus autoridades competentes a registrar o a tener acceso de un modo similar:

a. a todo sistema informático o a parte del mismo, así como a los datos informáticos en él almacenados; y
b. a todo dispositivo de almacenamiento informático que permita almacenar datos informáticos

en su territorio.

2. Cada Parte adoptará las medidas legislativas y de otro tipo que resulten necesarias para asegurarse de que, cuando, de conformidad con el apartado 1.a), sus autoridades registren o tengan acceso de un modo similar a un sistema informático específico o a una parte del mismo y tengan motivos para creer que los datos buscados se hallan almacenados en otro sistema informático o en una parte del mismo situado en su territorio, y que dichos datos son legítimamente accesibles a partir del sistema inicial o están disponibles por medio de dicho sistema inicial, puedan extender rápidamente el registro o el acceso de un modo similar al otro sistema.

3. Cada Parte adoptará las medidas legislativas y de otro tipo que resulten necesarias para facultar a sus autoridades competentes a confiscar o a obtener de un modo similar los datos informáticos a los que se haya accedido en aplicación de los párrafos 1 o 2. Estas medidas incluirán las siguientes prerrogativas:

a. confiscar u obtener de un modo similar un sistema informático o una parte del mismo, o un dispositivo de almacenamiento informático;
b. realizar y conservar una copia de esos datos informáticos;
c. preservar la integridad de los datos informáticos almacenados pertinentes; y
d. hacer inaccesibles o suprimir dichos datos informáticos del sistema informático consultado.

4. Cada Parte adoptará las medidas legislativas y de otro tipo que resulten necesarias para facultar a sus autoridades competentes a ordenar a toda persona que conozca el funcionamiento de un sistema informático o las medidas aplicadas para proteger los datos informáticos que contiene, que proporcione toda la información necesaria, dentro de lo razonable, para permitir la aplicación de las medidas previstas en los párrafos 1 y 2.

5. Los poderes y procedimientos mencionados en el presente artículo estarán sujetos a lo dispuesto en los artículos 14 y 15.

Título 5 – Obtención en tiempo real de datos informáticos

Artículo 20 – Obtención en tiempo real de datos relativos al tráfico

1. Cada Parte adoptará las medidas legislativas y de otro tipo que resulten necesarias para facultar a sus autoridades competentes:

a. a obtener o grabar con medios técnicos existentes en su territorio, y
b. a obligar a cualquier proveedor de servicios, en la medida de sus capacidades técnicas:

    i. a obtener o a grabar con medios técnicos existentes en su territorio, o

ii. a ofrecer a las autoridades competentes su colaboración y su asistencia para obtener o grabar

en tiempo real los datos relativos al tráfico asociados a comunicaciones específicas transmitidas en su territorio por medio de un sistema informático.

2. Cuando una Parte no pueda adoptar las medidas enunciadas en el apartado 1.a) por respeto a los principios establecidos en su ordenamiento jurídico interno, podrá, en su lugar, adoptar las medidas legislativas y de otro tipo que resulten necesarias para asegurar la obtención o la grabación en tiempo real de los datos relativos al tráfico asociados a comunicaciones específicas transmitidas en su territorio mediante la aplicación de medios técnicos existentes en dicho territorio.

3. Cada Parte adoptará las medidas legislativas y de otro tipo que resulten necesarias para obligar a un proveedor de servicios a mantener en secreto el hecho de que se haya ejercido cualquiera de los poderes previstos en el presente artículo, así como toda información al respecto.

4. Los poderes y procedimientos mencionados en el presente artículo estarán sujetos a lo dispuesto en los artículos 14 y 15.

Artículo 21 – Interceptación de datos relativos al contenido

1. Cada Parte adoptará las medidas legislativas y de otro tipo que resulten necesarias para facultar a sus autoridades competentes en lo que respecta a un repertorio de delitos graves que deberá definirse en su derecho interno a:

a. obtener o grabar con medios técnicos existentes en su territorio, y
b. obligar a un proveedor de servicios, en la medida de sus capacidades técnicas, a:

i. obtener o grabar con medios técnicos existentes en su territorio, o
ii. prestar a las autoridades competentes su colaboración y su asistencia para obtener o grabar,

en tiempo real los datos relativos al contenido de comunicaciones específicas transmitidas en su territorio por medio de un sistema informático.

2. Cuando una Parte no pueda adoptar las medidas enunciadas en el apartado 1.a) por respeto a los principios establecidos en su ordenamiento jurídico interno, podrá, en su lugar, adoptar las medidas legislativas y de otro tipo que resulten necesarias para asegurar la obtención o la grabación en tiempo real de los datos relativos al contenido de comunicaciones específicas transmitidas en su territorio con medios técnicos existentes en ese territorio.

3. Cada Parte adoptará las medidas legislativas y de otro tipo que resulten necesarias para obligar a un proveedor de servicios a mantener en secreto el hecho de que se haya ejercido cualquiera de los poderes previstos en el presente artículo, así como toda información al respecto.

4. Los poderes y procedimientos mencionados en el presente artículo estarán sujetos a lo dispuesto en los artículos 14 y 15.

Sección 3 – Jurisdicción

Artículo 22 – Jurisdicción

1. Cada Parte adoptará las medidas legislativas y de otro tipo que resulten necesarias para afirmar su jurisdicción respecto de cualquier delito previsto de conformidad con los artículos 2 a 11 del presente Convenio, cuando el delito se haya cometido:

a. en su territorio; o
b. a bordo de un buque que enarbole su pabellón; o
c. a bordo de una aeronave matriculada según sus leyes; o
d. por uno de sus nacionales, si el delito es susceptible de sanción penal en el lugar en el que se cometió o si ningún Estado tiene competencia territorial respecto del mismo.

2. Las Partes podrán reservarse el derecho a no aplicar, o a aplicar sólo en determinados casos o condiciones, las normas sobre jurisdicción establecidas en los apartados 1.b) a 1.d) del presente artículo o en cualquier parte de dichos apartados.

3. Cada Parte adoptará las medidas que resulten necesarias para afirmar su jurisdicción respecto de cualquier delito mencionado en el párrafo 1 del artículo 24 del presente Convenio cuando el presunto autor del mismo se halle en su territorio y no pueda ser extraditado a otra Parte por razón únicamente de su nacionalidad, previa demanda de extradición.

4. El presente Convenio no excluye ninguna jurisdicción penal ejercida por una Parte de conformidad con su derecho interno.

5. En el caso de que varias Partes reivindiquen su jurisdicción respecto de un presunto delito contemplado en el presente Convenio, las Partes interesadas celebrarán consultas, cuando ello sea oportuno, con el fin de decidir qué jurisdicción es más adecuada para entablar la acción penal.

Capítulo III – Cooperación internacional

Sección 1 – Principios generales

Título 1 – Principios generales relativos a la cooperación internacional

Artículo 23 – Principios generales relativos a la cooperación internacional

Las Partes cooperarán entre sí en la mayor medida posible de conformidad con las disposiciones del presente Capítulo, en aplicación de los instrumentos internacionales pertinentes sobre cooperación internacional en materia penal, de los acuerdos basados en legislación uniforme o recíproca y de su propio derecho interno, a efectos de las investigaciones o los procedimientos relativos a los delitos relacionados con sistemas y datos informáticos o para obtener pruebas en formato electrónico de los delitos.

Título 2 – Principios relativos a la extradición

Artículo 24 – Extradición

1. a. El presente artículo se aplicará a la extradición entre las Partes por los delitos definidos de conformidad con los artículos 2 a 11 del presente Convenio, siempre que sean castigados por la legislación de las dos Partes implicadas con una pena privativa de libertad de una duración de al menos un año, o con una pena más grave.

b. Cuando se aplique una pena mínima diferente en virtud de un tratado de extradición aplicable entre dos o más Partes, incluido el Convenio Europeo de Extradición (STE nº 24), o de un acuerdo basado en legislación uniforme o recíproca, se aplicará la pena mínima prevista en dicho tratado o acuerdo.

2. Se considerará que los delitos descritos en el párrafo 1 del presente artículo están incluidos entre los delitos que pueden dar lugar a extradición en todos los tratados de extradición concluidos entre o por las Partes. Las Partes se comprometerán a incluir dichos delitos entre los que pueden dar lugar a extradición en todos los tratados de extradición que puedan concluir.

3. Cuando una parte que condicione la extradición a la existencia de un tratado reciba una demanda de extradición de otra Parte con la que no ha concluido ningún tratado de extradición, podrá tomar el presente Convenio como fundamento jurídico de la extradición en relación con cualquiera de los delitos previstos en el párrafo 1 del presente artículo.

4. Las Partes que no condicionen la extradición a la existencia de un tratado reconocerán los delitos mencionados en el párrafo 1 del presente artículo como delitos que pueden dar lugar a extradición entre ellas.

5. La extradición estará sujeta a las condiciones previstas en el derecho interno de la Parte requerida o en los tratados de extradición vigentes, incluidos los motivos por los que la Parte requerida puede denegar la extradición.

6. Si se deniega la extradición por un delito mencionado en el párrafo 1 del presente artículo únicamente por razón de la nacionalidad de la persona reclamada o porque la Parte requerida se considera competente respecto de dicho delito, la Parte requerida deberá someter el asunto, a petición de la Parte requirente, a sus autoridades competentes a efectos de la acción penal pertinente, e informará, a su debido tiempo, de la conclusión del asunto a la Parte requirente. Dichas autoridades tomarán su decisión y realizarán sus investigaciones y procedimientos del mismo modo que para cualquier otro delito de naturaleza comparable, de conformidad con la legislación de dicha Parte.

7. a. Cada Parte comunicará al Secretario General del Consejo de Europa, en el momento de la firma o del depósito de su instrumento de ratificación, aceptación, aprobación o adhesión, el nombre y la dirección de cada autoridad responsable del envío o de la recepción de las demandas de extradición o de detención provisional, en ausencia de tratado.

b. El Secretario General del Consejo de Europa creará y mantendrá actualizado un registro de las autoridades designadas por las Partes. Cada Parte garantizará en todo momento la exactitud de los datos que figuren en el registro.

Título 3 – Principios generales relativos a la asistencia mutua

Artículo 25 – Principios generales relativos a la asistencia mutua

1. Las Partes se prestarán toda la ayuda mutua posible a efectos de las investigaciones o de los procedimientos relativos a los delitos relacionados con sistemas y datos informáticos o con el fin de obtener pruebas en formato electrónico de un delito.

2. Cada Parte adoptará asimismo las medidas legislativas y de otro tipo que resulten necesarias para cumplir con las obligaciones establecidas en los artículos 27 a 35.

3. Cada Parte podrá, en caso de urgencia, formular una solicitud de asistencia mutua, o realizar las comunicaciones relativas a la misma a través de medios de comunicación rápidos, como el fax o el correo electrónico, siempre que esos medios ofrezcan niveles suficientes de seguridad y de autenticación (incluido el criptado, en caso necesario), con confirmación oficial posterior si el Estado requerido así lo exige. El Estado requerido aceptará la solicitud y responderá a la misma por cualquiera de esos medios rápidos de comunicación.

4. Salvo en caso de que se disponga expresamente otra cosa en los artículos del presente Capítulo, la asistencia mutua estará sujeta a las condiciones establecidas en el derecho interno de la Parte requerida o en los tratados de asistencia mutua aplicables, incluidos los motivos sobre la base de los cuales la Parte requerida puede rechazar la cooperación. La Parte requerida no deberá ejercer su derecho a rehusar la asistencia mutua en relación con los delitos previstos en los artículos 2 a 11 únicamente porque la solicitud se refiera a un delito que dicha Parte considere de carácter fiscal.

5. Cuando, de conformidad con lo dispuesto en el presente Capítulo, la Parte requerida esté autorizada a condicionar la asistencia mutua a la existencia de doble tipificación penal, se considerará que dicha condición se satisface si el acto que constituye delito, y para el que se solicita la asistencia mutua, está tipificado como tal en su derecho interno, independientemente de que dicho derecho interno incluya o no el delito en la misma categoría o lo denomine o no con la misma terminología que la Parte requirente.

Artículo 26 – Información espontánea

1. Dentro de los límites de su derecho interno y sin que exista demanda previa, una Parte podrá comunicar a otra Parte información obtenida de sus propias investigaciones si considera que ello puede ayudar a la Parte destinataria a iniciar o a concluir investigaciones o procedimientos en relación con delitos previstos de conformidad con el presente Convenio, o cuando dicha información pueda conducir a una petición de cooperación de dicha Parte en virtud del presente Capítulo.

2. Antes de comunicar dicha información, la Parte que la proporciona podrá pedir que sea tratada de forma confidencial o que sólo se utilice bajo ciertas condiciones. Si la Parte destinataria no puede atender a dicha petición, deberá informar de ello a la otra Parte, que decidirá a continuación si, no obstante, debe proporcionar la información. Si la Parte destinataria acepta la información bajo las condiciones establecidas, estará obligada a respetarlas.

Título 4 – Procedimientos relativos a las solicitudes de asistencia mutua en ausencia de acuerdos internacionales aplicables

Artículo 27 – Procedimientos relativos a las solicitudes de asistencia mutua en ausencia de acuerdos internacionales aplicables

1. En ausencia de tratado de asistencia mutua o de acuerdo basado en legislación uniforme o recíproca en vigor entre la Parte requirente y la Parte requerida, se aplicarán las disposiciones de los párrafos 2 a 9 del presente artículo. Dichas disposiciones no se aplicarán cuando exista un tratado, acuerdo o legislación de este tipo, a menos que las Partes implicadas decidan aplicar en su lugar la totalidad o una parte del resto del presente artículo.

2. a. Cada Parte designará una o varias autoridades centrales encargadas de enviar las solicitudes de asistencia mutua o de responder a las mismas, de ejecutarlas o de remitirlas a las autoridades competentes para su ejecución;

b. las autoridades centrales comunicarán directamente entre sí;

c. en el momento de la firma o del depósito de su instrumento de ratificación, aceptación, aprobación o adhesión, cada Parte comunicará al Secretario General del Consejo de Europa los nombres y direcciones de las autoridades designadas en aplicación del presente párrafo.

d. el Secretario General del Consejo de Europa creará y mantendrá actualizado un registro de las autoridades centrales designadas por las Partes. Cada Parte garantizará en todo momento la exactitud de los datos que figuren en el registro.

3. Las solicitudes de asistencia mutua en virtud del presente artículo se ejecutarán de conformidad con el procedimiento especificado por la Parte requirente, salvo cuando dicho procedimiento sea incompatible con la legislación de la Parte requerida.

4. Además de las condiciones o los motivos de denegación previstos en el párrafo 4 del artículo 25, la asistencia mutua puede ser denegada por la Parte requerida:

a. si la solicitud tiene que ver con un delito que la Parte requerida considera de carácter político o vinculado a un delito de carácter político; o
b. si la Parte requerida estima que acceder a la solicitud podría atentar contra su soberanía, seguridad, orden público u otros intereses esenciales.

5. La Parte requerida podrá aplazar su actuación en respuesta a una solicitud si dicha actuación puede perjudicar a investigaciones o procedimientos llevados a cabo por sus autoridades.

6. Antes de denegar o aplazar su cooperación, la Parte requerida estudiará, previa consulta con la Parte requirente cuando proceda, si puede atenderse la solicitud parcialmente o bajo las condiciones que considere necesarias.

7. La Parte requerida informará rápidamente a la Parte requirente del curso que prevé dar a la solicitud de asistencia. Deberá motivar toda denegación o aplazamiento de la misma. La Parte requerida informará asimismo a la Parte requirente de cualquier motivo que imposibilite la ejecución de la asistencia o que pueda retrasarla sustancialmente.

8. La Parte requirente podrá solicitar que la Parte requerida mantenga confidenciales la presentación y el objeto de cualquier solicitud formulada en virtud del presente Capítulo, salvo en la medida en que sea necesario para la ejecución de la misma. Si la Parte requerida no puede acceder a la petición de confidencialidad, deberá informar de ello sin demora a la Parte requirente, quien decidirá a continuación si, no obstante, la solicitud debe ser ejecutada.

9. a. En caso de urgencia, las autoridades judiciales de la Parte requirente podrán dirigir directamente a las autoridades homólogas de la Parte requerida las solicitudes de asistencia y las comunicaciones relativas a las mismas. En tales casos, se remitirá simultáneamente una copia a la autoridad central de la Parte requerida a través de la autoridad central de la Parte requirente.

b. Toda solicitud o comunicación en virtud del presente párrafo podrá formularse a través de la Organización Internacional de Policía Criminal (Interpol).

c. Cuando se formule una solicitud en aplicación del apartado a) del presente artículo y la autoridad no tenga competencia para tratarla, la remitirá a la autoridad nacional competente e informará directamente de ello a la Parte requirente.

d. Las solicitudes o comunicaciones realizadas en aplicación del presente párrafo que no impliquen medidas coercitivas podrán ser transmitidas directamente por las autoridades competentes de la Parte requirente a las autoridades competentes de la Parte requerida.

e. En el momento de la firma o del depósito de su instrumento de ratificación, aceptación, aprobación o adhesión, las Partes podrán informar al Secretario General del Consejo de Europa de que, en aras de la eficacia, las solicitudes formuladas en virtud del presente párrafo deberán dirigirse a su autoridad central.

Artículo 28 – Confidencialidad y restricciones de uso

1. En ausencia de tratado de asistencia mutua o de acuerdo basado en legislación uniforme o recíproca en vigor entre la Parte requirente y la Parte requerida, se aplicarán las disposiciones del presente artículo. Dichas disposiciones no se aplicarán cuando exista un tratado, acuerdo o legislación de este tipo, a menos que las Partes interesadas decidan aplicar en su lugar la totalidad o una parte del presente artículo.

2. La Parte requerida podrá supeditar la transmisión de información o de material en respuesta a una solicitud al cumplimiento de las siguientes condiciones:

a. que se preserve su confidencialidad cuando la solicitud de asistencia no pueda ser atendida en ausencia de dicha condición; o
b. que no se utilicen para investigaciones o procedimientos distintos a los indicados en la solicitud.

3. Si la Parte requirente no pudiera satisfacer alguna de las condiciones mencionadas en el párrafo 2, informará de ello sin demora a la Parte requerida, quien determinará a continuación si, no obstante, la información ha de ser proporcionada. Si la Parte requirente acepta esta condición, estará obligada a cumplirla.

4. Toda Parte que proporcione información o material supeditado a alguna de las condiciones mencionadas en el párrafo 2 podrá exigir a la otra Parte precisiones sobre el uso que haya hecho de dicha información o material en relación con dicha condición.

Sección 2 – Disposiciones específicas

Título 1 – Asistencia mutua en materia de medidas provisionales

Artículo 29 – Conservación rápida de datos informáticos almacenados

1. Una Parte podrá solicitar a otra Parte que ordene o imponga de otro modo la conservación rápida de datos almacenados por medio de sistemas informáticos que se encuentren en el territorio de esa otra Parte, y en relación con los cuales la Parte requirente tenga intención de presentar una solicitud de asistencia mutua con vistas al registro o al acceso por un medio similar, la confiscación o la obtención por un medio similar, o a la revelación de dichos datos.

2. En toda solicitud de conservación formulada en virtud del párrafo 1 deberá precisarse:

a. la autoridad que solicita la conservación;
b. el delito objeto de la investigación o de procedimientos penales y una breve exposición de los hechos relacionados con el mismo;
c. los datos informáticos almacenados que deben conservarse y su relación con el delito;
d. toda información disponible que permita identificar al responsable de la custodia de los datos informáticos almacenados o el emplazamiento del sistema informático;
e. la necesidad de la medida de conservación; y
f. que la Parte tiene intención de presentar una solicitud de asistencia mutua con vistas al registro o al acceso por un medio similar, a la confiscación o a la obtención por un medio similar, o a la revelación de los datos informáticos almacenados.

3. Tras recibir la solicitud de otra Parte, la Parte requerida deberá adoptar todas las medidas adecuadas para proceder sin demora a la conservación de los datos solicitados, de conformidad con su derecho interno. A los efectos de responder a solicitudes de este tipo no se requiere la doble tipificación penal como condición para proceder a la conservación.

4. Cuando una Parte exige la doble tipificación penal como condición para atender a una solicitud de asistencia mutua con vistas al registro o al acceso por un medio similar, a la confiscación o a la obtención por un medio similar o a la revelación de los datos almacenados en relación con delitos diferentes de los previstos de conformidad con los artículos 2 a 11 del presente Convenio, podrá reservarse el derecho a denegar la solicitud de conservación en virtud del presente artículo en caso de que tenga motivos para creer que, en el momento de la revelación de los datos, no se cumplirá la condición de la doble tipificación penal.

5. Asimismo, las solicitudes de conservación sólo podrán ser denegadas si:

a. la solicitud se refiere a un delito que la Parte requerida considera de carácter político o vinculado a un delito de carácter político; o

b. la Parte requerida considera que la ejecución de la solicitud podría atentar contra su soberanía, seguridad, orden público u otros intereses esenciales.

6. Cuando la Parte requerida considere que la conservación por sí sola de los datos no bastará para garantizar su disponibilidad futura, o que pondrá en peligro la confidencialidad de la investigación de la Parte requirente, o causará cualquier otro perjuicio a la misma, informará de ello rápidamente a la Parte requirente, quien determinará a continuación la conveniencia, no obstante, de dar curso a la solicitud.

7. Las medidas de conservación adoptadas en respuesta a solicitudes como la prevista en el párrafo 1 serán válidas por un periodo mínimo de 60 días, con el fin de que la Parte requirente pueda presentar una solicitud con vistas al registro o el acceso por un medio similar, la confiscación o la obtención por un medio similar, o la revelación de los datos. Una vez recibida la solicitud, los datos deberán conservarse hasta que se tome una decisión sobre la misma.

Artículo 30 – Revelación rápida de datos conservados

1. Si, al ejecutar una solicitud formulada de conformidad con el artículo 29 para la conservación de datos relativos al tráfico de una determinada comunicación la Parte requerida descubriera que un proveedor de servicios de otro Estado ha participado en la transmisión de dicha comunicación, dicha Parte revelará rápidamente a la Parte requirente un volumen suficiente de datos relativos al tráfico para que pueda identificarse al proveedor de servicios, así como la vía por la que la comunicación ha sido transmitida.

2. La revelación de datos relativos al tráfico en aplicación del párrafo 1 sólo podrá ser denegada si:

a. la solicitud se refiere a un delito que la Parte requerida considera de carácter político o vinculado a un delito de carácter político; o
b. la Parte requerida considera que la ejecución de la solicitud podría atentar contra su soberanía, seguridad, orden público u otros intereses esenciales.

Título 2 – Asistencia mutua en relación con los poderes de investigación

Artículo 31 – Asistencia mutua en relación con el acceso a datos almacenados

1. Una Parte podrá solicitar a otra Parte el registro o el acceso de un modo similar, la confiscación o la obtención de un modo similar o la revelación de datos almacenados por medio de un sistema informático que se encuentre en el territorio de esa otra Parte, incluidos los datos conservados de conformidad con el artículo 29.

2. La Parte requerida responderá a la solicitud aplicando los instrumentos internacionales, acuerdos y legislación mencionados en el artículo 23, así como de conformidad con las disposiciones pertinentes del presente Capítulo.

3. La solicitud deberá responderse lo más rápidamente posible en los siguientes casos:

a. cuando existan motivos para creer que los datos pertinentes están particularmente expuestos al riesgo de pérdida o de modificación; o

b. cuando los instrumentos, acuerdos o legislación mencionados en el párrafo 2 prevean una cooperación rápida.

Artículo 32 – Acceso transfronterizo a datos almacenados, con consentimiento o cuando sean accesibles al público

Una Parte podrá, sin autorización de otra:

a. tener acceso a datos informáticos almacenados accesibles al público (fuente abierta), independientemente de la ubicación geográfica de los mismos; o
b. tener acceso a datos informáticos almacenados en otro Estado, o recibirlos, a través de un sistema informático situado en su territorio, si dicha Parte obtiene el consentimiento lícito y voluntario de la persona legalmente autorizada a revelárselos por medio de ese sistema informático.

Artículo 33 – Asistencia mutua para la obtención en tiempo real de datos relativos al tráfico

1. Las Partes se prestarán asistencia mutua para la obtención en tiempo real de datos relativos al tráfico asociados a comunicaciones específicas transmitidas en su territorio por medio de un sistema informático. A reserva de las disposiciones del párrafo 2, dicha asistencia mutua estará sujeta a las condiciones y procedimientos previstos en el derecho interno.

2. Cada Parte prestará dicha asistencia al menos en relación con los delitos para los cuales sería posible la obtención en tiempo real de datos relativos al tráfico en situaciones análogas a nivel interno.

Artículo 34 – Asistencia mutua en relación con la interceptación de datos relativos al contenido

Las Partes se prestarán asistencia mutua, en la medida en que lo permitan sus tratados y leyes internas aplicables, para la obtención o el registro en tiempo real de datos relativos al contenido de comunicaciones específicas transmitidas por medio de un sistema informático.

Título 3 – Red 24/7

Artículo 35 – Red 24/7

1. Cada Parte designará un punto de contacto localizable las 24 horas del día, siete días a la semana, con el fin de garantizar una asistencia inmediata para investigaciones relativas a delitos vinculados a sistemas y datos informáticos, o para obtener las pruebas en formato electrónico de un delito. Esta asistencia comprenderá toda acción que facilite las medidas que figuran a continuación, o su aplicación directa si lo permite el derecho y la práctica internos:

a. asesoramiento técnico;
b. conservación de datos, de conformidad con los artículos 29 y 30; y
c. obtención de pruebas, suministro de información de carácter jurídico y localización de sospechosos.

2. a. El punto de contacto de una Parte dispondrá de los medios para comunicarse con el punto de contacto de otra Parte siguiendo un procedimiento acelerado.

b. Si el punto de contacto designado por una Parte no depende de la autoridad o autoridades de dicha Parte responsables de la asistencia mutua internacional o de la extradición, dicho punto de contacto se asegurará de poder actuar coordinadamente con esta o estas autoridades por medio de un procedimiento acelerado.

3. Cada Parte garantizará la disponibilidad de personal formado y equipado con objeto de facilitar el funcionamiento de la red.

Capítulo IV – Cláusulas finales

Artículo 36 – Firma y entrada en vigor

1. El presente Convenio está abierto a la firma de los Estados miembros del Consejo de Europa y de los Estados no miembros que hayan participado en su elaboración.

2. El presente Convenio estará sujeto a ratificación, aceptación o aprobación. Los instrumentos de ratificación, aceptación o aprobación se depositarán en poder del Secretario General del Consejo de Europa.

3. El presente Convenio entrará en vigor el primer día del mes siguiente a la expiración de un plazo de tres meses desde la fecha en que cinco Estados, de los cuales al menos tres deberán ser miembros del Consejo de Europa, hayan expresado su consentimiento para quedar vinculados por el Convenio, de conformidad con lo dispuesto en los párrafos 1 y 2.

4. Para todo Estado signatario que exprese ulteriormente su consentimiento para quedar vinculado por el Convenio, éste entrará en vigor el primer día del mes siguiente a la expiración de un plazo de tres meses desde la fecha en que haya expresado dicho consentimiento, de conformidad con lo dispuesto en los párrafos 1 y 2.

Artículo 37 – Adhesión al Convenio

1. A partir de la entrada en vigor del presente Convenio, el Comité de Ministros del Consejo de Europa podrá, previa consulta con los Estados contratantes del Convenio y habiendo obtenido su consentimiento unánime, invitar a adherirse al presente Convenio a cualquier Estado que no sea miembro del Consejo de Europa y que no haya participado en su elaboración. La decisión se adoptará respetando la mayoría establecida en el artículo 20.d del Estatuto del Consejo de Europa y con el voto unánime de los representantes de los Estados contratantes con derecho a formar parte del Comité de Ministros.

2. Para todo Estado que se adhiera al Convenio de conformidad con el párrafo 1 precedente, el Convenio entrará en vigor el primer día del mes siguiente a la expiración de un plazo de tres meses desde la fecha del depósito del instrumento de adhesión en poder del Secretario General del Consejo de Europa.

Artículo 38 – Aplicación territorial

1. En el momento de la firma o del depósito del instrumento de ratificación, aceptación, aprobación o adhesión, todo Estado podrá designar el territorio o los territorios a los que se aplicará el presente Convenio.

2. Posteriormente, todo Estado podrá, en cualquier momento y por medio de una declaración dirigida al Secretario General del Consejo de Europa, hacer extensiva la aplicación del presente Convenio a cualquier otro territorio especificado en la declaración. El Convenio entrará en vigor respecto de dicho territorio el primer día del mes siguiente a la expiración de un plazo de tres meses desde la fecha en que el Secretario General haya recibido la declaración.

3. Toda declaración formulada en virtud de los dos párrafos precedentes podrá ser retirada, respecto de cualquier territorio especificado en la misma, mediante notificación dirigida al Secretario General del Consejo de Europa. La retirada surtirá efecto el primer día del mes siguiente a la expiración de un plazo de tres meses desde la fecha en que el Secretario General haya recibido la notificación.

Artículo 39 – Efectos del Convenio

1. El objeto del presente Convenio es completar los tratados o acuerdos multilaterales o bilaterales aplicables entre las Partes, incluidas las disposiciones:

– del Convenio Europeo de Extradición, abierto a la firma el 13 de diciembre de 1957 en París (STE nº 24)

– del Convenio Europeo de Asistencia Judicial en Materia Penal, abierto a la firma el 20 de abril de 1959 en Estrasburgo (STE nº 30),

– del Protocolo adicional al Convenio Europeo de Asistencia Judicial en Materia Penal, abierto a la firma el 17 de marzo de 1978 en Estrasburgo (STE nº 99).

2. Si dos o más Partes han celebrado ya un acuerdo o un tratado relativo a las cuestiones contempladas en el presente Convenio, o han regulado de otro modo sus relaciones al respecto, o si lo hacen en el futuro, podrán asimismo aplicar el citado acuerdo o tratado, o regular sus relaciones de conformidad con el mismo, en lugar del presente Convenio. No obstante, cuando las Partes regulen sus relaciones respecto de las cuestiones objeto del presente Convenio de forma distinta a la prevista en el mismo, lo harán de modo que no sea incompatible con los objetivos y principios del Convenio.

3. Nada de lo dispuesto en el presente Convenio afectará a otros derechos, restricciones, obligaciones y responsabilidades de cada Parte.

Artículo 40 – Declaraciones

Mediante declaración por escrito dirigida al Secretario General del Consejo de Europa, cualquier Estado podrá declarar, en el momento de la firma o del depósito de su instrumento de ratificación, aceptación, aprobación o adhesión, que se acoge a la facultad de exigir, llegado el caso, uno o varios elementos complementarios previstos en los artículos 2, 3, 6.1.b), 7, 9.3 y 27.9.e).

Artículo 41 – Cláusula federal

1. Un Estado federal podrá reservarse el derecho a cumplir las obligaciones especificadas en el Capítulo II del presente Convenio en la medida en que éstas sean compatibles con los principios fundamentales por los que se rijan las relaciones entre su gobierno central y los estados que lo constituyen u otras entidades territoriales análogas, a condición de que pueda garantizar la cooperación según lo previsto en el Capítulo III.

2. Cuando formule una reserva en virtud del párrafo 1, un Estado federal no podrá hacer uso de los términos de dicha reserva para excluir o reducir de manera sustancial sus obligaciones en virtud del Capítulo II. En todo caso, se dotará de medios amplios y efectivos para aplicar las medidas previstas en el citado Capítulo.

3. En lo relativo a las disposiciones del presente Convenio cuya aplicación sea competencia legislativa de cada uno de los estados constituyentes u otras entidades territoriales análogas, que no estén obligados por el sistema constitucional de la federación a adoptar medidas legislativas, el gobierno federal pondrá dichas disposiciones en conocimiento de las autoridades competentes de los estados constituyentes junto con su opinión favorable, alentándolas a adoptar las medidas adecuadas para su aplicación.

Artículo 42 – Reservas

Mediante notificación por escrito dirigida al Secretario del Consejo de Europa, cualquier Estado podrá declarar, en el momento de la firma o del depósito de su instrumento de ratificación, aceptación, aprobación o adhesión, que se acoge a una o varias de las reservas previstas en el párrafo 2 del artículo 4, el párrafo 3 del artículo 6, el párrafo 4 del artículo 9, el párrafo 3 del artículo 10, el párrafo 3 del artículo 11, el párrafo 3 del artículo 14, el párrafo 2 del artículo 22, el párrafo 4 del artículo 29 y el párrafo 1 del artículo 41. No podrá formularse ninguna otra reserva.

Artículo 43 – Mantenimiento y retirada de las reservas

1. Una Parte que haya formulado una reserva de conformidad con el artículo 42 podrá retirarla total o parcialmente mediante notificación por escrito dirigida al Secretario General del Consejo de Europa. Dicha retirada surtirá efecto en la fecha en que el Secretario General reciba la notificación. Si en la notificación se indica una fecha a partir de la cual ha de hacerse efectiva la retirada de una reserva y esta fecha es posterior a la fecha en la que el Secretario General ha recibido la notificación, la retirada se hará efectiva en dicha fecha posterior.

2. Una Parte que haya formulado una reserva de las mencionadas en el artículo 42 retirará dicha reserva, total o parcialmente, tan pronto como lo permitan las circunstancias.

3. El Secretario General del Consejo de Europa podrá solicitar periódicamente a las Partes que hayan formulado una o varias reservas conforme a lo dispuesto en el artículo 42, información sobre las perspectivas de su retirada.

Artículo 44 – Enmiendas

1. Cada Parte podrá proponer enmiendas al presente Convenio, que el Secretario General del Consejo de Europa comunicará a los Estados miembros del Consejo de Europa, a los Estados no miembros que hayan participado en la elaboración del presente Convenio y a cualquier Estado que se haya adherido o que haya sido invitado a adherirse de conformidad con lo dispuesto en el artículo 37.

2. Toda enmienda propuesta por cualquiera de las Partes será comunicada al Comité Europeo para Problemas Criminales (CDPC), quien someterá al Comité de Ministros su opinión sobre la enmienda propuesta.

3. El Comité de Ministros examinará la enmienda propuesta y la opinión presentada por el CDPC y, previa consulta con los Estados no miembros Partes en el presente Convenio, podrá adoptar la enmienda.

4. El texto de cualquier enmienda adoptada por el Comité de Ministros de conformidad con lo dispuesto en el párrafo 3 del presente artículo será remitido a las Partes para su aceptación.

5. Toda enmienda adoptada de conformidad con el párrafo 3 del presente artículo entrará en vigor treinta días después de que todas las Partes hayan informado al Secretario General de su aceptación.

Artículo 45 – Solución de controversias

1. Se mantendrá informado al Comité Europeo para Problemas Criminales (CDPC) del Consejo de Europa acerca de la interpretación y la aplicación del presente Convenio.

2. En caso de controversia entre las Partes sobre la interpretación o la aplicación del presente Convenio, las Partes intentarán llegar a un acuerdo mediante negociación o por cualquier otro medio pacífico de su elección, incluida la sumisión de la controversia al CDPC, a un tribunal arbitral cuyas decisiones serán vinculantes para las Partes en litigio, o a la Corte Internacional de Justicia, según acuerden dichas Partes.

Artículo 46 – Consultas entre las Partes

1. Las Partes se consultarán periódicamente, según sea necesario, con el fin de facilitar:

a. la utilización y la aplicación efectivas del presente Convenio, incluida la identificación de cualquier problema al respecto, así como las repercusiones de toda declaración o reserva formulada de conformidad con el presente Convenio;
b. el intercambio de información sobre novedades jurídicas, políticas o técnicas importantes observadas en el ámbito de la delincuencia informática y la obtención de pruebas en formato electrónico;
c. el estudio de la posibilidad de ampliar o enmendar el Convenio.

2. Se informará periódicamente al Comité Europeo para Problemas Criminales (CDPC) del resultado de las consultas mencionadas en el párrafo 1.

3. En caso necesario, el Comité Europeo para Problemas Criminales (CDPC) facilitará las consultas mencionadas en el párrafo 1 y adoptará las medidas necesarias para ayudar a las Partes en sus esfuerzos por ampliar o enmendar el Convenio. Expirado un

plazo de tres años como máximo desde la entrada en vigor del presente Convenio, el CDPC procederá, en cooperación con las Partes, a una revisión de todas las disposiciones de la Convención y propondrá, si procede, las enmiendas pertinentes.

4. Salvo cuando el Consejo de Europa los asuma, los gastos que ocasione la aplicación de las disposiciones del párrafo 1 serán sufragados por las Partes, en la forma que ellas mismas determinen.

5. Las Partes recibirán asistencia del Secretario del Consejo de Europa en el ejercicio de las funciones que dimanan del presente artículo.

Artículo 47 – Denuncia

1. Las Partes podrán denunciar en cualquier momento el presente Convenio mediante notificación dirigida al Secretario General del Consejo de Europa.

2. Dicha denuncia surtirá efecto el primer día del mes siguiente a la expiración de un plazo de tres meses desde la fecha en que el Secretario General haya recibido la notificación.

Artículo 48 – Notificación

El Secretario General del Consejo de Europa notificará a los Estados miembros del Consejo de Europa, a los Estados no miembros que hayan participado en la elaboración del presente Convenio, así como a cualquier Estado que se haya adherido o que haya sido invitado a adherirse al mismo:

a. cualquier firma;
b. el depósito de cualquier instrumento de ratificación, aceptación, aprobación o adhesión;
c. cualquier fecha de entrada en vigor del presente Convenio de conformidad con los artículos 36 y 37;
d. cualquier declaración presentada de conformidad con el artículo 40 o cualquier reserva formulada en virtud del artículo 42;
e. cualquier otro acto, notificación o comunicación relativos al presente Convenio.

En fe de lo cual, los infrascritos, debidamente autorizados a tal efecto, firman el presente Convenio.

Hecho en Budapest, el 23 de noviembre de 2001, en versión francesa e inglesa, ambos textos igualmente auténticos, y en un ejemplar único que se depositará en los archivos del Consejo de Europa. El Secretario General del Consejo de Europa remitirá copia certificada a cada uno de los Estados miembros del Consejo de Europa, a los Estados no miembros que hayan participado en la elaboración del Convenio y a cualquier Estado invitado a adherirse al mismo.

UNIDAD II: CONOCIMIENTOS LEGALES

2.- Ley 30071 y 30096 de Delitos Informáticos.

PODER LEGISLATIVO

CONGRESO DE LA REPUBLICA

LEY Nº 30170

EL PRESIDENTE DE LA REPÚBLICA

POR CUANTO:

LA COMISIÓN PERMANENTE DEL CONGRESO DE LA REPÚBLICA;

Ha dado la Ley siguiente:

LEY QUE MODIFICA EL ARTÍCULO 1 DE LA LEY 29631

Artículo 1. Objeto de la Ley
La presente Ley tiene como objeto modificar el artículo 1 de la Ley 29631, que en adelante se denominará "Ley de transferencia a título oneroso del predio rural terreno rústico, denominado Buena Vista o Los Anitos, de propiedad de la Sociedad de Beneficencia de Lima Metropolitana, a favor de la Municipalidad Provincial de Barranca".

Artículo 2. Modificación del artículo 1 de la Ley 29631
Modifícase el artículo 1 de la Ley 29631 con el siguiente texto:

"Artículo 1.- Transferencia de propiedad predial interestatal
Autorízase a efectuar la transferencia a título oneroso y a un valor comercial de S/. 8 695 500,00 (ocho millones seiscientos noventa y cinco mil quinientos y 00/100 nuevos soles) del predio denominado Buena Vista o Los Anitos, de propiedad de la Sociedad de Beneficencia de Lima Metropolitana, a favor de la Municipalidad Provincial de Barranca en el departamento de Lima. Dicho predio se encuentra ubicado en el distrito y provincia de Barranca, sector EPS Nueva Esperanza, valle Pativilca, con 93,3111 hectáreas, con un perímetro de 4 542,75 metros lineales, con Código Catastral: 8_2008805_100011 y la Unidad Catastral 100011, debidamente inscrito en el registro de la propiedad inmueble, con la Partida Nº P18014352 de la Zona Registral Nº IX-Sede Lima".

Artículo 3. Autorización de recursos y ajustes contables

3.1 Autorízase al Gobierno Regional de Lima, para atender el monto señalado en el artículo 1 de la Ley 29631, modificada por la presente Ley, por la transferencia predial, con cargo a sus recursos provenientes del canon, sobrecanon y regalías mineras, en dos ejercicios presupuestales, dentro de los tres primeros meses de cada año; transfiriendo a la Sociedad de Beneficencia de Lima Metropolitana, el 2014, el 50% del valor comercial del predio y, el 2015, el saldo del valor del predio. Asimismo, facúltase a las entidades involucradas para efectuar los ajustes contables que se requieran para implementar lo establecido en esta disposición legal.

3.2 El financiamiento a que se refiere el párrafo precedente se efectúa sin demandar recursos al Tesoro Público.

Artículo 4. Transferencia del predio
A la entrada en vigencia de la presente Ley, la Sociedad de Beneficencia de Lima Metropolitana transfiere física y legalmente el predio a que se refiere el artículo 1 de la Ley 29631, modificada por la presente Ley, a la Municipalidad Provincial de Barranca, inscribiéndose dicha transferencia en la partida registral inmobiliaria correspondiente.

Comuníquese al señor Presidente Constitucional de la República para su promulgación.

En Lima, a los diecisiete días del mes de febrero de dos mil catorce.

FREDY OTÁROLA PEÑARANDA
Presidente del Congreso de la República

JOSÉ LUNA GÁLVEZ
Tercer Vicepresidente del Congreso de la República

AL SEÑOR PRESIDENTE CONSTITUCIONAL DE LA REPÚBLICA

POR TANTO:

Mando se publique y cumpla.

Dado en la Casa de Gobierno, en Lima, a los nueve días del mes de marzo del año dos mil catorce.

OLLANTA HUMALA TASSO
Presidente Constitucional de la República

RENÉ CORNEJO DÍAZ
Presidente del Consejo de Ministros

1059231-1

LEY Nº 30171

EL PRESIDENTE DE LA REPÚBLICA

POR CUANTO:

LA COMISIÓN PERMANENTE DEL CONGRESO DE LA REPÚBLICA;

Ha dado la Ley siguiente:

LEY QUE MODIFICA LA LEY 30096, LEY DE DELITOS INFORMÁTICOS

Artículo 1. Modificación de los artículos 2, 3, 4, 5, 7, 8 y 10 de la Ley 30096, Ley de Delitos Informáticos
Modifícanse los artículos 2, 3, 4, 5, 7, 8 y 10 de la Ley 30096, Ley de Delitos Informáticos, en los siguientes términos:

"**Artículo 2. Acceso ilícito**
El que deliberada e ilegítimamente accede a todo o en parte de un sistema informático, siempre que se realice con vulneración de medidas de seguridad establecidas para impedirlo, será reprimido con pena privativa de libertad no menor de uno ni mayor de cuatro años y con treinta a noventa días-multa.
Será reprimido con la misma pena, el que accede a un sistema informático excediendo lo autorizado."

"**Artículo 3. Atentado a la integridad de datos informáticos**
El que deliberada e ilegítimamente daña, introduce, borra, deteriora, altera, suprime o hace inaccesibles datos informáticos, será reprimido con pena privativa de libertad no menor de tres ni mayor de seis años y con ochenta a ciento veinte días-multa."

"**Artículo 4. Atentado a la integridad de sistemas informáticos**
El que deliberada e ilegítimamente inutiliza, total o parcialmente, un sistema informático, impide el acceso a este, entorpece o imposibilita su funcionamiento o la prestación de sus servicios, será reprimido con pena privativa de libertad no menor de tres ni mayor de seis años y con ochenta a ciento veinte días-multa."

"**Artículo 5. Proposiciones a niños, niñas y adolescentes con fines sexuales por medios tecnológicos**
El que a través de internet u otro medio análogo contacta con un menor de catorce años para solicitar u obtener de él material pornográfico, o para llevar a cabo actividades sexuales con él, será reprimido con una pena privativa de libertad no menor de cuatro ni mayor de ocho años e inhabilitación conforme a los numerales 1, 2 y 4 del artículo 36 del Código Penal.
Cuando la víctima tiene entre catorce y menos de dieciocho años de edad y medie engaño, la pena será no menor de tres ni mayor de seis años e inhabilitación conforme a los numerales 1, 2 y 4 del artículo 36 del Código Penal."

"**Artículo 7. Interceptación de datos informáticos**
El que deliberada e ilegítimamente intercepta datos informáticos en transmisiones no públicas, dirigidos a un sistema informático, originados en un sistema informático o efectuado dentro del mismo, incluidas las emisiones electromagnéticas provenientes de

un sistema informático que transporte dichos datos informáticos, será reprimido con una pena privativa de libertad no menor de tres ni mayor de seis años.
La pena privativa de libertad será no menor de cinco ni mayor de ocho años cuando el delito recaiga sobre información clasificada como secreta, reservada o confidencial de conformidad con la Ley 27806, Ley de Transparencia y Acceso a la Información Pública.
La pena privativa de libertad será no menor de ocho ni mayor de diez cuando el delito comprometa la defensa, seguridad o soberanía nacionales.
Si el agente comete el delito como integrante de una organización criminal, la pena se incrementa hasta en un tercio por encima del máximo legal previsto en los supuestos anteriores."

"**Artículo 8. Fraude informático**
El que deliberada e ilegítimamente procura para sí o para otro un provecho ilícito en perjuicio de tercero mediante el diseño, introducción, alteración, borrado, supresión, clonación de datos informáticos o cualquier interferencia o manipulación en el funcionamiento de un sistema informático, será reprimido con una pena privativa de libertad no menor de tres ni mayor de ocho años y con sesenta a ciento veinte días-multa.
La pena será privativa de libertad no menor de cinco ni mayor de diez años y de ochenta a ciento cuarenta días-multa cuando se afecte el patrimonio del Estado destinado a fines asistenciales o a programas de apoyo social."

"**Artículo 10. Abuso de mecanismos y dispositivos informáticos**
El que deliberada e ilegítimamente fabrica, diseña, desarrolla, vende, facilita, distribuye, importa u obtiene para su utilización, uno o más mecanismos, programas informáticos, dispositivos, contraseñas, códigos de acceso o cualquier otro dato informático, específicamente diseñados para la comisión de los delitos previstos en la presente Ley, o el que ofrece o presta servicio que contribuya a ese propósito, será reprimido con pena privativa de libertad no menor de uno ni mayor de cuatro años y con treinta a noventa días-multa."

Artículo 2. Modificación de la tercera, cuarta y undécima disposiciones complementarias finales de la Ley 30096, Ley de Delitos Informáticos
Modifícanse la tercera, cuarta y undécima disposiciones complementarias finales de la Ley 30096, Ley de Delitos Informáticos, en los siguientes términos:

"**TERCERA. Coordinación interinstitucional entre la Policía Nacional, el Ministerio Público y otros organismos especializados**
La Policía Nacional del Perú fortalece el órgano especializado encargado de coordinar las funciones de investigación con el Ministerio Público. A fin de establecer mecanismos de comunicación con los órganos de gobierno del Ministerio Público, el centro de respuesta temprana del gobierno para ataques cibernéticos (Pe-CERT), la Oficina Nacional de Gobierno Electrónico e Informática (ONGEI) y los Organismos Especializados de las Fuerzas Armadas, la Policía Nacional centraliza la información aportando su experiencia en la elaboración de los programas y acciones para la adecuada persecución de los delitos informáticos, y desarrolla programas de protección y seguridad."

"**CUARTA. Cooperación operativa**
Con el objeto de garantizar el intercambio de información, los equipos de investigación conjuntos, la transmisión de documentos, la interceptación de comunicaciones y demás actividades correspondientes para dar efectividad a la presente Ley, la Policía Nacional del Perú, el Ministerio Público, el Poder Judicial, el Pe-CERT (Centro de respuesta temprana del gobierno para ataques cibernéticos), la ONGEI (Oficina Nacional de Gobierno Electrónico e Informática), Organismos Especializados de las Fuerzas Armadas y los operadores del sector privado involucrados en la lucha contra los delitos informáticos deben establecer protocolos de cooperación operativa reformada en el plazo de treinta días desde la vigencia de la presente Ley."

"**UNDÉCIMA. Regulación e imposición de multas por el Organismo Supervisor de Inversión Privada en Telecomunicaciones**
El Organismo Supervisor de Inversión Privada en Telecomunicaciones establece las multas aplicables a las empresas bajo su supervisión que incumplan con la obligación prevista en el numeral 4 del artículo 230 del Código Procesal Penal, aprobado por Decreto Legislativo 957.
Las empresas de telecomunicaciones organizan sus recursos humanos y logísticos a fin de cumplir con la debida diligencia y sin dilación la obligación prevista en el numeral 4 del artículo 230 del Código Procesal Penal.
El juez, en el término de setenta y dos horas, pone en conocimiento del órgano supervisor la omisión incurrida por la empresa a fin de que el Organismo Supervisor de Inversión Privada en Telecomunicaciones aplique la multa correspondiente."

Artículo 3. Incorporación del artículo 12 a la Ley 30096, Ley de Delitos Informáticos
Incorpórase el artículo 12 a la Ley 30096, Ley de Delitos Informáticos, en los siguientes términos:

"**Artículo 12. Exención de responsabilidad penal**
Está exento de responsabilidad penal el que realiza las conductas descritas en los artículos 2, 3, 4 y 10 con el propósito de llevar a cabo pruebas autorizadas u otros procedimientos autorizados destinados a proteger sistemas informáticos."

Artículo 4. Modificación de los artículos 158, 162 y 323 del Código Penal
Modifícanse los artículos 158, 162 y 323 del Código Penal, aprobado por Decreto Legislativo 635 y modificado por la Ley 30096, Ley de Delitos Informáticos, en los siguientes términos:

"**Artículo 158. Ejercicio de la acción penal**
Los delitos previstos en este Capítulo son perseguibles por acción privada, salvo en el caso del delito previsto en el artículo 154-A."

"**Artículo 162. Interferencia telefónica**
El que, indebidamente, interfiere o escucha una conversación telefónica o similar, será reprimido con pena privativa de libertad no menor de tres ni mayor de seis años.
Si el agente es funcionario público, la pena privativa de libertad será no menor de cuatro ni mayor de ocho años e inhabilitación conforme al artículo 36, incisos 1, 2 y 4.
La pena privativa de libertad será no menor de cinco ni mayor de ocho años cuando el delito recaiga sobre información clasificada como secreta, reservada o confidencial de conformidad con la Ley 27806, Ley de Transparencia y Acceso a la Información Pública.
La pena privativa de libertad será no menor de ocho ni mayor de diez años, cuando el delito comprometa la defensa, seguridad o soberanía nacionales.
Si el agente comete el delito como integrante de una organización criminal, la pena se incrementa hasta en un tercio por encima del máximo legal previsto en los supuestos anteriores."

"**Artículo 323. Discriminación e incitación a la discriminación**
El que, por sí o mediante terceros, discrimina a una o más personas o grupo de personas, o incita o promueve en forma pública actos discriminatorios, por motivo racial, religioso, sexual, de factor genético, filiación, edad, discapacidad, idioma, identidad étnica y cultural, indumentaria, opinión política o de cualquier índole, o condición económica, con el objeto de anular o menoscabar el reconocimiento, goce o ejercicio de los derechos de la persona, será reprimido con pena privativa de libertad no menor de dos años, ni mayor de tres o con prestación de servicios a la comunidad de sesenta a ciento veinte jornadas.
Si el agente es funcionario o servidor público la pena será no menor de dos, ni mayor de cuatro años e inhabilitación conforme al numeral 2 del artículo 36.
La misma pena privativa de libertad señalada en el párrafo anterior se impondrá si la discriminación, la incitación o promoción de actos discriminatorios se ha materializado mediante actos de violencia física o mental o a través de internet u otro medio análogo."

Artículo 5. Incorporación de los artículos 154-A y 183-B al Código Penal
Incorpóranse los artículos 154-A y 183-B al Código Penal, aprobado por Decreto Legislativo 635, con el siguiente texto:

"**Artículo 154-A. Tráfico ilegal de datos personales**
El que ilegítimamente comercializa o vende información no pública relativa a cualquier ámbito de la esfera

personal, familiar, patrimonial, laboral, financiera u otro de naturaleza análoga sobre una persona natural, será reprimido con pena privativa de libertad no menor de dos ni mayor de cinco años.
Si el agente comete el delito como integrante de una organización criminal, la pena se incrementa hasta en un tercio por encima del máximo legal previsto en el párrafo anterior."

"**Artículo 183-B. Proposiciones sexuales a niños, niñas y adolescentes**
El que contacta con un menor de catorce años para solicitar u obtener de él material pornográfico, o para llevar a cabo actividades sexuales con él, será reprimido con una pena privativa de libertad no menor de cuatro ni mayor de ocho años e inhabilitación conforme a los numerales 1, 2 y 4 del artículo 36.
Cuando la víctima tiene entre catorce y menos de dieciocho años de edad y medie engaño, la pena será no menor de tres ni mayor de seis años e inhabilitación conforme a los numerales 1, 2 y 4 del artículo 36."

Artículo 6. Modificación del numeral 4 del artículo 230 del Código Procesal Penal
Modifícase el numeral 4 del artículo 230 del Código Procesal Penal, modificado por la Ley 30096, Ley de Delitos Informáticos, con el siguiente texto:

"**Artículo 230. Intervención, grabación o registro de comunicaciones telefónicas o de otras formas de comunicación y geolocalización de teléfonos móviles**
(...)

4. Los concesionarios de servicios públicos de telecomunicaciones deben facilitar, en forma inmediata, la geolocalización de teléfonos móviles y la diligencia de intervención, grabación o registro de las comunicaciones que haya sido dispuesta mediante resolución judicial, en tiempo real y en forma ininterrumpida, las 24 horas de los 365 días del año, bajo apercibimiento de ser pasible de las responsabilidades de Ley en caso de incumplimiento. Los servidores de las indicadas empresas deben guardar secreto acerca de las mismas, salvo que se les citare como testigo al procedimiento.
Dichos concesionarios otorgarán el acceso, la compatibilidad y conexión de su tecnología con el Sistema de Intervención y Control de las Comunicaciones de la Policía Nacional del Perú. Asimismo, cuando por razones de innovación tecnológica los concesionarios renueven sus equipos y software, se encontrarán obligados a mantener la compatibilidad con el sistema de intervención y control de las comunicaciones de la Policía Nacional del Perú.
(...)."

DISPOSICIÓN COMPLEMENTARIA DEROGATORIA

ÚNICA. Derogación del artículo 6 de la Ley 30096, Ley de Delitos Informáticos
Derógase el artículo 6 de la Ley 30096, Ley de Delitos Informáticos.

Comuníquese al señor Presidente Constitucional de la República para su promulgación.

En Lima, a los diecisiete días del mes de febrero de dos mil catorce.

FREDY OTÁROLA PEÑARANDA
Presidente del Congreso de la República

JOSÉ LUNA GÁLVEZ
Tercer Vicepresidente del Congreso de la República

AL SEÑOR PRESIDENTE CONSTITUCIONAL
DE LA REPÚBLICA

POR TANTO:

Mando se publique y cumpla.

Dado en la Casa de Gobierno, en Lima, a los nueve días del mes de marzo del año dos mil catorce.

OLLANTA HUMALA TASSO
Presidente Constitucional de la República

RENÉ CORNEJO DÍAZ
Presidente del Consejo de Ministros

1059231-2

PODER EJECUTIVO

AGRICULTURA Y RIEGO

Designan Jefe de la Unidad de Logística y Patrimonio del Programa de Desarrollo Productivo Agrario Rural - AGRO RURAL

RESOLUCION DIRECTORAL EJECUTIVA
Nº 052-2014-MINAGRI-DVM-DIAR-AGRO RURAL-DE

Lima, 6 de marzo de 2014

VISTA:

La carta de renuncia presentada por el Licenciado Adolfo Martín Estrada Gamarra, y;

CONSIDERANDO:

Que, mediante Resolución Directoral Ejecutiva N° 001-2014-MINAGRI-DVM-DIAR-AGRO RURAL-DE, se designó al Licenciado Adolfo Martín Estrada Gamarra en el cargo de Jefe de la Unidad de Logística y Patrimonio del Programa de Desarrollo Productivo Agrario Rural - AGRO RURAL, del Ministerio de Agricultura y Riego;
Que, el citado funcionario ha presentado su renuncia al cargo, la misma que se ha visto pertinente aceptar y designar a su reemplazante;
De conformidad con lo establecido en la Ley N° 27594, Ley que regula la participación del Poder Ejecutivo en el Nombramiento y Designación de Funcionarios Públicos y en uso de las atribuciones conferidas en el Manual de Operaciones, aprobado mediante Resolución Ministerial Nº 1120-2008-AG;

SE RESUELVE:

Artículo 1°.- ACEPTAR la renuncia formulada por el Licenciado ADOLFO MARTÍN ESTRADA GAMARRA al cargo de Jefe de la Unidad de Logística y Patrimonio del Programa de Desarrollo Productivo Agrario Rural - AGRO RURAL, del Ministerio de Agricultura y Riego, dándosele las gracias por los servicios prestados.
Artículo 2º.- DESIGNAR al Licenciado HUGO ERNESTO VILELA CONSUELO en el cargo de Jefe de la Unidad de Logística y Patrimonio del Programa de Desarrollo Productivo Agrario Rural - AGRO RURAL, del Ministerio de Agricultura y Riego, cargo considerado de confianza.
Artículo 3º.- DISPONER la publicación de la presente resolución en el Diario Oficial "El Peruano" y en el Portal Electrónico del Programa de Desarrollo Productivo Agrario Rural - AGRO RURAL (www.agrorural.gob.pe).

Regístrese, comuníquese y publíquese.

CÉSAR SOTOMAYOR CALDERÓN
Director Ejecutivo
Programa de Desarrollo Productivo
Agrario Rural - AGRO RURAL

1058565-1

Designan Jefa de la Oficina de Planificación del Programa de Desarrollo Productivo Agrario Rural - AGRO RURAL

RESOLUCIÓN DIRECTORAL EJECUTIVA
Nº 053-2014-MINAGRI-DVM-DIAR-AGRO RURAL-DE

Lima, 6 de marzo de 2014

VISTA:

La Resolución Directoral Ejecutiva N° 047-2014-MINAGRI-DVM-DIAR-AGRO RURAL-DE, y;

CONSIDERANDO:

Que, mediante la Resolución del Vista, se encargaron las funciones de Jefe de la Oficina de Planificación del Programa

ORGANOS AUTONOMOS

CONTRALORIA GENERAL

INSTITUCIONES EDUCATIVAS

JURADO NACIONAL DE ELECCIONES

MINISTERIO PUBLICO

SUPERINTENDENCIA DE BANCA, SEGUROS Y ADMINISTRADORAS PRIVADAS DE FONDOS DE PENSIONES

GOBIERNOS LOCALES

PROVINCIAS

MUNICIPALIDAD PROVINCIAL DE PALLASCA - CABANA

PODER LEGISLATIVO

CONGRESO DE LA REPUBLICA

LEY Nº 30096

EL PRESIDENTE DE LA REPÚBLICA

POR CUANTO:

El Congreso de la República
Ha dado la Ley siguiente:

EL CONGRESO DE LA REPÚBLICA;
Ha dado la Ley siguiente:

LEY DE DELITOS INFORMÁTICOS

CAPÍTULO I

FINALIDAD Y OBJETO DE LA LEY

Artículo 1. Objeto de la Ley
La presente Ley tiene por objeto prevenir y sancionar las conductas ilícitas que afectan los sistemas y datos informáticos y otros bienes jurídicos de relevancia penal, cometidas mediante la utilización de tecnologías de la información o de la comunicación, con la finalidad de garantizar la lucha eficaz contra la ciberdelincuencia.

CAPÍTULO II

DELITOS CONTRA DATOS Y SISTEMAS INFORMÁTICOS

Artículo 2. Acceso ilícito
El que accede sin autorización a todo o parte de un sistema informático, siempre que se realice con vulneración de medidas de seguridad establecidas para impedirlo, será reprimido con pena privativa de libertad no menor de uno ni mayor de cuatro años y con treinta a noventa días multa.

Será reprimido con la misma pena el que accede a un sistema informático excediendo lo autorizado.

Artículo 3. Atentado contra la integridad de datos informáticos
El que, a través de las tecnologías de la información o de la comunicación, introduce, borra, deteriora, altera, suprime o hace inaccesibles datos informáticos, será reprimido con pena privativa de libertad no menor de tres ni mayor de seis años y con ochenta a ciento veinte días multa.

Artículo 4. Atentado contra la integridad de sistemas informáticos

El que, a través de las tecnologías de la información o de la comunicación, inutiliza, total o parcialmente, un sistema informático, impide el acceso a este, entorpece o imposibilita su funcionamiento o la prestación de sus servicios, será reprimido con pena privativa de libertad no menor de tres ni mayor de seis años y con ochenta a ciento veinte días multa.

CAPÍTULO III

DELITOS INFORMÁTICOS CONTRA LA INDEMNIDAD Y LIBERTAD SEXUALES

Artículo 5. Proposiciones a niños, niñas y adolescentes con fines sexuales por medios tecnológicos

El que, a través de las tecnologías de la información o de la comunicación, contacta con un menor de catorce años para solicitar u obtener de él material pornográfico, o para llevar a cabo actividades sexuales con él, será reprimido con pena privativa de libertad no menor de cuatro ni mayor de ocho años e inhabilitación conforme a los numerales 1, 2 y 4 del artículo 36 del Código Penal.

Cuando la víctima tiene entre catorce y menos de dieciocho años de edad y medie engaño, la pena será no menor de tres ni mayor de seis años e inhabilitación conforme a los numerales 1, 2 y 4 del artículo 36 del Código Penal.

CAPÍTULO IV

DELITOS INFORMÁTICOS CONTRA LA INTIMIDAD Y EL SECRETO DE LAS COMUNICACIONES

Artículo 6. Tráfico ilegal de datos

El que crea, ingresa o utiliza indebidamente una base de datos sobre una persona natural o jurídica, identificada o identificable, para comercializar, traficar, vender, promover, favorecer o facilitar información relativa a cualquier ámbito de la esfera personal, familiar, patrimonial, laboral, financiera u otro de naturaleza análoga, creando o no perjuicio, será reprimido con pena privativa de libertad no menor de tres ni mayor de cinco años.

Artículo 7. Interceptación de datos informáticos

El que, a través de las tecnologías de la información o de la comunicación, intercepta datos informáticos en transmisiones no públicas, dirigidas a un sistema informático, originadas en un sistema informático o efectuadas dentro del mismo, incluidas las emisiones electromagnéticas provenientes de un sistema informático que transporte dichos datos informáticos, será reprimido con pena privativa de libertad no menor de tres ni mayor de seis años.

La pena privativa de libertad será no menor de cinco ni mayor de ocho años cuando el delito recaiga sobre información clasificada como secreta, reservada o confidencial de conformidad con las normas de la materia.

La pena privativa de libertad será no menor de ocho ni mayor de diez años cuando el delito comprometa la defensa, la seguridad o la soberanía nacionales.

CAPÍTULO V

DELITOS INFORMÁTICOS CONTRA EL PATRIMONIO

Artículo 8. Fraude informático

El que, a través de las tecnologías de la información o de la comunicación, procura para sí o para otro un provecho ilícito en perjuicio de tercero mediante el diseño, introducción, alteración, borrado, supresión, clonación de datos informáticos o cualquier interferencia o manipulación en el funcionamiento de un sistema informático, será reprimido con una pena privativa de libertad no menor de tres ni mayor de ocho años y con sesenta a ciento veinte días multa.

La pena será privativa de libertad no menor de cinco ni mayor de diez años y de ochenta a ciento cuarenta días multa cuando se afecte el patrimonio del Estado destinado a fines asistenciales o a programas de apoyo social.

CAPÍTULO VI

DELITOS INFORMÁTICOS CONTRA LA FE PÚBLICA

Artículo 9. Suplantación de identidad

El que, mediante las tecnologías de la información o de la comunicación suplanta la identidad de una persona natural o jurídica, siempre que de dicha conducta resulte algún perjuicio, material o moral, será reprimido con pena privativa de libertad no menor de tres ni mayor de cinco años.

CAPÍTULO VII

DISPOSICIONES COMUNES

Artículo 10. Abuso de mecanismos y dispositivos informáticos

El que fabrica, diseña, desarrolla, vende, facilita, distribuye, importa u obtiene para su utilización uno o más mecanismos, programas informáticos, dispositivos, contraseñas, códigos de acceso o cualquier otro dato informático, específicamente diseñados para la comisión de los delitos previstos en la presente Ley, o el que ofrece o presta servicio que contribuya a ese propósito, será reprimido con pena privativa de libertad no menor de uno ni mayor de cuatro años y con treinta a noventa días multa.

Artículo 11. Agravantes

El juez aumenta la pena privativa de libertad hasta en un tercio por encima del máximo legal fijado para cualquiera de los delitos previstos en la presente Ley cuando:

1. El agente comete el delito en calidad de integrante de una organización criminal.
2. El agente comete el delito mediante el abuso de una posición especial de acceso a la data o información reservada o al conocimiento de esta información en razón del ejercicio de un cargo o función.
3. El agente comete el delito con el fin de obtener un beneficio económico, salvo en los delitos que prevén dicha circunstancia.
4. El delito compromete fines asistenciales, la defensa, la seguridad y la soberanía nacionales.

DISPOSICIONES COMPLEMENTARIAS FINALES

PRIMERA. Codificación de la pornografía infantil

La Policía Nacional del Perú puede mantener en sus archivos, con la autorización y supervisión respectiva del Ministerio Público, material de pornografía infantil, en medios de almacenamiento de datos informáticos, para fines exclusivos del cumplimiento de su función. Para tal efecto, cuenta con una base de datos debidamente codificada.

La Policía Nacional del Perú y el Ministerio Público establecen protocolos de coordinación en el plazo de treinta días a fin de cumplir con la disposición establecida en el párrafo anterior.

SEGUNDA. Agente encubierto en delitos informáticos

El fiscal, atendiendo a la urgencia del caso particular y con la debida diligencia, puede autorizar la actuación de agentes encubiertos a efectos de realizar las investigaciones de los delitos previstos en la presente Ley y de todo delito que se cometa mediante tecnologías de la información o de la comunicación, con prescindencia de si los mismos están vinculados a una organización criminal, de conformidad con el artículo 341 del Código Procesal Penal, aprobado mediante el Decreto Legislativo 957.

TERCERA. Coordinación interinstitucional de la Policía Nacional del Perú con el Ministerio Público

La Policía Nacional del Perú fortalece al órgano especializado encargado de coordinar las funciones de investigación con el Ministerio Público. A fin de establecer mecanismos de comunicación con los órganos de gobierno del Ministerio Público, la Policía Nacional del Perú centraliza la información aportando su experiencia en la elaboración de los programas y acciones para

la adecuada persecución de los delitos informáticos, y desarrolla programas de protección y seguridad.

CUARTA. Cooperación operativa
Con el objeto de garantizar el intercambio de información, los equipos de investigación conjuntos, la transmisión de documentos, la interceptación de comunicaciones y demás actividades correspondientes para dar efectividad a la presente Ley, la Policía Nacional del Perú, el Ministerio Público, el Poder Judicial y los operadores del sector privado involucrados en la lucha contra los delitos informáticos deben establecer protocolos de cooperación operativa reforzada en el plazo de treinta días desde la vigencia de la presente Ley.

QUINTA. Capacitación
Las instituciones públicas involucradas en la prevención y represión de los delitos informáticos deben impartir cursos de capacitación destinados a mejorar la formación profesional de su personal –especialmente de la Policía Nacional del Perú, el Ministerio Público y el Poder Judicial– en el tratamiento de los delitos previstos en la presente Ley.

SEXTA. Medidas de seguridad
La Oficina Nacional de Gobierno Electrónico e Informática (ONGEI) promueve permanentemente, en coordinación con las instituciones del sector público, el fortalecimiento de sus medidas de seguridad para la protección de los datos informáticos sensibles y la integridad de sus sistemas informáticos.

SÉTIMA. Buenas prácticas
El Estado peruano realiza acciones conjuntas con otros Estados a fin de poner en marcha acciones y medidas concretas destinadas a combatir el fenómeno de los ataques masivos contra las infraestructuras informáticas y establece los mecanismos de prevención necesarios, incluyendo respuestas coordinadas e intercambio de información y buenas prácticas.

OCTAVA. Convenios multilaterales
El Estado peruano promueve la firma y ratificación de convenios multilaterales que garanticen la cooperación mutua con otros Estados para la persecución de los delitos informáticos.

NOVENA. Terminología
Para efectos de la presente Ley, se entenderá, de conformidad con el artículo 1 del Convenio sobre la Ciberdelincuencia, Budapest, 23.XI.2001:

a. **Por sistema informático:** todo dispositivo aislado o conjunto de dispositivos interconectados o relacionados entre sí, cuya función, o la de alguno de sus elementos, sea el tratamiento automatizado de datos en ejecución de un programa.
b. **Por datos informáticos:** toda representación de hechos, información o conceptos expresados de cualquier forma que se preste a tratamiento informático, incluidos los programas diseñados para que un sistema informático ejecute una función.

DÉCIMA. Regulación e imposición de multas por la Superintendencia de Banca, Seguros y AFP
La Superintendencia de Banca, Seguros y AFP establece la escala de multas atendiendo a las características, complejidad y circunstancias de los casos aplicables a las empresas bajo su supervisión que incumplan con la obligación prevista en el numeral 5 del artículo 235 del Código Procesal Penal, aprobado por el Decreto Legislativo 957.
El juez, en el término de setenta y dos horas, pone en conocimiento del órgano supervisor la omisión incurrida por la empresa, con los recaudos correspondientes sobre las características, complejidad y circunstancias del caso particular, a fin de aplicarse la multa correspondiente.

UNDÉCIMA. Regulación e imposición de multas por el Organismo Supervisor de Inversión Privada en Telecomunicaciones
El Organismo Supervisor de Inversión Privada en Telecomunicaciones establece la escala de multas atendiendo a las características, complejidad y circunstancias de los casos aplicables a las empresas bajo su supervisión que incumplan con la obligación prevista en el numeral 4 del artículo 230 del Código Procesal Penal, aprobado por el Decreto Legislativo 957.
El juez, en el término de setenta y dos horas, pone en conocimiento del órgano supervisor la omisión incurrida por la empresa, con los recaudos correspondientes sobre las características, complejidad y circunstancias del caso particular, a fin de aplicarse la multa correspondiente.

DISPOSICIONES COMPLEMENTARIAS MODIFICATORIAS

PRIMERA. Modificación de la Ley 27697, Ley que otorga facultad al fiscal para la intervención y control de comunicaciones y documentos privados en caso excepcional
Modifícase el artículo 1 de la Ley 27697, Ley que otorga facultad al fiscal para la intervención y control de comunicaciones y documentos privados en caso excepcional, modificado por el Decreto Legislativo 991, en los siguientes términos:

"**Artículo 1. Marco y finalidad**
La presente Ley tiene por finalidad desarrollar legislativamente la facultad constitucional otorgada a los jueces para conocer y controlar las comunicaciones de las personas que son materia de investigación preliminar o jurisdiccional.
Solo podrá hacerse uso de la facultad prevista en la presente Ley en los siguientes delitos:

1. Secuestro.
2. Trata de personas.
3. Pornografía infantil.
4. Robo agravado.
5. Extorsión.
6. Tráfico ilícito de drogas.
7. Tráfico ilícito de migrantes.
8. Delitos contra la humanidad.
9. Atentados contra la seguridad nacional y traición a la patria.
10. Peculado.
11. Corrupción de funcionarios.
12. Terrorismo.
13. Delitos tributarios y aduaneros.
14. Lavado de activos.
15. Delitos informáticos."

SEGUNDA. Modificación de la Ley 30077, Ley contra el crimen organizado
Modifícase el numeral 9 del artículo 3 de la Ley 30077, Ley contra el crimen organizado, en los siguientes términos:

"**Artículo 3. Delitos comprendidos**
La presente Ley es aplicable a los siguientes delitos:
(...)
9. Delitos informáticos previstos en la ley penal."

TERCERA. Modificación del Código Procesal Penal
Modifícase el numeral 4 del artículo 230, el numeral 5 del artículo 235 y el literal a) del numeral 1 del artículo 473 del Código Procesal Penal, aprobado por el Decreto Legislativo 957, en los siguientes términos:

"**Artículo 230. Intervención o grabación o registro de comunicaciones telefónicas o de otras formas de comunicación**
(...)
4. Los concesionarios de servicios públicos de telecomunicaciones deberán facilitar, en el plazo máximo de treinta días hábiles, la geolocalización de teléfonos móviles y la diligencia de intervención, grabación o registro de las comunicaciones, así como la información sobre la identidad de los titulares del servicio, los números de registro del cliente, de la línea telefónica y del equipo, del tráfico de llamadas y los números de protocolo de internet, que haya sido dispuesta mediante resolución judicial, en tiempo real y en forma ininterrumpida,

las veinticuatro horas de los trescientos sesenta y cinco días del año, bajo apercibimiento de ser pasible de las responsabilidades de ley en caso de incumplimiento. Los servidores de las indicadas empresas deberán guardar secreto acerca de las mismas, salvo que se les citare como testigos al procedimiento. El juez fija el plazo en atención a las características, complejidad y circunstancias del caso en particular.

Dichos concesionarios otorgarán el acceso, la compatibilidad y conexión de su tecnología con el Sistema de Intervención y Control de las Comunicaciones de la Policía Nacional del Perú. Asimismo, cuando por razones de innovación tecnológica los concesionarios renueven sus equipos o software, se encontrarán obligados a mantener la compatibilidad con el Sistema de Intervención y Control de las Comunicaciones de la Policía Nacional del Perú.

Artículo 235. Levantamiento del secreto bancario

(...)

5. Las empresas o entidades requeridas con la orden judicial deberán proporcionar, en el plazo máximo de treinta días hábiles, la información correspondiente o las actas y documentos, incluso su original, si así se ordena, y todo otro vínculo al proceso que determine por razón de su actividad, bajo apercibimiento de las responsabilidades establecidas en la ley. El juez fija el plazo en atención a las características, complejidad y circunstancias del caso en particular.

Artículo 473. Ámbito del proceso y competencia

1. Los delitos que pueden ser objeto de acuerdo, sin perjuicio de los que establezca la Ley, son los siguientes:

PERÚ Presidencia del Consejo de Ministros | Autoridad Nacional del Servicio Civil | servir HERRAMIENTA DEL PERÚ QUE CRECE

COMUNICADO
N° 001-2013-SERVIR/GDCRSC
PRESENTACIÓN DEL PDP ANUALIZADO 2014

El Plan de Desarrollo de Personas (PDP) es una herramienta de gestión que promueve el desarrollo de las capacidades del personal al servicio del Estado, asegurando la pertinencia, transparencia, mérito y eficiencia en el uso de los recursos públicos, con la finalidad de promover el logro de los objetivos estratégicos de la entidad y brindar un servicio de calidad al ciudadano.

En tal sentido, la elaboración y presentación del PDP Anualizado 2014 ante SERVIR es fundamental y obligatoria para las entidades públicas del Gobierno Nacional, Gobierno Regional y Gobierno Local Provincial, según lo señala el **Decreto Supremo Nº 009-2010-PCM, siendo el plazo máximo de presentación el 30 de enero del 2014.** SERVIR viene publicando la relación del cumplimiento de la presentación de los PDP en su página web: **www.servir.gob.pe/pdp**, y la actualiza de manera mensual.

SERVIR tiene previsto el desarrollo de capacitaciones en Lima y en el interior del país para las entidades que lo soliciten. Para poder participar será necesario que las entidades se comuniquen al correo **pdp@servir.gob.pe**, o llamen al teléfono 206-3370, anexo: 3349 manifestando su interés en participar. **Las solicitudes se registrarán hasta el 31 de octubre del 2013.**

Para mayor información puede comunicarse con nosotros al teléfono 206-3370, anexo: 3349 y al correo electrónico señalado anteriormente.

Gerencia de Desarrollo de Capacidades y Rendimiento del Servicio Civil

PERÚ PROGRESO PARA TODOS

a) Asociación ilícita, terrorismo, lavado de activos, delitos informáticos, contra la humanidad;"

CUARTA. Modificación de los artículos 162, 183-A y 323 del Código Penal

Modifícanse los artículos 162, 183-A y 323 del Código Penal, aprobado por el Decreto Legislativo 635, en los siguientes términos:

"**Artículo 162. Interferencia telefónica**
El que, indebidamente, interfiere o escucha una conversación telefónica o similar será reprimido con pena privativa de libertad no menor de tres ni mayor de seis años.
Si el agente es funcionario público, la pena privativa de libertad será no menor de cuatro ni mayor de ocho años e inhabilitación conforme al artículo 36, incisos 1, 2 y 4.
La pena privativa de libertad será no menor de cinco ni mayor de ocho años cuando el delito recaiga sobre información clasificada como secreta, reservada o confidencial de conformidad con las normas de la materia.
La pena privativa de libertad será no menor de ocho ni mayor de diez años cuando el delito comprometa la defensa, la seguridad o la soberanía nacionales.

Artículo 183-A. Pornografía infantil
El que posee, promueve, fabrica, distribuye, exhibe, ofrece, comercializa o publica, importa o exporta por cualquier medio objetos, libros, escritos, imágenes, videos o audios, o realiza espectáculos en vivo de carácter pornográfico, en los cuales se utilice a personas de catorce y menos de dieciocho años de edad, será sancionado con pena privativa de libertad no menor de seis ni mayor de diez años y con ciento veinte a trescientos sesenta y cinco días multa.
La pena privativa de libertad será no menor de diez ni mayor de doce años y de cincuenta a trescientos sesenta y cinco días multa cuando:

1. El menor tenga menos de catorce años de edad.
2. El material pornográfico se difunda a través de las tecnologías de la información o de la comunicación.

Si la víctima se encuentra en alguna de las condiciones previstas en el último párrafo del artículo 173 o si el agente actúa en calidad de integrante de una organización dedicada a la pornografía infantil, la pena privativa de libertad será no menor de doce ni mayor de quince años.
De ser el caso, el agente será inhabilitado conforme a los numerales 1, 2 y 4 del artículo 36.

Artículo 323. Discriminación
El que, por sí o mediante terceros, discrimina a una o más personas o grupo de personas, o incita o promueve en forma pública actos discriminatorios, por motivo racial, religioso, sexual, de factor genético, filiación, edad, discapacidad, idioma, identidad étnica y cultural, indumentaria, opinión política o de cualquier índole, o condición económica, con el objeto de anular o menoscabar el reconocimiento, goce o ejercicio de los derechos de la persona, será reprimido con pena privativa de libertad no menor de dos años ni mayor de tres o con prestación de servicios a la comunidad de sesenta a ciento veinte jornadas.
Si el agente es funcionario o servidor público, la pena será no menor de dos ni mayor de cuatro años e inhabilitación conforme al numeral 2 del artículo 36.
La misma pena privativa de libertad señalada en el párrafo anterior se impondrá si la discriminación se ha materializado mediante actos de violencia física o mental, o si se realiza a través de las tecnologías de la información o de la comunicación."

DISPOSICIÓN COMPLEMENTARIA DEROGATORIA

ÚNICA. Derogatoria

Deróganse el numeral 3 del segundo párrafo del artículo 186 y los artículos 207-A, 207-B, 207-C y 207-D del Código Penal.

Comuníquese al señor Presidente Constitucional de la República para su promulgación.

En Lima, a los veintisiete días del mes de setiembre de dos mil trece.

FREDY OTÁROLA PEÑARANDA
Presidente del Congreso de la República

MARÍA DEL CARMEN OMONTE DURAND
Primera Vicepresidenta del Congreso de la República

AL SEÑOR PRESIDENTE CONSTITUCIONAL DE LA REPÚBLICA

POR TANTO:

Mando se publique y cumpla.

Dado en la Casa de Gobierno, en Lima, a los veintiún días del mes de octubre del año dos mil trece.

OLLANTA HUMALA TASSO
Presidente Constitucional de la República

JUAN F. JIMÉNEZ MAYOR
Presidente del Consejo de Ministros

1003117-1

PODER EJECUTIVO

PRESIDENCIA DEL CONSEJO DE MINISTROS

Crean Comisión Multisectorial encargada de elaborar la propuesta de Estrategia de Saneamiento de la Pequeña Minería y de la Minería Artesanal

RESOLUCIÓN SUPREMA Nº 340-2013-PCM

Lima, 21 de octubre de 2013

CONSIDERANDO:

Que, mediante Decreto Supremo N° 032-2013-EM se establecen los mecanismos encaminados a continuar y fortalecer el proceso de formalización de la pequeña minería y minería artesanal a que se refiere el Decreto Legislativo N° 1105 y Decreto Supremo N° 006-2012-EM;

Que, la Segunda Disposición Complementaria, Transitoria y Final del Decreto Supremo N° 032-2013-EM, dispone que mediante Resolución Suprema se creará una Comisión a cargo de elaborar la propuesta de Estrategia de Saneamiento de la Pequeña Minería y de la Minería Artesanal, que deberá reportar sus actividades a la Comisión Permanente de Seguimiento de las Acciones del Gobierno frente a la Minería Ilegal y del Desarrollo del proceso de formalización conformada por Decreto Supremo N° 075-2012-PCM, modificado por el Decreto Supremo N° 076-2013-PCM;

Que, en tal razón, es necesaria la creación de una Comisión Multisectorial de naturaleza temporal con el objeto de elaborar la propuesta de Estrategia de Saneamiento de la Pequeña Minería y de la Minería Artesanal, en el marco de lo previsto en el numeral 2 del artículo 36° de la Ley Nº 29158 - Ley Orgánica del Poder Ejecutivo, el cual dispone que toda Comisión Multisectorial de carácter temporal se crea formalmente mediante resolución suprema refrendada por el Presidente del Consejo de Ministros y los titulares de los sectores involucrados;

Estando a lo expuesto y de conformidad con lo previsto en el numeral 8 del artículo 118° de la Constitución Política del Perú; la Ley Nº 29158 - Ley Orgánica del

DELITOS INFORMÁTICOS EN LA LEY 30096 Y LA

MODIFICACIÓN DE LA LEY 30071.

Por: prof. Dr. Dr. h. c. Felipe Villavicencio Terreros[1]

PALABRAS CLAVES: *Tic, Cibergobierno, Cibereducacion, Cibersalud, Pishing, Ciberdelincuente, Hackers, Crackers, Sabotaje Informático, Bomba Lógica, Rutinas De Cancer, Gusanos, Malware, Browser, Cookie, Dialup, Digital Signature.*

RESUMEN: *En los últimos tiempos, producto del desarrollo de las tecnologías informáticas se ha ido desarrollando una nueva forma de criminalidad denominada delitos informativos.*

---

[1] *Profesor de derecho penal y criminología. Abogado por la Universidad Nacional Mayor de San Marcos. Doctor por la Universidad de Buenos Aires. Doctor Honoris Causa por la Universidad Nacional de Piura. Miembro del Subcomité de Naciones Unidas para la Prevención de la Tortura (SPT). Este trabajo ha sido posible gracias a la colaboración de mi alumno* ***Vilmer De la Cruz Paulino.***

En relación a esta nueva forma delictiva, en el Perú se ha emitido una Ley penal especial cuya finalidad es prevenir y sancionar las conductas ilícitas que afectan los sistemas y datas informáticos, así como los secreto de comunicaciones, y los demás bienes jurídicos que resulte afectado con esta modalidad delictiva como son el patrimonio, la fe pública y la libertad sexual. La Ley N° 30096 "Ley de delitos informativos" fue promulgada el 21 y publicado el 22 de octubre del 2013 en el diario oficial "El Peruano". Luego fue parcialmente modificada por la Ley N° 30171 "Ley que modifica la Ley 30096, Ley de delitos informativos", promulgada el 9 y publicada el 10 de marzo del 2014.

I. CONSIDERACIONES GENERALES

1. INTRODUCCION

El proceso de integración cultural, económica y social a nivel mundial, conocido como *"globalización",* viene acompañado del gran desarrollo de la tecnología de la Información y comunicación (en adelante TIC) y la masificación de la misma, viene jugando un papel importante en el desarrollo cultural. Las nuevas herramientas que ofrecen las TIC al servicio del hombre están relacionadas con la *transmisión, procesamiento y almacenamiento* digitalizado de información, así como un conjunto de procesos y productos que simplifican la comunicación y hacen más viables la interacción entre las personas. Un aporte tecnológico que reforzó el poder de las TIC es, sin lugar a dudas, el internet (*vgr*. *messenger*, *correo electrónico, facebook, twitter, web*). Este nuevo descubrimiento superó el paradigma real del tiempo-espacio en la interacción humana en tanto la comunicación se podía dar en tiempo real sin importar la distancia. Por otra parte, las aplicaciones de las TIC a partir de internet, entre ellos *"cibergobierno", "cibereducacion"* y *"cibersalud"* se consideran elementos habilitantes para el desarrollo social puesto que proporcionan un canal eficaz para distribuir una amplia gama de servicios básicos en zonas remotas y rurales, pues estas aplicaciones facilitan el logro de los objetivos de desarrollo prospectivo, mejoras en las condiciones sanitarias y medioambientales.

Si bien los diversos ámbitos de interacción se ven favorecidos por la fluidez que le brinda esta nueva alternativa tecnológica, no obstante, se incrementan los riesgos relacionados a las tecnologías informáticas y de comunicación[2]. El desarrollo de la tecnología también ha traído consigo nuevas formas delictuales que tienen por medio y/o finalidad los sistemas informáticos e internet.

Las principales características de vulnerabilidad que presenta el mundo informático son las siguientes:

[2] AROCENA, Gustavo A.; "La regulación de los delitos informativos en el código penal argentino. Introducción a la ley nacional N° 26.388", **en** Boletín Mexicano de Derecho Comparado, nueva serie, año XLV, N° 135, México 2012, pág. 945- 988.

a. La falta de jerarquía en la red, que permite establecer sistemas de control, lo que dificulta la verificación de la información que circula por este medio.
b. El creciente número de usuarios, y la facilidad de acceso al medio tecnológico.
c. El anonimato de los cibernautas que dificulta su persecución tras la comisión de un delito a través de este medio.
d. La facilidad de acceso a la información para alterar datos, destruir sistemas informáticos.

Otro factor determinante es la rápida difusión de información a través de este medio tecnológico a muy bajo costo que permite a las organizaciones delictivas perpetrar delitos con mayor facilidad.[3]

Es necesario mencionar que el hecho de criminalizar algunas conductas desplegadas en el mundo informático, no implica desconocer las ventajas y facilidades brindadas por estos sistemas. Son evidentes los beneficios de los adelantos tecnológicos que trae para la sociedad el uso de la tecnología informática y comunicación. Sin embargo, como lo expresa el informe del *12º Congreso de las Naciones Unidas sobre Prevención del Delito y Justicia Penal*[4], estos adelantos tecnológicos posibilitan una nueva modalidad de cometer los delitos tradicionales como el fraude y la distribución de pornografía infantil y a su vez facilita la comisión de nuevos delitos como la penetración en redes informáticas, el envío de correo basura, la pesca de los datos *"pishing",* la piratería digital, la propagación maliciosa de virus y otros ataques contra las infraestructuras de información esenciales.

Antes de empezar a analizar la *Ley de Delitos Informáticos*, es necesario mencionar que esta Ley tiene como fuente directa la COMJIB[5] (*Bases para la elaboración de un instrumento internacional en materia de cibercriminalidad*) y el Convenio sobre la ciberdelincuencia – Budapest.

2. LOS DELITOS INFORMÁTICOS: *CONCEPTO Y MODALIDADES*

Los delitos informáticos[6] se vinculan con la idea de la comisión del crimen a través del empleo de la computadora, internet, etc.; sin embargo esta forma de criminalidad no solo

[3] Vide: CARNEVALI RODRÍGUEZ, Raúl; "La criminalidad organizada. Una aproximación al derecho penal italiano, en particular la responsabilidad de las personas jurídicas y la confiscación", Vol. 16, Ius Et Praxis Nº 2, Talca, 2010, pág. 273.

[4] Vide: Informe del 12º Congreso de las Naciones Unidas sobre Prevención del Delito y Justicia Penal, pág. 61.

[5] COMJIB "Conferencia de Ministros de Justicia de los Países Iberoamericanos".

[6] Debido al desarrollo de la tecnología y entre ellos la computadora, y dado la nueva forma de comisión de delitos a través de las tecnologías es que se ha optado por denominar indistintamente a este tipo de delitos como "delito de abuso de computadoras", "delitos bajo la influencia de la computadora", "criminalidad de la información y la comunicación", "criminalidad de internet", "criminalidad multimedia", y en el Perú se denomina "delitos informáticos". Todo estas denominación identifican de manera general la problemática de la delincuencia mediante las computadoras y el empleo de las comunicaciones; sin embargo, para efectos didáctico en la doctrina se prefiere la

se comete a través de estos medios, pues éstos son solo instrumentos que facilitan pero no determinan la comisión de estos delitos. Esta denominación, es poco usada en las legislaciones penales; no obstante bajo ella se describe una nueva forma de criminalidad desarrollada a partir del elevado uso de la tecnología informática[7].

Para Mühlen, el delito informático ha de comprender todo comportamiento delictivo en el que la computadora es el instrumento o el objetivo del hecho[8]. En similar sentido Dannecker concibe el delito informativo como aquella forma de criminalidad que se encuentra directa o indirectamente en relación con el procesamiento electrónico de datos y se comete con la presencia de un equipo de procesamiento electrónico de datos.

Por nuestra parte, entendemos a la criminalidad informática como aquellas conductas dirigidas a burlar los sistemas de dispositivos de seguridad, esto es invasiones a computadoras, correos o sistemas de datas mediante una clave de acceso; conductas típicas que únicamente pueden ser cometidos a través de la tecnología. En un sentido amplio, comprende a todas aquellas conductas en las que las TIC son el objetivo, el medio o el lugar de ejecución, aunque afecten a bienes jurídicos diversos y que plantea problemas criminológicos y penales, originados por las características propias del lugar de comisión[9].

De la concepción de los delitos informáticos, se entiende que no todo delito puede ser clasificado como delito informático por el solo hecho de haber empleado la computadora u otro instrumento tecnológico. Es necesario determinar que conductas pueden ser clasificados como delitos informáticos y cuales no, a pesar de su vinculación con una computadora, un procesador de datos o la red de información. Al respecto, uno de los criterios a utilizar sería que un delito para ser clasificado dentro de los delitos informáticos no sea posible de realizarse sin la intervención de la informática, porque es el medio informático lo que va caracterizar este delito[10]; *vgr. el difamar a una persona a través de los medios de comunicación sea correo electrónico,facebook y/o twitter, no puede constituirse como un delito informático, por el solo hecho de emplear la tecnología informática como medio; porque este delito puede realizarse a través de otros medios como son verbal, escrito, etc. Sin embargo, los delitos de ingresar sin autorización a un sistema de datos, sabotear la base de datos si se clasifican dentro de los delitos informativos porque no es posible la comisión de estos delito sin la intervención de la informática.*

Respecto de los delitos informativos, Krutisch citado por Mazuelos, identifica tres tipos de categorías: *manipulación informática, sabotaje informático* y *acceso no autorizado a datos*

---

denominación de "*delitos informáticos*" para identificar la criminalidad vinculada a la tecnología**;** *Vide.* MAZUELOS COELLO, Julio F.; "Modelos de imputación en el derecho penal informático", pág. 40.

[7] MAZUELOS COELLO, Julio F.; óp., cit., pág. 40.

[8] Mühlen **citado por¸** Mazuelos Coello, Julio F.; "Modelos de imputación en el derecho penal informático", óp., cit., pág. 41.

[9] MIRÓ LINARES, Francisco; "El cibercrimen. Fenomenología y criminología de la delincuencia en el ciberespacio", Marcial Pons, Madrid, 2012, pág. 44.

[10] Vide. MAZUELOS COELLO, Julio F.; "Delitos informativos: una aproximación a la regulación del Código Penal peruano", en RPDJP N° 2, Lima, 2001, pág. 253 y ss.

o sistema computarizados[11]*;* pero no son categorías de delitos, sino modos de cometer los delitos informativos.

3. ANTECEDENTES DE LOS DELITOS INFORMÁTICOS

El delito informático, en un inicio se encontraba tipificado en el Art. 186° inc. 3, segundo párrafo del Código Penal de 1991. Esta regulación no era propia de un delito autónomo, sino como una agravante del delito de hurto[12]. En la actualidad, los delitos informáticos están previstos en el Capítulo X[13] del CP: los artículos 207°-A *(interferencia, acceso o copia ilícita contenida en base de datos),* 207°-B *(alteración, daño o destrucción de base de datos),* 207°-C *(circunstancias cualificantes agravantes),* 207°-D (*tráfico ilegal de datos),* y en las leyes penales especiales.

Entre estas leyes penales especiales, se encuentra la Ley Nº 30096[14] "*Ley de Delitos Informáticos".* Esta Ley de Delitos Informáticos está conformado por siete capítulos que se estructuran de la siguiente manera: *finalidad y objeto de la ley* (Cap. I), *delitos contra datos y sistemas informáticos* (Cap. II), *delitos informáticos contra la indemnidad y libertad sexual* (Cap. III), *delitos informáticos contra la in*timidad *y el secreto de las comunicaciones* (Cap. IV), *delitos informáticos contra el patrimonio* (Cap. V), *delitos informáticos contra la fe pública* (Cap. VI), *disposiciones comunes* (Cap. VII).

Posteriormente, se promulgo la Ley N° 30171[15] *"Ley que modifica la Ley N° 30096, Ley de Delitos Informáticos".* La finalidad de esta ley fue adecuar la Ley N° 30096 a los estándares legales del Convenio Sobre la Cibercriminalidad (en adelante convenio de Budapest), al incorporar en la redacción típica de los artículos 2, 3, 4, 7, 8 y 10, de la referida Ley la posibilidad de cometer el delito *deliberada e ilegítimamente*. Las modificaciones de la Ley Nº 30171, con respecto a los delitos informáticos, consisten en las siguiente:

- **Art. 1°.-** Modificación de los artículos 2°, 3°, 4°, 5°, 7°, 8° y 10° de la *Ley N° 30096 Ley de Delitos Informáticos*.
- **Art. 2°.-** Modificación de la tercera, cuarta y undécima disposiciones complementarias finales de la *Ley N° 30096 Ley de Delitos Informáticos*.
- **Art. 3°.-** Incorporación del artículo 12° a la *Ley N° 30096 Ley de Delitos Informáticos*.
- **Art. 4°.-** Modificación de los artículos 158°, 162° y 323° del Código Penal.

---

[11] KRUTISCH citado por MAZUELOS COELLO, Julio F.; óp., cit., pág. 40.

[12]BRAMONT- ARIAS TORRES, Luis A.; "Delitos informáticos", **en** Revista Peruana de Derecho de la Empresa, DERECHO INFORMATICO Y TELEINFORMATICA JURIDICA, Nº 51, ASESORANDINA. Lima 2000.

[13] Capitulo incorporado por la Ley Nº 27309, publicado el 17/07/2000.

[14] Publicado el 22 octubre 2013. Esta Ley tiene su origen en el PROYECTO DE LEY N° 34/ 2011-CR, presentado al congreso el 11 de agosto del 2011.

[15]Publicado el 10 de marzo 2014. Esta Ley tiene su origen en el PROYECTO DE LEY N° 2991/ 2013-CR, presentado al congreso el 25 de noviembre del 2011.

- **Art. 5°.-** Incorporación de los artículos 154°-A y 183°-B del Código Penal.
- **Única Disposición Complementaria Derogatoria**.- deroga el artículo 6° de la *Ley N° 30096 Ley de Delitos Informáticos.*

4. FINALIDAD Y OBJETO DE LA LEY

El Art. 1º de la Ley de delitos informáticos establece que la finalidad de la ley es prevenir y sancionar las conductas ilícitas que afectan los sistemas, las datas informáticos, el secreto de las comunicaciones; y otros bienes jurídicos de relevancia penal -*patrimonio, la fe pública y la libertad sexual, etc.*- que puedan ser afectados mediante la utilización de las TIC, con la finalidad de garantizar las condiciones mínimas para que las personas gocen del derecho a la libertad y desarrollo. Con esta Ley, se intenta garantizar la lucha eficaz contra la ciberdelincuencia.

Esta Ley no responde políticocriminalmente a la necesidad de ejercer la función punitiva del Estado enfocada en la protección de la información, sino, tiene como principal objetivo la estandarización de la ley penal peruana con el ordenamiento penal internacional, principalmente por la Convenio contra la cibercriminalidad del Consejo Europeo (CETS 185), denominado Convenio de Budapest[16].

5. BIEN JURÍDICO TUTELADO

El bien jurídico tutelado en los delitos informáticos se concibe en los planos de manera conjunta y concatenada; en el primero se encuentra la "información" de manera general *(información almacenada, tratada y transmitida mediante los sistemas de tratamiento automatizado de datos*), y en el segundo, los demás bienes afectados a través de este tipo de delitos como son la *indemnidad sexual, intimidad, etc*. Respecto de la información, debe ser entendida como el contenido de las bases y/o banco de datas o el producto de los procesos informáticos automatizados*;* por lo tanto se constituye en un bien autónomo de *valor económico* y es la importancia del "valor económico" de la información lo que ha hecho que se incorpore como bien jurídico tutelado[17].

Sin embargo, creemos que la información se debe considerar de diferentes formas, y no solo como un valor económico, sino como un valor intrínseco de la persona por la fluidez y el trafico jurídico, y por los sistemas que lo procesan o automatizan los mismos que

[16] *Vide.* Ley Nº 30096 "*Ley de delitos informáticos*", octava disposición complementaria: "*El Estado peruano promoverá la firma y ratificación de convenios multilaterales que garanticen la cooperación mutua con otros Estados para la persecución de los delitos informáticos".*

[17] Cfr. GUTIERREZ FRANCES, "Atentados contra la información como valor económico de empresa" Mazuelos Coello/REYNA ALFARO, "Delitos informático"/DURAND VALLADARES, "Los delitos informáticos en el Código Penal Peruano" URQUIZO OLAECHEA, Revista Peruana de Ciencias Penales. N° 11, Lima 2002.

equiparan a los bienes protegidos tradicionales tales como el patrimonio (*fraude informático*), la reserva, la intimidad y confidencialidad de los datos (*agresiones informáticas a la esfera de la intimidad*), seguridad o fiabilidad del trafico jurídico probatorio (*falsificación de datos o documentos probatorios*), etc.

Por tanto, en este tipo de delitos no se puede establecer a la información como el único bien jurídico afectado, por ser el principal y el más importante; sino a un conjunto de bienes que son afectados[18], debido a la característica de la conducta típica en esta modalidad delictiva que colisiona con diversos intereses colectivos. Es en ese sentido que coincidimos con María Luz Gutiérrez Francés quien señala que es un delito pluriofensivo[19] sin perjuicio que uno de tales bienes este independientemente tutelado por otro tipo penal[20].

6. PERFIL DEL CIBERDELINCUENTE.

El perfil del ciberdelincuente -*sujeto activo*- en esta modalidad delictual requiere ciertas habilidades y conocimientos en el manejo del sistema informático[21], por ello también se les ha calificado como delincuentes de "*cuello blanco*"[22], que tienen como características:

- Poseer importantes conocimientos informáticos.
- Ocupar lugares estratégicos en su centro laboral, en los que se maneja información de carácter sensible (*se denomina delitos ocupacionales, ya que se comenten por la ocupación que se tiene y el acceso al sistema*).

Para Marcelo Manson, los infractores de la Ley penal en materia de Delitos Informáticos no son delincuentes comunes y corrientes sino que por el contrario, son personas especializadas en la materia informática.[23] Agrega que "*las personas que cometen los delitos informáticos son aquellas que poseen ciertas características que no presentan el denominador común, esto es habilidades para el manejo de los sistemas informáticos y que*

---

[18] GONZÁLES DE CHAVES CALAMITA, María E.; "El llamado ´delito informático´", **en** Anales de la Facultad de Derecho de la Universidad de la Laguna N° 21, España, 2004, pág. 44 – 65.

[19] GUTIERREZ FRANCES, María; "Fraude Informático y estafa" Centro de Publicaciones del Ministerio de Justicia, Madrid 1991.

[20]Por la ubicación sistemática de estos delitos dentro del código penal de 1991 y antes de la dación de la Ley penal especial Nº 30096, el bien jurídico considerado era el patrimonio *por las conductas dirigidas a dañar, alterar o destruir una base de datos. Vide*. GALVEZ VILLEGAS, Tomas/ DELGADO TOVAR, Walter; "Derecho Penal Parte Especial", T III, Jurista Editores, Lima 2002, pág.1207.

[21] AZAOLA CALDERON, Luis; "Delitos informáticos y Derecho penal", UBIJUS, México 2010, pág. 27.

[22]"Se le denomina así a la delincuencia informática debido a los estudios sobre criminalidad informática orientados en las manifestaciones en el ámbito económico patrimonial, donde la doctrina determino que el sujeto activo del delito informático poseída un alto nivel socioeconómico", en AZAOLA CALDERON, Luis; "Delitos informáticos y Derecho penal", óp., cit., pág. 27- 28.

[23]MANSON, Marcelo; "Legislación sobre delitos informáticos", **en** https://dl.dropbox.com/u//dl.legislacioncomparada.pdf. [visto el 27 de diciembre 2013].

por su situación laboran en puestos estratégicos donde se manejan información sensible."Por su parte, Camacho Losa considera que el perfil de estas personas no coincide con el de un delincuente marginal y caracteriza a los autores de estas infracciones como empleados de confianza de las empresas afectadas.[24] Tambien, Vives Antón y Gonzales Cussac afirman que "sujeto activo puede ser tanto las personas legítimamente autorizadas para acceder y operar el sistema (*operadores, programadores u otros*), como terceros no autorizados que acceden a las terminales públicas o privadas"[25]

Gutiérrez Francés y Ruiz Vadillo difieren de estos puntos de vista y sostienen que "*el autor del delito informático puede serlo cualquiera, no precisando el mismo de determinados requisitos personales o conocimientos técnicos cualificados*"[26]. Por nuestra parte, si bien consideramos que el sujeto activo puede ser cualquier persona (*con conocimientos y habilidades en informática*) y compartimos parcialmente la postura que el sujeto activo debe ocupar un puesto laboral que le permita acceder a información sensible, sin embargo, no están excluidos los sujetos que sin ocupar algún cargo estratégico pueden ser sujeto activo por sus habilidades y conocimientos sobre la informática. Por ende, se trata de **delitos de dominio**.

Se pueden identificar diferentes sujetos activos que se les denomina de diferente manera dependiendo del modo como actúan y que conductas son las que realizan:

HACKERS.- Son personas dedicadas, por afición u otro interés, a violar programas y sistemas supuestamente impenetrables, conocido como "*delincuente silencioso o tecnológico*". Les gusta indagar por todas partes, conocer el funcionamiento de los sistemas informáticos; son personas que realizan esta actividad como reto intelectual, sin producir daño alguno con la única finalidad de descifrar y conocer los sistemas informáticos. Para Sieber los hacker son "*personas que acceden sin autorización a un sistema de proceso de datos a través de un proceso de datos a distancia, no cometido con finalidades manipuladoras, fraudulentas, de espionaje, ni sabotaje, sino sencillamente como paseo por placer no autorizado*"[27]. Morón Lerma define a los hacker como *"personas que acceden o interfieren sin autorización, de forma subrepticia, a un sistema informático o redes de comunicación electrónica de datos y utilizan los mismos sin autorización o más allá de lo autorizado"*[28]

[24] CAMACHO LOSA, L; "El delito informático" GRAFICAS CONDOR, Madrid 1987, pág. 83- 84.
[25] VIVES ANTÓN y GONZÁLES CUSSAC, "Comentarios al código Penal 1995", Ed. TIRONT BLANCH, Valencia 1996, pág. 1238.
[26]GUTIERRES FRANCES, M; "Fraude informático y estafa"/ RUIZ VADILLO, E; "tratamiento a la delincuencia informática", en AZAOLA CALDERON, Luis; "Delitos informáticos y Derecho penal", óp., cit., pág. 29.
[27] SIEBER, Ulrich: "Criminalidad informática: peligro y prevención", pág. 77, MIR PUIG, S; "Delincuencia informática".
[28] MORON LERMA, ESTHER; "Internet y Derecho Penal: hacking y otras conductas ilícitas en la red", ED. ARANZADI, Navarra, 2002, 2° ed., pág. 51.

CRACKERS.- Son personas que se introducen en sistemas remotos con la intención de destruir datos, denegar el servicio a usuarios legítimos, y en general a causar problemas a los sistemas, procesadores o redes informáticas, conocidos como “piratas electrónicos.” La característica que los diferencia de los hacker es que los crackers usan programas ya creados que pueden adquirir, normalmente vía internet; mientras que los hackers crean sus propios programas, tiene mucho conocimiento sobre los programas y conocen muy bien los lenguajes informáticos[29].Por otra parte, Morant Vidal define a estos sujetos como “*personas que se introducen en sistemas remotos con la intención de destruir datos, denegar el servicio a usuarios legítimos, y en general a causar problemas*”[30]. También, Alfonso Laso sostiene que el cracker “*es la persona que, de manera intencionada, se dedica a eliminar o borrar ficheros, a romper los sistemas informáticos, a introducir virus, etc.*”[31].

7. LA SITUACIÓN DE LAS PERSONAS JURIDICAS COMO SUJETO ACTIVO Y SUJETO PASIVO.

6.1. SUJETO ACTIVO

Dada la vigencia del principio *Societas delinquere non potest*, en el derecho penal nacional no se puede considerar a la persona jurídica como sujeto activo. Sin embargo, se cuentan con las figuras de las Consecuencias Accesorias (art. 105 CP), el actuar por otro (art. 27 CP) y reglas procesales en el Código Procesal Penal del 2004, cuando se trata de delitos cometidos a través de las personas jurídicas y además, el Acuerdo Plenario N° 7-2009/CJ-116 : Personas Jurídicas y Consecuencias Accesorias.

Sin embargo, la ley de delitos informáticos regula dos supuestos de carácter administrativos donde la persona jurídica se niega a brindar información sobre el levantamiento del secreto bancario (*Decima disposición complementaria final*) y cuando se niega a brindar información referente a los registros de comunicaciones telefónicas (*Undécima disposición complementaria final*), cuando así lo solicite a través de una orden judicial; a consecuencia de esto la SBS y OPSITEL respectivamente les aplicaran una sanción administrativa consistente en un multa.

6.2. SUJETO PASIVO

[29]AZAOLA CALDERON, Luis; óp., cit., pág. 32.

[30] MORANT VIDAL, J; “protección penal de la intimidad frente a las nuevas tecnologías”, Ed. PRACTICA DE DERECHO, Valencia, 2002, pág. 44.

[31]DE ALFONSO LASO, D; “El hackerin blanco. Una conducta ¿punible o impune?”, en Internet y derecho penal, Cuadernos de Derecho Judicial, Consejo General del poder Judicial, Madrid, 2001, pág.110- 111.

La persona jurídica sí puede ser considerada como sujeto pasivo, como por ejemplo, empresas públicas y privadas (*bancos, instituciones públicas, industrias, seguros, etc.*), aunque en ciertos casos, estas personas jurídicas no denuncien los delitos del que son víctimas por cierto temor al desprestigio o al impacto entre sus clientes y consecuentes efectos económicos desfavorables.

Además, esta ley menciona dos supuestos en donde la persona jurídica es sujeto pasivo de los delitos informáticos, el Art. 6° "*Tráfico ilegal de datos, que consiste en crear, ingresar o utilizar indebidamente una base de datos sobre una persona natural o* ***jurídica***", y el Art. 9° "*Suplantación de identidad, él que mediante las TIC suplanta la identidad de una persona natural o* ***jurídica****".*

Gutiérrez Francés señala que el sujeto pasivo por excelencia del ilícito informático es la persona jurídica[32] , debido al tráfico económico en el que desarrollan sus aactividades, por ello son los sectores más afectados por la criminalidad mediante computadoras, y entre ellos están: la banca, las instituciones públicas, industria de transformación, etc.

II. DE LOS DELITOS INFORMÁTICOS EN LA LEY N° 30096

1. DELITOS CONTRA DATOS Y SISTEMAS INFORMÁTICOS (CAP. II)

Este capítulo está conformado por las siguientes figuras penales: **Art. 2º** (*acceso ilícito*), **Art. 3º** (*atentando a la integridad de datos informáticos*) y **Art. 4º** (*atentando a la integridad de sistemas informáticos*).

> *Art. 2º.-* "*El que deliberada e ilegítimamente accede a todo o parte de un sistema informático, siempre que se realice con vulneración de medidas de seguridad establecidas para impedirlo, será reprimido con pena privativa de libertad no menor de uno ni mayor de cuatro años y con treinta a noventa días-multa.*
>
> *Será reprimido con la misma pena el que accede a un sistema informático excediendo lo autorizado*".

Esta figura penal de *Acceso ilícito* sanciona la violación de la confidencialidad, que se realiza a través del acceso no autorizado al sistema, vulnerando las medidas de seguridad

[32] GUTIÉRREZ FRANCES, M; "Fraude informático y estafa", Ministerio de Justicia, Madrid, 1991, pág. 76.

establecida para evitar que ajenos ingresen a un sistema informático[33]; el verbo rector "***acceder"*** se entiende el hecho de entrar en un lugar o pasar a él, que en esta figura se entiende el acto de entrar sin autorización del titular a un sistema, y el término ***"vulnerar"*** se entiende como *"transgredir, quebrantar, violar una ley o precepto"*[34] que se entiende al hecho de trasgredir las barreras de protección diseñados por el sistema.[35]

Por la característica que presenta este tipo penal -*acceso ilícito*- se le puede calificar como un *delito de mera actividad*, porque esta figura exige el acto de acceder *(entrar en un lugar o pasar a él)* sin autorización a un sistema informático, vulnerar *(transgredir, quebrantar, violar una ley o precepto)* las medidas de seguridad, de esta manera se configura el ilícito; por tanto el delito queda consumado en el momento que se vulnera las medidas de seguridad establecida para impedir el acceso ilícito, y para ellos es necesario que se realice esta conducta con dolo. *Vgr. el acceso a la cuenta de correo electrónico ajeno protegido mediante una contraseña de seguridad, el acceso no autorizado al sistema informático de una entidad aprovechando las debilidades inadvertidas por la programación*.

La fuente legal de este artículo es el Convenio de Budapest, porque cumple con describir la acción delictiva en los mismos términos estandarizados de la norma internacional: por mencionar los términos "*deliberación*", "*falta de legitimación*"[36] de la acción contenida en el texto del Convenio de Budapest guarda cierta identidad con el dolo (conocimiento y voluntad).[37]

> *Art. 3º.-* "*El que deliberada e ilegítimamente daña, introduce, borra, deteriora, altera, suprime o hace inaccesible datos informáticos, será reprimido con pena privativa de libertad no menor de tres ni mayor de seis años y con ochenta a ciento veinte días multa*".

---

[33] Diccionario de la Real Academia Española http://lema.rae.es/drae/?val=acceder [visto el 28 de marzo 2014].

[34] Diccionario de la Real Academia Española http://lema.rae.es/drae/?val=vulnerar [visto el 28 de marzo 2014].

[35] STERN, Enrique; "El sentido de la privacidad, la intimidad y la seguridad en el mundo digital: ámbito y límites", REVISTA EGUZKILORE Nº 21, pág. 187.

[36] Ver Convenio sobre la ciberdelincuencia – Budapest, 23.XI.2001: Cap. II, sección 1º, titulo 1º, Art. 2º.- Acceso ilícito.

[37] VILLAVICENCIO TERREROS, Felipe, "Derecho Penal- Parte general", Ed. Grijley, Lima, 2013, pág. 354.

Esta figura penal sanciona la conducta de dañar (causar detrimento, perjuicio, menoscabo)[38], introducir *(entrar en un lugar)*[39], borrar *(desvanecer, quitar, hacer que desaparezca algo)*[40]deteriorar (e*mpeorar, degenerar*)[41], alterar *(estropear, dañar, descomponer)*[42], suprimir *(hacer cesar, hacer desaparecer)*[43] y hacer inaccesible los datos informáticos a través de la utilización de las TIC; por la característica que presenta este tipo penal *–atentado a la integridad de los datos informático-* es clasificado como un *delito de mera actividad,* porque esta figura exige el solo cumplimiento del tipo penal, la sola realización de la conducta de *introducir, borrar, deteriorar, alterar, suprimir y hacer inaccesible* los datos informáticos para que se pueda configurar el ilícito, sin importar el resultado posterior, por tanto el delito queda consumado al realizarse cualquiera de estos actos.

Este artículo es compatible parcialmente con el Art. 4º del Convenio de Budapest[44] que sanciona el atentado contra la integridad y la disponibilidad del dato informático.

> *Art. 4º.- "El que deliberada e ilegítimamente inutiliza, total o parcialmente, un sistema informático, impide el acceso a este, entorpece o imposibilita su funcionamiento o la prestación de sus servicios, será reprimido con pena privativa de la libertad no menor de tres ni mayor de seis años y con ochenta a ciento veinte días-multa".*

Está figura penal sanciona las conductas que están dirigidas a inutilizar *(hacer inútil, vano o nulo algo)*[45] total o parcialmente un sistema informático, entorpecer *(retardar, dificultar)*[46]e

---

[38] Diccionario de la Real Academia Española http://lema.rae.es/drae/?val=dañar [visto el 28 de marzo 2014].

[39]Diccionario de la Real Academia Española http://lema.rae.es/drae/?val=introducir [visto el 28 de marzo 2014].

[40]Diccionario de la Real Academia Española http://lema.rae.es/drae/?val=borrar [visto el 28 de marzo 2014].

[41]Diccionario de la Real Academia Española http://lema.rae.es/drae/?val=deteriorar [visto el 28 de marzo 2014].

[42]Diccionario de la Real Academia Española http://lema.rae.es/drae/?val=alterar [visto el 28 de marzo 2014].

[43]Diccionario de la Real Academia Española http://lema.rae.es/drae/?val=suprimir [visto el 28 de marzo 2014].

[44] Ver Convenio sobre la ciberdelincuencia – Budapest, 23.XI.2001: Cap. II, sección 1º, titulo 1º, Art. 4º.- Ataques a la integridad de los datos.

[45] Diccionario de la Real Academia Española http://lema.rae.es/drae/?val=inutilizar [visto el 28 de marzo 2014].

[46]Diccionario de la Real Academia Española http://lema.rae.es/drae/?val=entorpecer [visto el 28 de marzo 2014].

imposibilitar *(quitar la posibilidad de ejecutar o conseguir algo)*[47]su funcionamiento o la prestación de sus servicios utilizando las TIC; por la característica que presenta este tipo penal –*atentado contra la integridad de sistemas informáticos*- se clasifica como un *delito de resultado,* porque para la configuración de este injusto penal no basta con cumplir el tipo que es *(inutilizar o perturbar)*, sino además es necesario que la acción vaya seguida de un resultado *(impedir el acceso, imposibilitar su funcionamiento, o la prestación de sus servicios),* por tanto el delito se consuma cuando se impide el *acceso, imposibilita su funcionamiento*, *etc.,* del sistema informático, caso contrario el hecho solo dará lugar a la *tentativa.*

Este artículo guarda cierta relación de compatibilidad con el Art. 5º del Convenio de Budapest[48] en tanto se puede entender la "obstaculización grave" de un sistema informático con el de la "inutilización total o parcial" del sistema.

Son ejemplos de esta figura penal los siguientes delitos:

DELITO DE DAÑO.- comportamiento consistente en dañar, destruir o inutilizar un bien, en este caso es el sistema informático, expresa Bramont- Arias que el delito de daños existirá si usuarios, carentes de autorización, alteran o destruyen archivos o bancos de datos a propósito; la destrucción total de programas y de datos ponen en peligro la estabilidad económica de una empresa[49].El *modus operandi* se viene perfeccionando con el tiempo: *virus, cáncer rotudtine*. Estos actos deben causar un perjuicio patrimonial.

EL SABOTAJE INFORMÁTICO.- consiste, básicamente, en *borrar, suprimir o modificar (alterar)* sin autorización funciones o datos de las computadoras con intención de obstaculizar el funcionamiento normal del sistema, que se conoce comúnmente como "virus informático"[50]. Marchena Gómez señala que el "*sabotaje informático es la conducta que consiste en la destrucción o en la producción generalizada de daños*"[51]. Morant Vidal señala que "*el sabotaje informático se dirige a inutilizar los sistemas informáticos causando daños a los programas*"[52].

[47]Diccionario de la Real Academia Española http://lema.rae.es/drae/?val=imposibilitar [visto el 28 de marzo 2014].

[48]Ver Convenio sobre la ciberdelincuencia – Budapest, 23.XI.2001: Cap. II, sección 1º, titulo 1º, Art. 5º.- Ataques a la integridad del sistema.

[49] BRAMONT- ARIAS, Luis A.; "Delitos informáticos", en Revista Peruana de Derecho de la Empresa, DERECHO INFORMATICO Y TELEINFORMATICA JURIDICA, Nº 51, ASESORANDINA. Lima 2000.

[50]AZAOLA CALDERON, Luis; "Delitos informáticos y Derecho penal", UBIJUS, México 2010, pág. 69.

[51] MARCHENA GOMEZ, M; "El sabotaje informático: entre los delitos de daños y desordenes públicos", en Internet y Derecho Penal, Cuadernos de Derecho Judicial, Madrid 2001, pág. 356.

[52] MORANT VIDAL, J; "Protección penal de la intimidad frente a las nuevas tecnologías", Ed. PRACTICA DE DERECHO, Valencia 2003, pág. 46- 47.

Las técnicas que permiten cometer sabotaje informático son las siguientes:[53]

BOMBA LÓGICA.- introducción de un programa de un conjunto de instrucciones indebidas que van a actuar en determinada fecha, destruyendo datos del ordenador, distorsionando el funcionamiento del sistema o paralizando el mismo.

RUTINAS CANCER.- Son distorsiones al funcionamiento del programa, la característica es la auto reproducción.

GUSANOS.- Se infiltran en los programas ya sea para modificar o destruir los datos, pero a diferencia de los virus estos no pueden regenerarse.

VIRUS INFORMATICO Y MALWARE.- Elementos informáticos que destruyen el uso de ciertos antivirus[54]. *Vgr. borrar los antecedentes policiales, judiciales y penales de una persona; alterar la deuda real de un cliente; cambiar la clave secreta o eliminar la cuenta electrónica (correo, twitter, Facebook) para impedir al titular el acceso a su cuenta*.

2. DELITOS INFORMÁTICOS CONTRA LA INDEMNIDAD Y LIBERTAD SEXUALES (CAP. III)

Este capítulo está conformado por el tipo penal del **Art. 5º** (*proposición a niños, niñas y adolescentes con fines sexuales por medios tecnológicos*), que sanciona la propuesta sexual (*solicitar u obtener material pornográfico, llevar a cabo actividades sexuales*) a niños, niñas y adolescentes utilizando los medios tecnológicos.

> *Art. 5º.-* "*El que a través de internet u otro medio análogo contacta con un menor de catorce años para solicitar u obtener de él material pornográfico, o para llevar a cabo actividades sexuales con él, será reprimido con pena privativa de libertad no menor de cuatro ni mayor de ocho años e inhabilitación conforme a los numerales 1, 2 y 4 del artículo 36 del Código Penal.*
>
> *Cuando la víctima tiene entre catorce y menos de dieciocho años de edad y medie engaño, la pena será no menor de tres ni mayor de seis años e inhabilitación conforme a los numerales 1, 2 y 4 del artículo 36° del código Penal".*

[53]AZAOLA CALDERON, Luis; "Delitos informáticos y Derecho penal", UBIJUS, México 2010, pág. 70.

[54] MATA BARRANCO, Norberto J/ HERNÁNDEZ DÍAZ, Leyre; "El delito de daños informativos: una tipificación defectuosa"; **en**, Revista de Estudios Penales y Criminológicos, Vol. XXIX, España, 2009, pág. 311- 362.

Se sanciona el *contacto (establecer contacto o comunicación con alguien)*[55] *realizado* con un menor de edad con fines a obtener material pornográficos o con el propósito de llevar a cabo actividades sexuales que involucren el quebrantamiento de la indemnidad o libertad sexual del menor (*violación sexual o actos contra el pudor*); en este artículo hay dos supuestos:

- El primer supuesto es el **contacto** con un *menor de catorce* años para solicitar, obtener material pornográfico o para realizar actos sexuales, cuya pena es de 4 a 8 años de pena privativa de libertad e inhabilitación.
- El segundo supuesto es el **contacto** con un *menor que tiene entre catorce y dieciocho* años para solicitar, obtener material pornográfico o para realizar actos sexuales, cuya pena es de 3 a 6 años de pena privativa de libertad e inhabilitación

Este tipo sanciona el acto de *contactar* que significa *"establecer contacto o comunicación con alguien"*[56], y el término "*para*" es un elemento subjetivo que determina la intención del sujeto activo y es este elemento que convierte a la figura penal en un *tipo de tendencia interna trascendente (delitos de intención)*[57]*,* porque este ilícito "parte interna" requiere de una intención especial, que no corresponde a la parte externa objetiva que en este caso es obtener material pornográfico y/o tener actividades sexuales con el menor; por consiguiente, el tipo legal queda consumado cuando se produce el resultado típico, no siendo necesario que el agente consiga realizar su especifica tendencia trascendente, por estas características se clasifica a esta figura como un *delito de resultado cortado,* porque en este ilícito el agente persigue un resultado que está más allá del tipo y que ha de producirse por sí solo, sin su intervención y con posterioridad.[58]

En esta figura penal el legislador adelanta las barreras de punibilidad al sancionar el solo hecho de contactar con el menor de edad, sin importar si logra su objetivo el cual es obtener material pornográfico o llegar a tener actividad sexual, sin embargo este articulo tiene muchas falencias que podría violar el principio de legalidad*,* al no tener una redacción clara, y a consecuencia de este error se podría sancionar a personas que solo contactan con un menor de edad sin tener la finalidad de obtener material pornográfico y otro similar porque el término *contactar* no está delimitado, por consiguiente se estaría sancionando el solo hecho de establecer un "contacto" o comunicación con un menor de edad.

---

[55]Diccionario de la Real Academia Española http://www.rae.es/recursos/diccionarios/drae [visto el 28 de marzo 2014].

[56] Diccionario de la Real Academia Española http://www.rae.es/recursos/diccionarios/drae [visto el 28 de marzo 2014].

[57] VILLAVICENCIO TERREROS, Felipe; "Derecho Penal- Parte General", 3° reimpresión de la 1° ed., GRIJLEY, Lima 2010 pág. 375, Define a los tipos de tendencia interna trascendente como aquellos delitos "cuya parte interna requiere de una intención especial que consiste en la búsqueda de un resultado diferente al exigido típicamente y que, por ende, no es exigente para la consumación del delito, debiendo entenderse solo para efectos de llenar el tipo".

[58]VILLAVICENCIO TERREROS, Felipe, op. cit. Pág. 375.

DELITOS CONTRA LA LIBERTAD SEXUAL.- son acciones destinado a vulnerar tanto la indemnidad sexual como la libertad sexual del menor.

Este delito se consuma con la sola proposición, a un menor de edad con fines sexuales, ya sea para obtener material pornográfico o para acceder a la actividad sexual, esta conducta es sancionable porque afecta la indemnidad del menor y la libertad sexual y el medio utilizado para facilitar el contacto es la informática.

PORNOGRAFÍA INFANTIL.- en esta conducta tipificada se denota la intención del legislador de proteger penalmente varios bienes jurídicos, cuya titularidad corresponde a menores de edad, cuales son los adecuados procesos de formación y socialización de unos y otros y, su intimidad.[59]

Lo que se busca sancionar con esta tipo penal es el acto de *ofrecer, vender, distribuir, exhibir* material pornográfico de menores de edad. Esta conducta está referida a un sujeto activo indiferenciado (*delito de dominio*), es de mencionar que esta modalidad es dolosa: el sujeto ha de conocer la naturaleza del material y ha de querer realizarlo, difundir o poseer con dichos fines siendo indiferente que lo haga con ánimo lubrico o de lucro.

3. DELITOS INFORMÁTICOS CONTRA LA INTIMIDAD Y EL SECRETO DE LAS COMUNICACIONES (CAP. IV)

Este capítulo está conformado por las siguientes figuras penales: **Art. 6º** *(Derogado por la ley 30171 Ley que Modifica la Ley 30096, Ley de Delitos Informáticos[60])*, **Art. 7º** (*interceptación de datos informáticos*).

> *Art. 6°.- (derogado por la Única Disposición Derogatoria de la Ley 30171 "Ley que modifica la Ley 30096")*
>
> *Art. 7º.-* "*El que deliberadamente e ilegítimamente intercepta datos informáticos en transmisiones no públicas, dirigidas a un sistema informático, originadas en un sistema informático o efectuadas dentro del mismo, incluidas las emisiones electromagnéticas provenientes de un sistema informático que transporta dichos datos informáticos, será reprimido con pena privativa de la libertad no menor de tres ni mayor de seis años.*

[59] ORTS BERENGUER, Enrique/ ROIG TORRES, Margarita; "Delitos informáticos y delitos comunes cometidos a través de la informática", TIRANT LO BLANCH, Valencia 2001, pág. 129.

[60]El artículo 6º de la Ley Nº 30096, Ley de Delitos Informáticos; fue derogado por la UNICA DISPOSICION COMPLEMENTARIA DEROGATORIA de la Ley Nº 30171 "Ley que modifica la Ley Nº 30096, Ley de Delitos Informáticos"

La pena privativa de libertad será no menor de cinco ni mayor de ocho años cuando el delito recaiga sobre información clasificada como secreta, reservada o confidencial de conformidad con la Ley 27806, Ley de Transparencia y Acceso a la información Pública.

La pena privativa de libertad será no menor de ocho ni mayor de diez años cuando el delito comprometa la defensa, la seguridad o la soberanía nacionales.

Si el agente comete el delitos como integrante de una organización criminal, la pena se incrementa hasta en un tercio por encima del máximo legal previsto en los supuestos anteriores."

La figura penal sanciona la conducta que deliberada e ilegítimamente intercepta *(Interrumpe, obstruye una vía de comunicación)*[61] datos informáticos y las emisiones electromagnéticas que transportan estos datos en las transmisiones privadas. Este artículo contiene tres agravantes:

- El primer agravante se aplica cuando la interceptación recaiga sobre *información clasificada como secreta, reservada o confidencial,* de conformidad con la Ley 27806, Ley de Transparencia y Acceso a la información Pública. cuya penalidad oscila entre cinco a ocho años
- El segundo agravante se aplica cuando la interceptación recaiga sobre *información que compromete a la defensa, seguridad o soberanía nacional*, cuya penalidad oscila entre ocho a diez años.
- La tercera agravante consiste en la calidad del agente *–integrante de una organización criminal-* comete el delitos como cuya penalidad se incrementa hasta en un tercio por encima del máximo legal previsto en los supuestos anteriores.

Este injusto penal *-interceptar datos informáticos-* es un delito de *peligro abstracto* y por ende, solo basta con demostrar la interceptación de datos informáticos para que el delito quede consumado. Por ende, se clasifica como un *delito de mera actividad* porque basta con el sólo hecho de interceptar datos informáticos para que se consuma el delito. *Vgr. interceptación de archivos que contengan información relacionado con una investigación reservada por ley, interceptación de comunicaciones que contenga información sensible que puede ser utilizado por algún país en un contexto bélico.*

[61]Diccionario de la Real Academia Española http://lema.rae.es/drae/?val=interceptar (visto el 28 de marzo 2014).

4. DELITOS INFORMÁTICOS CONTRA EL PATRIMONIO (CAP. V)

Este capítulo está integrado por el **Art. 8** (*fraude informático*), que sanciona la acción de *diseñar, introducir, alterar, borrar, suprimir y clonar datos informáticos* en perjuicio de tercero.

> *Art. 8°.-* "*El que deliberadamente e ilegítimamente procura para sí o para otro un provecho ilícito en perjuicio de tercero mediante el diseño, introducción, alteración, borrado, supresión, clonación de datos informáticos o cualquier interferencia o manipulación en el funcionamiento de un sistema informático, será reprimido con una pena privativa de libertad no menor de tres ni mayor de ocho años y con sesenta a ciento veinte días multa.*
>
> *La pena será privativa de libertad no menor de cinco ni mayor de diez años y de ochenta a ciento cuarenta días multa cuando se afecte el patrimonio del Estado destinado a fines asistenciales o a programas de apoyo social*".

Este injusto penal –*fraude informático*- sanciona diversas conductas, entre ellos: diseñar *(proyecto o plan)*[62], introducir *(entrar en un lugar)*[63], alterar *(estropear, dañar, descomponer)*[64], borrar *(desvanecer, quitar, hacer que desaparezca algo)*[65], suprimir *(hacer cesar, hacer desaparecer)*[66], clonar *(producir clones)*[67] datos informáticos o cualquier interferencia, o manipular *(operar con las manos o con cualquier instrumento)*[68] el funcionamiento de un sistema informático procurando *(conseguir o adquirir algo)*[69] un beneficio para sí o para otro en perjuicio de tercero; y por la forma como esta estructurado –*a propósito de la mala redacción que genera mucha confusión al momento de interpretar la figura, y las conductas inadecuadas como "diseñar, introducir, alterar, borrar y suprimir"*

[62]Diccionario de la Real Academia Española http://www.rae.es/recursos/diccionarios/drae [visto el 28 de marzo 2014].
[63]Diccionario de la Real Academia Española http://www.rae.es/recursos/diccionarios/drae [visto el 28 de marzo 2014].
[64]Diccionario de la Real Academia Española http://www.rae.es/recursos/diccionarios/drae [visto el 28 de marzo 2014].
[65]Diccionario de la Real Academia Española http://www.rae.es/recursos/diccionarios/drae [visto el 28 de marzo 2014].
[66]Diccionario de la Real Academia Española http://www.rae.es/recursos/diccionarios/drae [visto el 28 de marzo 2014].
[67]Diccionario de la Real Academia Española http://www.rae.es/recursos/diccionarios/drae [visto el 28 de marzo 2014].
[68]Diccionario de la Real Academia Española http://www.rae.es/recursos/diccionarios/drae [visto el 28 de marzo 2014].
[69]Diccionario de la Real Academia Española http://www.rae.es/recursos/diccionarios/drae [visto el 28 de marzo 2014].

que no encajan en el delito de fraude informático, estas conductas son propios del delito de daño- se clasifica como un *delito de resultado* porque no basta cumplir con el tipo penal para que se consume el delito de fraude informático, sino que además, es necesario que esa acción vaya seguida de un resultado separado de la misma conducta el que consiste en causar un perjuicio a tercero, de otro modo el delito quedaría en tentativa. *Vgr. Clonar tarjetas bancarias, el fraude informático afecta los programa social JUNTOS, PENSIÓN 65, destinados a apoyo social.*

Este artículo es compatible con el Art. 8 del Convenio de Budapest[70], porque ambos artículos sancionan el empleo indebido de datos informáticos, la manipulación del funcionamiento del sistema mismo.

5. DELITOS INFORMÁTICOS CONTRA LA FE PÚBLICA (CAP. VI)

El Art. 9º de la ley (*suplantación de identidad*), sanciona la suplantación de identidad de una persona natural o jurídica, siempre que de esto resulte algún perjuicio.

> *Art. 9°.-* "*El que, mediante las tecnologías de la información o de la comunicación suplanta la identidad de una persona natural o jurídica, siempre que de dicha conducta resulte algún perjuicio, será reprimido con pena privativa de libertad no menor de tres ni mayor de cinco años*".

Este tipo penal sanciona el hecho se suplantar *(ocupar con malas artes el lugar de alguien, defraudándole el derecho, empleo o favor que disfrutaba)*[71] la identidad de una persona natural o jurídica causando algún perjuicio.

La *suplantación de identidad* se puede calificar como un delito de resultado porque no basta con realizar la conducta típica de "*suplantar*" la identidad, sino que además es necesario que esa acción vaya seguida de un resultado separado de la misma conducta que consiste en causar un perjuicio, caso contrario quedaría en tentativa. *Vgr. crear perfiles falsos en las redes sociales (correo electrónico, Facebook, twitter) atribuidos a personas naturales y/o jurídicas para engañar y perjudicar a terceros*[72]*.*

---

[70] Ver Convenio sobre la ciberdelincuencia – Budapest, 23.XI.2001: Cap. II, sección 1º, titulo 2º, Art. 8º.- fraude informático.

[71] Diccionario de la Real Academia Española http://lema.rae.es/drae/?val=suplantar (visto el 28 de marzo 2014).

[72] "una abogada había sido suplantada en el Facebook y correo electrónico, por la pareja de su amiga, fingiendo ser lesbiana, para captar personas y ganarse la confianza a través del falso perfil y poder obtener materiales (fotos intimas) que luego eran utilizados para extorsionar a sus víctimas que ingenuamente creyeron estar en contacto con la persona suplantada, este acto trajo perjuicios económico, laboral, familiar, psicológico a la suplantada", CUARTO PODER REPORTAJE DE NOTICIA DE FECHA (02/12/13).

6. DISPOSICIONES COMUNES (CAP. VII)

El capítulo VII de la ley está integrado por las siguientes figuras penales: **Art. 10º** (*abuso de mecanismos y dispositivos informáticos*) y el **Art. 11º** *(agravantes*).

> *Art. 10°.-* "*El que deliberadamente e ilegítimamente fabrica, diseña, desarrolla, vende, facilita, distribuye, importa u obtiene para su utilización, uno o más mecanismos, programas informáticos dispositivos, contraseñas, códigos de acceso o cualquier otro dato informático, específicamente diseñados para la comisión de los delitos previstos en la presente Ley, o el que ofrece o presta servicio que contribuya a ese propósito, será reprimido con pena privativa de libertad no menor de uno ni mayor de cuatro años y con treinta a noventa días-multa*".

Se sanciona diversas conductas, entre ellas : fabricar *(producir objetos en serie, generalmente por medios mecánicos)*[73]*,* diseñar *(hacer un diseño)*[74], desarrollar, vender *(traspasar a alguien por el precio convenido la propiedad de lo que uno posee*)[75], facilitar *(proporcionar o* entregar)[76], distribuir *(entregar una mercancía a los vendedores y consumidores)*[77], importa *(dicho de una mercancía: valer o llegar a cierta cantidad)*[78] *y* obtener *(alcanzar, conseguir y lograr algo que se merece, solicita o pretende),* para la utilización de mecanismos, programas informáticos, contraseñas, etc., diseñados específicamente para la comisión de los delitos previstos en esta ley. Este artículo es una expresión del adelantamiento de las barreras punitivas porque se sanciona la participación y más aún el sólo hecho de ofrecer un servicio que facilite la comisión de algún delito previsto en la presente ley.

---

[73]Diccionario de la Real Academia Española http://www.rae.es/recursos/diccionarios/drae [visto el 28 de marzo 2014].
[74]Diccionario de la Real Academia Española http://www.rae.es/recursos/diccionarios/drae [visto el 28 de marzo 2014].
[75]Diccionario de la Real Academia Española http://www.rae.es/recursos/diccionarios/drae [visto el 28 de marzo 2014].
[76]Diccionario de la Real Academia Española http://www.rae.es/recursos/diccionarios/drae [visto el 28 de marzo 2014].
[77]Diccionario de la Real Academia Española http://www.rae.es/recursos/diccionarios/drae [visto el 28 de marzo 2014].
[78]Diccionario de la Real Academia Española http://www.rae.es/recursos/diccionarios/drae [visto el 28 de marzo 2014].

Este tipo penal –*abuso de mecanismos y dispositivos informáticos*- se clasifica como un *delito de mera actividad*, porque la figura exige cumplir con la conducta mencionado en el tipo penal para la consumación del delito sin importar el resultado posterior. Aquí el legislador adelanta las barreras de punibilidad al sancionar el solo hecho de fabricar, diseñar, vender, etc., mecanismos, programas orientados a cometer diversos delitos previstos en la ley. Esta figura penal poseería las características del llamado *derecho penal del enemigo* porque se sanciona actos preparatorios alegando la puesta en peligro de la seguridad informática. *Vgr. tráfico de datos de usuarios y contraseñas obtenidas ilícitamente para cometer fraudes informáticos, comercializar equipos especializados en capturar, interceptar información.*

Este artículo es compatible con el Art 6º de la Convención de Budapest, sin embargo hay una interpretación muy amplia, un vacío de este articulo por cuanto se extiende a toda gama de delitos previstos en la presente ley y que podría generar problemas en la interpretación judicial, debido a la extensión de ilícitos como : *interferencia telefónica, pornografía infantil, etc.*

> *Art. 11º.-* "*El juez aumenta la pena privativa de libertad hasta un tercio por encima del máximo legal fijado para cualquiera de los delitos previstos en la presente Ley, cuando:*
>
> 1. *El agente activo integra una organización criminal.*
> 2. *El agente tiene posición especial de acceso a la data o información reservada.*
> 3. *El delito se comete para obtener un fin económico.*
> 4. *El delito compromete fines asistenciales, la defensa, la seguridad y soberanía nacional."*

Se regulan las agravantes de los delitos previstos en la presente ley, y en base a esta norma el juez puede aumentar la pena hasta en un tercio por encima del máximo legal fijado; vgr: participación de integrantes de la organización criminal en la comisión de delitos informáticos, el acceso ilícito a la cuenta de correo electrónico a cambio de un pago*(los hackers de un centro comercial).*

> *Art. 12º.-* "*Está exento de responsabilidad penal el que realiza las conductas descritas en los artículos 2, 3, 4 y 10 con el propósito de llevar a cabo pruebas autorizadas u otros procedimientos autorizados destinados a proteger sistemas informáticos* "[79]

[79]Artículo 12º.- **EXENCIÓN DE RESPONSABILIDAD PENAL,** incorporado por el Art. 3º de la Ley Nº 30171 "*Ley que modifica la Ley Nº 30096, Ley de Delitos Informáticos*", publicado el 10 de marzo del 2014.

Este artículo incorporado por el Art. 3º de la Ley Nº 30171 "*Ley que modifica la Ley Nº 30096, Ley de Delitos Informáticos*", exime de responsabilidad penal a toda persona que realiza alguna de las conductas reguladas en los artículos 2º, 3º, 4º y 10º de la presente Ley. Esta cláusula de exención de responsabilidad se fundamenta en la conducta legal – autorizada por la autoridad correspondiente- para realizar pruebas u otro procedimiento con el objetivo de proteger los sistemas y datos informáticos.

Esta norma es compatible con el artículo 6°, inc. 2 del Convenio de Budapest.

7. SANCIONES A PERSONAS JURIDICAS IMPUESTAS POR ORGANISMOS REGULADORES.

La nueva ley de delitos informáticos contiene once disposiciones complementarias finales, de las cuales solo nos enfocaremos a las referentes a las personas jurídicas, que se encuentran en la décima y undécima DCF de la nueva ley.

> Regulación e imposición de multas por la Superintendencia de Bancas, Seguros y AFP.
>
> ***DÉCIMA.-*** ***"****La Superintendencia de Banca, Seguros y AFP establece la escala de multas atendiendo a las características, complejidad y circunstancias de los casos aplicables a las empresas bajo su supervisión que incumplan con la obligación prevista en el numeral 5 del artículo 235° del Código Procesal Penal, aprobado por Decreto Legislativo 957.*
> *El juez, en el término de setenta y dos horas, pone en conocimiento del órgano supervisor la omisión incurrida por la empresa, con lo recaudos correspondientes sobre las características, complejidad y circunstancias del caso particular, a fin de aplicarse la multa correspondiente"*

Esta disposición establece que la Superintendencia de Banca, Seguros y AFP determina la escala de multa de acuerdo a la característica, complejidad y circunstancias de los casos aplicables de las empresas bajo su supervisión que incumplan con la obligación de acuerdo con el Art. 235° inciso 3 del Código Procesal penal.

Este tipo legal tienen las características de una *norma en blanco* porque se complementa en otra ley *(Ley general del sistema financiero y del sistema de seguros y orgánica de la superintendencia de banca y seguros ley no 26702)* para establecer las sanciones a las empresas que omiten una orden judicial.

Esta modificación completa el círculo de la facultad sancionadora que tiene el Estado, con la sanción administrativa por el incumplimiento de las entidades del sistema financiero de

la obligación de entregar la información correspondiente a la orden judicial de levantamiento del secreto bancario.

Regulación e imposición de multas por el organismo Supervisor de Inversión privada en telecomunicaciones.

UNDÉCIMA.- ***"****El Organismo Supervisor de Inversión Privada en Telecomunicaciones establece la escala de multas atendiendo a las características, complejidad y circunstancias de los casos aplicables a las empresas bajo su supervisión que incumplan con la obligación prevista en el numeral 4 del artículo 230° del Código Procesal Penal, aprobado por Decreto Legislativo 957.*
El juez, en el término de setenta y dos horas, pone en conocimiento del órgano supervisor la omisión incurrida por la empresa, con los recaudos correspondientes sobre las características, complejidad y circunstancias del caso particular, a fin de aplicarse la multa correspondiente."

El Organismo Supervisor de Inversión privada en telecomunicaciones establece la escala de multas atendiendo a las características, complejidad y circunstancias de los casos aplicables a las empresas bajo su supervisión que incumplan la obligación prevista en el numeral 4º del Art. 230º del Código Procesal Penal.

Esta modificación sanciona administrativamente el incumplimiento de las empresas prestadoras de servicios de comunicaciones y telecomunicaciones de la obligación de posibilitar la diligencia judicial de intervención, grabación o registro de las comunicaciones y telecomunicaciones.

III. REFORMAS DEL CÓDIGO PENAL RELACIONADO CON LOS DELITOS INFORMATICOS

Los artículos 158°, 162º y 323° del Código Penal fueron modificado por el Art. 4º de la Ley Nº 30171º "*Ley que modifica la Ley Nº 30096º, Ley de delitos informáticos*" en los siguientes términos:

Art. 158º.-"*Los delitos previstos en este capítulo son perseguibles por acción privada, salvo en el caso del delitos previsto en el artículo 154°-A"*

Este artículo, antes de la modificatoria, establecía la acción privada para los delitos comprendido en el Capítulo II "*Violación de la intimidad*". A partir de la incorporación del artículo 154°-A "*Tráfico ilegal de datos personales*", se prevé la acción pública solo para el mencionado artículo incorporado.

> *Art. 162º.- "El que, indebidamente, interfiere o escucha una conversación telefónica o similar, será reprimido con pena privativa de libertad no menor de tres ni mayor de seis años.*
>
> *Si el agente es funcionario público, la pena privativa de libertad será no menor de cuatro ni mayor de ocho años e inhabilitación conforme al artículo 36, inciso 1, 2 y 4.*
>
> *La pena privativa de libertad será no menor de cinco ni mayor de ocho años cuando el delito recaiga sobre información clasificada como secreta, reservada o confidencial de conformidad con la Ley 27806, Ley de Transparencia y Acceso a la información Pública.*
>
> *La pena privativa de libertad será no menor de ocho ni mayor de diez años cuando el delito comprometa la defensa, la seguridad o la soberanía nacionales.*
>
> *Si el agente comete el delitos como integrante de una organización criminal, la pena se incrementa hasta en un tercio por encima del máximo legal previsto en los supuestos anteriores."*

La modificación de este artículo se da porque la redacción anterior era muy amplia y dejaba al arbitrio del juzgador determinar qué información se clasifica como secreta, reservada o confidencial. De ahí la necesidad de precisar la agravante del delito de interceptación telefónica cuando afecte la información secreta, reservada o confidencial y, esta precisión se encuentra en la Ley N° 27806 "*Ley de transparencia y acceso a la información pública*".

A modo de información, debe mencionarse que después de la promulgación de la Ley Nº 30096, el 5 de diciembre del año 2013 se ha presentado otro **PROYECTO DE LEY Nº 3048/ 2013- CR**[80] que busca modificar el mencionado artículo, argumentado que no se ha

[80]Proyecto de Ley presentado el 5 de diciembre del 2013 por el Congresista de la República José Luna Gálvez, integrante del Grupo Parlamentario Solidaridad Nacional.

regulado correctamente la conducta a sancionar, además agrega algunas agravantes como es el móvil de la interceptación[81].

> Art. 154°-A.- "*El que ilegítimamente comercializar o información no publica relativa a cualquier ámbito de la esfera personal, familiar, patrimonial, laboral, financiera u otro de naturaleza análogo sobre una persona natural, será reprimido con pena privativa de libertad no menor de tres ni mayor de cinco años.*
>
> *Si el agente comete el delito como integrante de una organización criminal, la pena se incrementa hasta en un tercio por encima del máximo legal previsto en el párrafo anterior*"[82].

Este figura penal sanciona la conducta de comercializar *(comercializar, traficar, vender promover, favorecer o facilitar)* información no publica, independientemente si con estos actos se causa algún perjuicio.

Este injusto penal –*Tráfico ilegal de datos*- por la característica que presenta es un *tipo de tendencia interna trascendente* por que presenta el elemento subjetivo "*para*" que denota una intención especial consistente en la búsqueda de un resultado diferente exigido típicamente, por tanto se clasifica como un *delito de resultado cortado* por que el agente busca un resultado que está más allá del tipo el cual es *comercializar, traficar, etc*., una base de datos. Ejemplo: La comercialización de bases de datos que contienen nombres, documentos de identidad, edad, estado civil, domicilio, teléfono, ocupación, puesto laboral, remuneración, etc.

---

[81]El **PROYECTO DE LEY Nº 3048/ 2013- CR** pretende incrementa las sanciones contempladas para este ilícito en su modalidad básica e incluye dos conductas que agravan la figura penal, en los supuestos de ***recaer sobre información clasificada como secreta, reservada o confidencial de conformidad con las normas de la materia*** y ***compromete la defensa, seguridad o la soberanía nacional***. Este proyecto pretende una mejor regulación de la conducta prohibida, al sancionar no solo el hecho de interferir o escuchar una conversación telefónica, sino sobre todo al consideran que también se debió incluir el hecho de **GRABAR**, porque según fundamentan no es lo mismo interceptar, escuchar y grabar. Otra circunstancia que considera agravante, es el referido al móvil por el que se realiza la conducta típica, ya sea para obtener un provecho tanto para el autor como para un tercero a cambio de dinero y otra ventaja, o si la intención es para perjudicar a la victima de interceptación sea de manera económica o de otra manera. Otra circunstancia que considera agravante, es el referido al móvil por el que se realiza la conducta típica, ya sea para obtener un provecho tanto para el autor como para un tercero a cambio de dinero y otra ventaja, o si la intención es para perjudicar a la victima de interceptación sea de manera económica o de otra manera.

[82] Articulo incorporado al Código Penal por la Ley Nº 30171.

> Art. 183°-B.- "*El que contacta con un menor de catorce años para solicitar u obtener de él material pornográfico, o para llevar a cabo actividades sexuales con él, será reprimido con una pena privativa de libertad no menor de cuatro ni mayor de ocho años e inhabilitación conforme a los numerales 1, 2 y 4 del artículo 36.*
>
> Cuando la víctima tiene entre catorce y menos de dieciocho años de edad y medie engaño, la pena será no menor de tres ni mayor de seis años e inhabilitación conforme a los numerales *1, 2 y 4 del artículo 36*"[83].

Esta figura penal sanciona la conducta de contactar *(Establecer contacto o comunicación con alguien[84])* con un menor de catorce años para solicitar u obtener de él material pornográfico, o para llevar a cabo actividades sexuales. La norma regula la agravante cuando la víctima tiene entre catorce y menos de dieciocho años y medie engaño, para este supuesto la pena a imponer será no menor de tres ni mayor de seis años.

Las *proposiciones sexuales a niños, niñas y adolescentes,* por las características que presenta el tipo, se puede calificar como un *tipo de tendencia interna trascendente* por que presenta el elemento subjetivo "*para*" que denota una intención especial consistente en la búsqueda de un resultado diferente exigido típicamente, por tanto se clasifica como un *delito de resultado cortado* por que el agente busca un resultado que está más allá del tipo el cual es *obtener material pornográfico o tener acto sexual con la menor*.

IV. BIBLIOGRAFIA

- ADÁN DEL RIO, Carmen; "La persecución y sanción de los delitos informáticos", CUADERNO VASCO DE CRIMINOLOGÍA, Nº 20, Vasco 2006.
- AROCENA, Gustavo A.; "La regulación de los delitos informativos en el código penal argentino. Introducción a la ley nacional N° 26.388", **en** Boletín Mexicano de Derecho Comparado, nueva serie, año XLV, N° 135, México 2012, pág. 945- 988.
- AZAOLA CALDERON, Luis; "Delitos informáticos y Derecho penal", UBIJUS, México 2010.

[83] Articulo incorporado al Código Penal por la Ley Nº 30171.
[84]Diccionario de la Real Academia Española http://lema.rae.es/drae/?val=contactar [visto el 28 de marzo 2014].

- BRAMONT- ARIAS TORRES, Luis A.; “Delitos informáticos”, **en** Revista Peruana de Derecho de la Empresa, DERECHO INFORMATICO Y TELEINFORMATICA JURIDICA, Nº 51, ASESORANDINA. Lima 2000.
- CAMACHO LOSA, L; “El delito informático” GRAFICAS CONDOR, Madrid 1987.
- CARNEVALI RODRÍGUEZ, Raúl; “La criminalidad organizada. Una aproximación al derecho penal italiano, en particular la responsabilidad de las personas jurídicas y la confiscación”, Vol. 16, Ius Et Praxis Nº 2, Talca, 2010.
- CORCOY BIDASOLO, Mirentxu; “Problemática de la persecución penal de los denominados delitos informáticos: particular referencia a la participación criminal y al ámbito espacio temporal de comisión de los hechos”, CUADERNO VASCO DE CRIMINOLOGÍA, Nº 21, Vasco 2001.
- DÍAZ GÓMEZ, A., «El delito informático, su problemática y la cooperación internacional como paradigma de su solución: El Convenio de Budapest, REDUR 8, Rioja 2010
- DE ALFONSO LASO, D; “El hackerin blanco. Una conducta ¿punible o impune?”, en Internet y derecho penal, Cuadernos de Derecho Judicial, Consejo General del poder Judicial, Madrid, 2001, pág.110- 111.
- DOVAL PAIS, Antonio; “La intimidad y los secretos de la empresa como objeto de ataque por medios informáticos”, CUADERNO VASCO DE CRIMINOLOGÍA, Nº 22, Vasco 2008.
- DURAND VALLADARES, “Los delitos informáticos en el Código Penal Peruano” **en** Revista Peruana de Ciencias Penales. N° 11, Lima 2002.
- FARALDO CABANA, Patricia; “Los conceptos de manipulación informática y artificio semejante en el delito de estafa informática”, CUADERNO VASCO DE CRIMINOLOGÍA, Nº 21, Vasco 2007.
- GALVEZ VILLEGAS, Tomas/ DELGADO TOVAR, Walter; “Derecho Penal Parte Especial”, T III, Jurista Editores, Lima 2002.
- GONZÁLES DE CHAVES CALAMITA, María E.; “El llamado ´delito informático´”, **en** Anales de la Facultad de Derecho de la Universidad de la Laguna N° 21, España, 2004.
- GÓMEZ MARTIN, Víctor; “El delito de fabricación, puesta en circulación y tenencia de medios destinados a la neutralización de dispositivos protectores de programas informáticos”, REVISTA ELECTRÓNICA DE CIENCIA PENAL Y CRIMINOLOGÍA, Barcelona 2002.

- GÓMEZ TOMILLO, Manuel; "Autoría y participación por difusión de contenidos ilícitos a través de sistema informáticos: especial referencia a los delitos contra la propiedad intelectual, la publicidad engañosa y la distribución de pornografía infantil", CUADERNO VASCO DE CRIMINOLOGÍA, Nº 20, Vasco 2006.
- GUTIERREZ FRANCES, María; "Fraude Informático y estafa", **en** Centro de Publicaciones del Ministerio de Justicia, Madrid 1991.
- MANSON, Marcelo; "Legislación sobre delitos informáticos", **en** https://dl.dropbox.com/u//dl. legislacioncomparada.pdf. [visto el 27 de diciembre 2013].
- MARCHENA GOMEZ, M; "El sabotaje informático: entre los delitos de daños y desordenes públicos", en Internet y Derecho Penal, Cuadernos de Derecho Judicial, Madrid 2001.
- MATA BARRANCO, Norberto J/ HERNÁNDEZ DÍAZ, Leyre; "El delito de daños informativos: una tipificación defectuosa"; **en**, Revista de Estudios Penales y Criminológicos, Vol. XXIX, España, 2009.
- MAZUELOS COELLO, Julio F.; "Delitos informativos: una aproximación a la regulación del Código Penal peruano", en RPDJP N° 2, Lima, 2001, pág. 253 y ss.
- MIRÓ LINARES, Francisco; "El cibercrimen. Fenomenología y criminología de la delincuencia en el ciberespacio", Marcial Pons, Madrid, 2012.
- MORANT VIDAL, J; "protección penal de la intimidad frente a las nuevas tecnologías", Ed. PRACTICA DE DERECHO, Valencia, 2003.
- MORON LERMA, ESTHER; "Internet y Derecho Penal: hacking y otras conductas ilícitas en la red", ED. ARANZADI, 2° ed., Navarra, 2002,
- ORTS BERENGUER, Enrique/ ROIG TORRES, Margarita; "Delitos informáticos y delitos comunes cometidos a través de la informática", TIRANT LO BLANCH, Valencia 2001.
- ROMERO CASABONA, C; "poder informático y seguridad jurídica", FUNDESCO, Madrid 1987.
- VILLAVICENCIO TERREROS, Felipe, "Derecho Penal- Parte general", 4 reemp., Grijley, Lima, 2013.
- VIVES ANTÓN y GONZÁLES CUSSAC, "Comentarios al código Penal 1995", Ed. TIRONT BLANCH, Valencia 1996, pág. 1238.

V. GLOSARIO DE TÉRMINOS

- ACTIVO PATRIMONIAL: Conjunto de bienes y derechos que integran el haber de una persona física o jurídica.
- BASE DE DATOS: Conjunto completo de ficheros informáticos que reúnen informaciones generales o temáticas, que generalmente están a disposición de numerosos usuarios.
- BROWSER (BUSCADOR): El software para buscar y conseguir información de la red WWW. Los más comúnmente usados son Microsoft Explorer, Firefox y Opera.
- COOKIE: Es un archivo o datos dejados en su computadora por un servidor u otro sistema al que se hayan conectado. Se suelen usar para que el servidor registre información sobre aquellas pantallas que usted ha visto y de la información personalizada que usted haya mandado. Muchos usuarios consideran esto como una invasión de privacidad, ya que casi ningún sistema dice lo que está haciendo. Hay una variedad de "anti-cookie" software que automáticamente borra esa información entre visitas a su sitio.
- DIALUP (MARCAR): El método de conectarse con Internet vía la línea de teléfono normal mediante un modem, en vez de mediante una LAN (Red Local) o de una línea de teléfono alquilada permanentemente. Esta es la manera más común de conectarse a Internet desde casa si no ha hecho ningún arreglo con su compagina de teléfono o con un ISP. Para conexiones alternativas consulte con su ISP primero.
- DIGITAL SIGNATURE (FIRMA DIGITAL): El equivalente digital de una firma autentica escrita a mano. Es un dato añadido a un fichero electrónico, diciendo que el dueño de esa firma escribió o autorizo el Archivo.
- DOCUMENTO ELECTRÓNICO: Es la representación en forma electrónica de hechos jurídicamente relevantes susceptibles de
- HTTP (HYPER TEXT TRANSPORT PROTOCOL): El conjunto de reglas que se usa en Internet para pedir y ofrecer páginas de la red y demás información. Es lo que pone al comienzo de una dirección, tal como "http: /," para indicarle al buscador que use ese protocolo para buscar información en la página.
- INTERNET SERVICE PROVIDER (ISP) (PROVEEDOR DE SERVICIO DE INTERNET) Una persona, organización o compagina que provee acceso a Internet. Además del acceso a Internet, muchos ISP proveen otros servicios tales como anfitrión de Red, servicio de nombre, y otros servicios informáticos.
- MENSAJE DE DATOS: Es toda aquella información visualizada, generada enviada, recibida, almacenada o comunicada por medios informáticos, electrónicos, ópticos, digitales o similares.
- MODEM: Un aparato que cambia datos del computador a formatos que se puedan transmitir más fácilmente por línea telefónica o por otro tipo de medio.
- SISTEMA TELEMÁTICO. Conjunto organizado de redes de telecomunicaciones que sirven para trasmitir, enviar, y recibir información tratada de forma automatizada.
- SISTEMA DE INFORMACIÓN: Se entenderá como sistema de información, a todo sistema utilizado para generar, enviar, recibir, procesar o archivar de cualquier forma de mensajes de Datos.

- SISTEMA INFORMÁTICO: Conjunto organizado de programas y bases de datos que se utilizan para, generar, almacenar, tratar de forma automatizada datos o información cualquiera que esta sea.
- SOCIEDAD DE LA INFORMACIÓN: La revolución digital en las tecnologías de la información y las comunicaciones (TIC) ha creado una plataforma para el libre flujo de información, ideas y conocimientos en todo el planeta. Ha causado una impresión profunda en la forma en que funciona el mundo. La Internet se ha convertido en un recurso mundial importante, que resulta vital tanto para el mundo desarrollado por su función de herramienta social y comercial, como para el mundo en desarrollo por su función de pasaporte para la participación equitativa y para el desarrollo económico, social y educativo.
- SOPORTE LÓGICO: Cualquiera de los elementos (tarjetas perforadas, cintas o discos magnéticos, discos ópticos) que pueden ser empleados para registrar información en un sistema informático.
- SOPORTE MATERIAL: Es cualquier elemento corporal que se utilice para registrar toda clase de información.
- TELEMÁTICA: neologismo que hace referencia a la comunicación informática, es decir la transmisión por medio de las redes de telecomunicaciones de información automatizada.

UNIDAD II: CONOCIMIENTOS LEGALES

3.- Retención de datos y secreto profesional- Comisión de Derechos Humanos de Barcelona FBE 30 de enero 2015.

Retención de datos y secreto profesional
Comisión de Derechos Humanos de Barcelona FBE 30 de enero 2015

Contenido:

Introducción

La Comisión de Derechos Humanos (CDH) de la FBE está preocupada con la preservación del secreto profesional y la confianza que es el centro de todas las relaciones profesionales entre abogados y clientes: el de la confidencialidad del cliente. Nuestra preocupación surge de la evolución de la Internet, que ha erosionado la protección de datos, e hizo una comunicación confidencial vulnerables entre abogado y cliente, el abogado y los tribunales, y un abogado a otro.

El Comité de Derechos Humanos reconoce que hay diferentes niveles de protección en diferentes países de Europa. La armonización de estas normas traerá beneficios a los ciudadanos y residentes de los estados miembros. La Unión Europea permite a los Estados miembros a trabajar juntos para proteger la confidencialidad y la confianza basada en el secreto profesional. La protección y preservación de la relación abogado-cliente de la confianza es el área específica de preocupación de los abogados europeos, y uno que consideramos ser un área importante de la directiva o reglamento de la UE.

Primera parte: La retención de datos y la Unión Europea.

En 2006, la UE promulgó la retención de datos Directiva 2006/24. La Directiva trata de garantizar que se dispone de datos de las comunicaciones[1], por un período limitado de tiempo, para prevenir, investigar, detectar y enjuiciar delitos graves, como, en particular, la delincuencia organizada y los actos terroristas. Para lograr esto, se requiere que los proveedores de servicios de comunicaciones electrónicas de acceso público o de redes públicas de comunicaciones para retener datos de tráfico y localización, así como ciertos datos relacionados necesarios para identificar al usuario. La Directiva no permitía la grabación y la retención del contenido de la comunicación.[2]

Antes de la Directiva 95/46 / CE en el artículo 6 contiene obligaciones relativas a las medidas para garantizar la confidencialidad y seguridad del tratamiento de los datos. Los objetivos de la Directiva 2006/24 / CE debían armonizar las obligaciones de los proveedores de conservar

[1] El artículo 2 del / la Directiva 2006/24 CE establece que a los efectos de los "datos" Directiva significa datos de tráfico y de localización y los datos relacionados necesarios para identificar al abonado o usuario. Esto se conoce como el "quién", "dónde" y "cuándo" de datos. Es el contexto, no el contenido de comunicaciones que está en cuestión

[2] Baker & McKenzie April newsletter April 2014

determinados datos y asegurar que éstos estén disponibles para el propósito de la investigación, la detección de estos datos y enjuiciamiento de delitos graves, tal como se define por cada Estado miembro en su legislación nacional. Dado que esto no puede ser alcanzado de manera suficiente por cada Estado miembro por sí solo, puede lograrse mejor a nivel comunitario, con motivo de la presente Directiva. De conformidad con el principio de proporcionalidad, la Directiva no excede de lo necesario para alcanzar dichos objetivos.

Directiva 2006/24 / CE[3] pretende garantizar el pleno cumplimiento de los derechos fundamentales de los ciudadanos al respeto de la vida privada y las comunicaciones y a la protección de sus datos de carácter personal, consagrado en Artes 7 y 8 de la Carta de los Derechos Fundamentales de la Unión Europea.

Segunda parte: La Decisión de la Corte Europea de Justicia y el desafío a la Directiva 04 2014

La Directiva 2006/24 fue invalidada por el Tribunal de Justicia en su sentencia en el caso "Digital Derechos Irlanda".[4]

Estados miembros Irlanda y Austria solicitaron una sentencia, con las observaciones presentadas por los gobiernos de Irlanda, Austria, España, Francia, Italia, Polonia, Portugal, Reino Unido, así como el Parlamento Europeo, el Consejo de la Unión Europea y la Comisión Europea .

El juicio establece el artículo 5 de la 2006/24 / CE[5], que enumera las categorías de datos que deben conservarse y en el artículo 5, párrafo 2 dice "ningún dato que revele el contenido de la comunicación pueden ser retenidos de conformidad con la presente Directiva."

En su sentencia, el Tribunal declaró que:

> *"A pesar de que la Directiva sobre conservación de datos no permite la retención del contenido de la comunicación o de la información consultada utilizando una red de comunicaciones electrónicas, la Corte consideró" no inconcebible "que la retención de los datos en cuestión podría tener un efecto escalofriante en la utilización, por los abonados o usuarios registrados, de los medios de comunicación electrónicos cubiertas por la Directiva sobre el ejercicio de la libertad de expresión, garantizado por el artículo 11 de la Carta de los Derechos Fundamentales de la Unión Europea ".*[6]

La Directiva interfiere de manera seria con los derechos al respeto de la vida privada y las comunicaciones, y para la protección de datos de carácter personal, consagrado en Artes 7 y 8 de la Carta.

---

[3] Junto con la Directiva 2002/58 / CE

[4] Sentencia de 8 de abril de 2014 en los asuntos acumulados C-293/12 Digital Rights Irlanda y C-594/12 Seitlinger http://curia.europa.eu/juris/document/document.jsf?docid=150642&doclang=EN

[5](a) datos necesarios para rastrear e identificar el origen de una comunicación; (b) datos necesarios para identificar el destino de una comunicación; datos necesarios (c) para identificar la fecha, hora y duración de una comunicación; (d) datos necesarios para identificar el tipo de comunicación; (e) datos necesarios para identificar el equipo de comunicación de los usuarios o lo que se considera ser el equipo; (f) datos necesarios para identificar la localización del equipo de comunicación móvil

[6] Estoy en deuda con Baker & McKenzie, que ha proporcionado información útil en abril 2014http://www.bakermckenzie.com/files/Publication/fcf2ef80-c7f6-4361-a782-660857c40248/Presentation/PublicationAttachment/cac82cb1-74a4-4451-bef6-6829c1ecf1c5/ALGermanyPublicLawApril2014.pdf

En definitiva la decisión del Tribunal de Justicia se hizo sobre la base de que "al adoptar la Directiva 2006/24, el legislador de la UE había excedido los límites impuestos por el principio de proporcionalidad a la luz de los artículos 7 [respeto a la vida privada y familiar], 8 [de protección de los datos personales] y 52 (1) [limitación de los derechos de] de la Carta [de Derechos Fundamentales de la Unión Europea].”

El Tribunal consideró que la retención de los datos no "*afecta negativamente a la esencia de los derechos fundamentales a la protección de datos personales*" y es, en principio, justificada por un objetivo de interés general, a saber, el enjuiciamiento de delitos graves, lo que garantiza seguridad pública.[7]

La importancia de la sentencia es que el Tribunal consideró que la Directiva viola el principio de proporcionalidad, que exige "*que los actos de las instituciones de la UE sean aptos para alcanzar los objetivos legítimos perseguidos por la normativa controvertida y no excedan los límites de lo que es apropiado y necesario para alcanzar estos objetivos* ".

La Corte encontró que aunque la retención de datos puede ser considerada como "*aptos para alcanzar el objetivo perseguido*" por la Directiva, las medidas de conservación establecidas por la Directiva no podían considerarse "necesarias" para lograr el objetivo legislativo (párrafo 46, 51 ss.). Según el Tribunal, el legislador de la Unión ha excedido los límites impuestos por el principio de proporcionalidad y, por lo tanto era válido.

> *La Directiva sobre conservación de datos cubre todas las personas y todos los medios de comunicación electrónica, así como todos los datos de tráfico sin ninguna diferenciación, limitación o excepción que se realizan en la luz del objetivo de luchar contra la delincuencia grave. En particular, la Directiva se aplica incluso a las personas para quienes no hay evidencia de que sugiere que su conducta podría tener un vínculo, incluso una indirecta o remota, a un delito grave.*[8]
>
> *Asimismo, no requiere ninguna relación entre los datos cuya conservación no se proporciona para y una amenaza para la seguridad pública ni limita la retención de los datos relativos a un período de tiempo determinado, en particular la zona geográfica o un círculo de personas determiadas probabilidades de estar involucrados en un delitos graves oa las personas que podrían contribuir, por la retención de los datos, a la prevención, detección o enjuiciamiento de delitos graves.*

Incluso aquellas personas cuya comunicación deben estar sujetos al secreto profesional, incluyendo el secreto profesional, estarían cubiertos bajo esta cobertura manta. Además, el Tribunal criticó la Directiva por no prescribe criterios objetivos para determinar los límites del acceso de las autoridades nacionales competentes a los datos y su uso posterior.

Debería haber un examen previo llevado a cabo por un tribunal o por un órgano administrativo independiente de la solicitud de acceso y la conservación de datos por una autoridad nacional competente.[9] La Corte también determinó que el período de retención de

---

[7] Sentencia del Tribunal de Justicia (Gran Sala) 08 de abril de 2014. El párrafo 39

[8] Sentencia del Tribunal de Justicia (Gran Sala) 08 de abril 2014.Paragraph 58 "Además, no prevé ninguna excepción, con el resultado de que se aplica incluso a las personas cuyas comunicaciones están sujetos, según las normas de Derecho interno, a las obligaciones de secreto profesional "

[9] Sentencia del Tribunal de Justicia (Gran Sala) 08 de abril 2014.Paragraph 62

datos de al menos seis meses, sin ningún tipo de distinción entre las categorías de datos no haya estado justificada en virtud del principio de proporcionalidad. Tampoco hubo suficientes salvaguardias para garantizar la protección efectiva de los datos durante el período de retención.

Tercera parte: Los Estados miembros de la UE

La decisión prejudicial fue solicitada por Irlanda y Austria, y la decisión ahora cubre su jurisprudencia nacional.

En todos los demás Estados miembros de la UE, las leyes nacionales de transposición de la Directiva sobre conservación de datos seguirán siendo válidas hasta desafiado, de conformidad con las normas procesales nacionales, ante los tribunales nacionales. Alguna de la siguiente información está tomada de la página web de Baker & McKenzie.[10]

En **Francia**, por ejemplo, la ley nacional de transposición de la Directiva sobre conservación de datos puede ser impugnada ante el Conseil Constitutionel por medio de una pregunta de continuar decisión preliminar (prioritaire de constitutionnalité) como resultado de un proceso judicial pendiente.

En **Alemania**, el Tribunal Constitucional Federal había declarado, en su sentencia de 2 de marzo de 2010 que la normativa alemana de transposición de la Directiva sobre conservación de datos violaron el derecho fundamental a la intimidad de las comunicaciones electrónicas garantizados por la Constitución alemana. A raíz de la sentencia del Tribunal Constitucional, el Gobierno Federal de Alemania no ha intentado reintroducir legislación de transposición de la Directiva sobre conservación de datos en línea con los requisitos establecidos en la sentencia del Tribunal Constitucional Federal, a pesar de un procedimiento de infracción que la Comisión Europea había iniciado contra la República Federal de Alemania.

En **Italia**, la sección pertinente del Código de Protección de Datos italiano puede ser impugnada ante la Corte costituzionale italiana.

En **Polonia**, el Tribunal Constitucional tiene que decidir sobre varias denuncias, la anulación de la transposición de la Directiva de conservación de datos de la UE de la legislación nacional y se espera que la Corte declare la normativa nacional a ser nula y sin efecto.

En **Romania**, los derechos de comunicación están protegidos en virtud del artículo 28 de la Constitución y el Defensor del pueblo independiente oye casos de denuncia, pero es criticado como proporcionar poco acceso a la justicia para los ciudadanos.

En **España,** la legislación nacional puede ser recurrida ante el Tribunal Constitucional, donde se medirían las normas contra los principios de protección de datos nacional y los derechos fundamentales, presumiblemente con un resultado idéntico a la sentencia del Tribunal de Justicia Europeo.

En el **Reino Unido**, el gobierno del Reino Unido introdujo una legislación de "emergencia" tres meses después de la sentencia del TJCE en la forma de la Ley de conservación de datos y Poderes de Investigación 2014 (DRIPA).[11] Ahora propone modificar DRIPA para retener

[10] http://www.bakermckenzie.com/files/Publication/fcf2ef80-c7f6-4361-a782-

[11] Vía s.17 de su lucha contra el terrorismo y la Ley de Seguridad

datos adicionales acerca de las direcciones IP y el Ministerio del Interior ha consultado sobre la revisión de adquisición y divulgación de datos de comunicación y Retención de Comunicaciones de Datos Códigos de Prácticas en virtud del Reglamento de la Ley de los poderes de investigación de 2000 (RIPA). La consulta sobre los códigos de prácticas pretende tener en cuenta las observaciones formuladas por el Tribunal de Justicia Europeo que todas las personas, incluso a los que las comunicaciones deben ser cubiertos por el secreto profesional, pueden tener sus datos de comunicaciones interceptadas y almacenadas. . Serias preocupaciones se han planteado en relación con la falta de control judicial o independiente, y la propuesta de poderes sobre la retención de datos a aumentado.

En general, los proveedores de servicios públicos de comunicaciones y redes públicas de comunicaciones seguirán sujetas a las obligaciones de retención de datos nacionales, siempre y cuando las leyes nacionales aplicables no se invalidan en los Estados miembros. Baker & McKenzie comentan que es probable que la Comisión Europea va a renovar sus esfuerzos para establecer un marco legal para armonizar las disposiciones de los Estados miembros en materia de conservación de datos con el propósito de la investigación, detección y enjuiciamiento de delitos graves, teniendo en cuenta las consideraciones detalladas de proporcionalidad enumeradas por el Tribunal de Justic ia Europeo.

Es de esperar que, en el futuro, se establecerán nuevas (y "mejoradas") obligaciones de retención de datos en virtud del derecho de la UE, exigiendo a las empresas de telecomunicaciones de conservar datos, sujeto a estrictos requisitos de seguridad, en las instalaciones de almacenamiento de datos "en la Unión Europea ". Estos centros de datos deben estar sujetos a "control", llevado a cabo sobre la base de la legislación de la UE, por "una autoridad independiente."

Ya sea que la Comisión Europea va a optar por la armonización de las normas de retención de datos europeos sobre la base de otra directiva o por el uso del instrumento jurídico de "reglamento", es actualmente una cuestión abierta. Teniendo en cuenta el período de tiempo prolongado requerido para la transposición de una directiva a la legislación nacional y el resultado probable de un mosaico de normas nacionales diferentes, es posible que la Comisión Europea va a optar por un Reglamento de retención de datos, lo que tendría efectos jurídicos directos en todos los Estados miembros de la UE y no requiere mucho tiempo transposición a la legislación nacional.[12]

Cuarta parte: informe de las Naciones Unidas sobre Derechos Humanos y Terrorismo

El 23 de septiembre de 2014, la informe del Relator Especial[13] sobre la promoción y protección de los derechos humanos y las libertades fundamentales en la lucha contra el terrorismo se presentó a la Asamblea General.[14]

El Relator Especial describe el ritmo del cambio tecnológico como "dinámica", que "permitió a algunos Estados a asegurar el acceso mayor a las comunicaciones y datos de contenido sin sospecha previa. Unidos ahora son capaces de aplicar los algoritmos automatizados 'minería

[12] Baker & McKenzie newsletter April 2014
[13] Ben Emmerson
[14] http://s3.documentcloud.org/documents/1312939/un-report-on-human-rights-and-terrorism.pdf

de datos' para Dragnet un universo potencialmente ilimitada de tráfico de comunicaciones ".[15] El artículo 17 del Pacto Internacional de Derechos Civiles y Políticos dispone que cualquier interferencia en las comunicaciones privadas debe ser prescrita por la ley y deben ser un medio necesario y proporcionado para alcanzar un objetivo legítimo de política pública.[16] En opinión del Relator Especial, la existencia de programas de vigilancia de masas constituye un obstáculo capaz desproporcionada en el derecho a la intimidad.[17]

El Alto Comisionado para los Derechos Humanos informó el 30 de junio de 2014[18] y llegó a la conclusión de que la práctica de muchos Estados reveló una falta de legislación adecuada nacional y / o la ejecución, la debilidad de las garantías procesales y la supervisión ineficaz, lo que contribuye a la falta de rendición de cuentas por las injerencias arbitrarias o ilegales en derecho a la intimidad.

Quinta parte: FBE y Retención de Datos

La Comisión de Derechos Humanos de la FBE propone lo siguiente para la discusión como recomendaciones para la FBE para poner a la Unión Europea:

1. Comunicaciones sujetos a secreto profesional debe estar exento de las medidas de retención de datos a menos que una orden judicial ha sido concedida a acceder a los datos a los fines de la investigación, detección y enjuiciamiento de delitos graves;

2. Las comunicaciones que requieren secreto profesional legal deben ser identificados en la fuente;

3. Los Estados deben establecer criterios claros y transparentes para la conservación de datos de acuerdo con el propósito de la investigación, detección y enjuiciamiento de delitos graves;

4. Los datos que se retiene por los gobiernos se debe mantener en condiciones de seguridad;

5. Debe preverse la destrucción irreversible de datos después del período de retención;

6. Los Estados deben establecer organismos fuertes e independientes de supervisión que son los recursos adecuados;[19]

7. Los Estados deben establecer tribunales donde los individuos pueden buscar remedio eficaz para la presunta violación de sus derechos a la privacidad en línea; Los Estados deben establecer un mecanismo independiente que es capaz de llevar a cabo una revisión exhaustiva e imparcial;[20]

8. Los Estados deben establecer un mecanismo independiente que es capaz de llevar a cabo una revisión exhaustiva e imparcial;[21]

---

[15] Paragraph 8 UN Report on Protection and Promotion of human rights and fundamental freedoms while countering terrorism
[16] Paragraph 11 UN Report on Protection and Promotion of human rights and fundamental freedoms while countering terrorism
[17] Paragraph 18 UN Report on Protection and Promotion of human rights and fundamental freedoms while countering terrorism
[18] A/HRC/27/37
[19] Paragraph 61 of Special Rapporteur UN Report on Protection and Promotion of human rights and fundamental freedoms while countering terrorism
[20] Paragraph 61 of Special Rapporteur UN Report on Protection and Promotion of human rights and fundamental freedoms while countering terrorism
[21] Paragraph 61 of Special Rapporteur UN Report on Protection and Promotion of human rights and fundamental freedoms while countering terrorism

9. Todos los Estados miembros deben contar con una legislación que protege a almacenamiento y revelación de datos a tercera partes;

10. Los funcionarios públicos que trabajan en los gobiernos nacionales, regionales y locales deben estar vinculados por la misma protección de los datos en poder de los gobiernos;

11. Divulgación por un funcionario público debe llevar a sanciones penales;

12. La UE debe tener reglas para prevenir la interceptación de datos por parte de actores no estatales;

13. Los abogados deben publicar sus preocupaciones por el impacto en la sociedad, el impacto en el acceso a la justicia y el imperio de la ley, si la relación abogado-cliente se ha roto;

14. Debe haber una legislación nacional en los Estados miembros para consagrar los derechos digitales;

15. Debe haber una carta europea de derechos digitales;

16. Debe haber una carta mundial de los derechos digitales;

Sexta parte: Soluciones de Protección de prácticas para los abogados, algunas sugerencias:

Tor (el anonimato de la red) T O R: The Onion Router

Este es un software libre para permitir el anonimato en línea. Tor dirige el tráfico de Internet a través de una red de voluntarios en todo el mundo consiste en 5000 relés para ocultar la localización del usuario y el uso. Su uso está diseñado para proteger la privacidad de los usuarios, así como su capacidad de realizar comunicaciones confidenciales por mantener sus actividades en Internet.

El término "encaminamiento de cebolla" se refiere a capas de cifrado, como las capas de una cebolla. Tor cifra los datos originales, incluyendo la dirección IP de destino, varias veces y lo envía a través de un circuito virtual que comprende sucesivas repetidores Tor, seleccionados aleatoriamente. Cada relé descifra una capa de cifrado para revelar sólo el siguiente relevo en el circuito con el fin de transmitir los datos cifrados restantes. El relé última descifra la capa más interna de la encriptación y envía los datos originales a su destino sin revelar, o incluso saber, la dirección IP de origen. Debido a que el enrutamiento de la comunicación se oculta en parte en cada tramo en el circuito Tor, este método elimina cualquier punto en el que la comunicación se puede-des anónima a través de la vigilancia de la red que se basa en conocer su origen y destino. La independencia de aplicación de Tor que lo diferencia de la mayoría de otras redes de anonimato: funciona en el nivel corriente de Transmission Control Protocol (TCP).

Pretty Good Privacy (PGP)

PGP es un programa informático de cifrado y descifrado de datos que proporciona privacidad y autenticación para la comunicación de datos. PGP se utiliza para firmar, cifrar y descifrar los textos, correos electrónicos, archivos, directorios, y para aumentar la seguridad de las comunicaciones por correo electrónico. PGP se puede utilizar para enviar mensajes de

confidencialidad. PGP combina el cifrado de clave simétrica y el cifrado de clave pública. El mensaje se encripta utilizando un algoritmo de cifrado simétrico, lo que requiere una clave simétrica. Cada clave simétrica se utiliza sólo una vez (y también se llama una clave de sesión. El mensaje y su clave de sesión se envían al receptor. La clave de sesión se debe enviar al receptor para que sepan cómo descifrar el mensaje. Para proteger el mensaje durante la transmisión, que se cifra con la clave pública del receptor. Sólo la clave privada que pertenece al receptor puede descifrar la clave de sesión.

La Comisión de Derechos Humanos recomienda que los miembros FBE alientan las asociaciones de abogados en sus países para investigar y utilizar medios seguros de comunicación digital.

Professor Sara Chandler, Comisión de Derechos Humanos, con gracias a Timothy Hill, Colegio de Abogados de Inglaterra y Gales

UNIDAD III: INFORMATICA FORENSE

1.- La Cadena de Custodia Informático Forense.

Revista ACTIVA, ISSN 2027-8101. Núm 3, enero-junio 2012, pp. 67-81
Tecnológico de Antioquia, Medellín (Colombia)

La cadena de custodia informático-forense

Computer forensics chain of custody

Luis Enrique Arellano
Ing. Informático-Abogado-Licenciado en Criminalística
Universidad Tecnológica Nacional-Argentina

Carlos Mario Castañeda
Ingeniero de Sistemas MsC
Tecnológico de Antioquia

Recibido: 1 de marzo 2012
Aprobado: 1 de abril 2012

Resumen

La cadena de custodia tiene como finalidad brindarle soporte veraz a la prueba digital ante el juez, en medio de lo que se conoce como el debido proceso. Por tal motivo deben establecerse los procedimientos indicados para garantizar la idoneidad de los métodos aplicados para la sustracción de la evidencia informática. Así se garantiza una base efectiva para el juzgamiento y la validez ante cualquier fuero judicial internacional. Para esto, es necesario que se eviten suplantaciones, modificaciones, alteraciones, adulteraciones o simplemente su destrucción (común en la evidencia digital, ya sea mediante borrado o denegación de servicio). Procedimiento controlado y supervisable, la cadena de custodia informático-forense se aplica a los indicios materiales o virtuales relacionados con un hecho delictivo o no, desde su localización hasta su

Valoración por los encargados de administrar justicia. Este artículo lista los procedimientos en cada caso de recopilación de evidencia informática.

Palabras claves: Cadena de custodia, informática forense, validez de la prueba.

Abstract

The aim of the chain of custody is to provide digital evidence with a truthful stand before the judge, by following the established course of law. Thus an effective ground for judgment and validity before any other international court are guaranteed. To do that, it is important to avoid any forgery, modification, tampering or destruction of evidence (be it delete or denial of service). A controlled and monitorable procedure, the computer forensic chain of custody is applied to material and virtual evidence related to a criminal event or otherwise, from its finding all the way up to its appraisal. This paper lists all the procedures to be followed to gather computer evidence for forensic applications.

Keywords: Chain of custody, computer forensics, validity of evidence.

La preservación de la cadena de custodia sobre la prueba indiciaria criminalística es obligación de la totalidad de los miembros del poder judicial, los operadores del derecho y sus auxiliares directos. Entre estos últimos debemos incluir el personal de las fuerzas de seguridad, la policía judicial y el conjunto de peritos oficiales, de oficio y consultores técnicos o peritos de parte.

Así, la implementación de mecanismos efectivos de recopilación de evidencias debe incluir procedimientos que aseguren la confiabilidad de la información recolectada. Dicha confiabilidad incluye la trazabilidad, *(Establecer un mecanismo que permita realizar un seguimiento estricto de los elementos probatorios, desde su detección hasta el momento de su disposición definitiva)* la confidencialidad, la autenticidad, la integridad y el no repudio de los datos. En términos sencillos, implica establecer mecanismos de garantía de que los elementos probatorios ofrecidos como prueba documental informática son confiables, es decir, que no han sufrido alteración o adulteración alguna desde su recolección.

1. La cadena de custodia informático-forense

El juez debe poder confiar en dichos elementos digitales, por considerarlos auténticos "testigos mudos", desde el punto de vista criminalístico clásico y evaluarlos en tal sentido, guiado por la sana crítica, la prueba tasada o las libres convicciones, según sea el caso y la estructura judicial en que se desarrolle el proceso. Desde la detección, la identificación, la fijación, la recolección, la protección, el resguardo, el empaque y el traslado de la evidencia del lugar del hecho real o virtual, hasta la presentación como elemento probatorio, la cadena de custodia debe garantizar que la evidencia recolectada en la escena es la misma que se está presentando ante el evaluador o decisor.

Consideramos la cadena de custodia como un procedimiento controlado que se aplica a los indicios materiales (prueba indiciaria) relacionados con un hecho delictivo o no, desde su localización hasta su valoración, por parte de los encargados de administrar justicia y que busca asegurar la inocuidad y la esterilidad técnica en el manejo de los mismos, evitando alteraciones, sustituciones, contaminaciones o destrucciones, hasta su disposición definitiva por orden judicial.

Con este fin es necesario establecer un riguroso y detallado registro, que identifique la evidencia y sus poseedores, indicando el lugar, la hora, la fecha, el nombre y la dependencia involucrada en el secuestro, la interacción posterior y su depósito en la sede que corresponda (judicial o no).

Si carece de alguno de estos componentes, la prueba documental informática recolectada no habrá alcanzado el valor probatorio pretendido. Es importante considerar el valor de los indicios recabados en el proceso de investigación, análisis y argumentación del cual dependen. En este marco de referencia adquirirán relevancia y pertinencia; de ahí la necesidad de evitar en lo posible la impugnación de los mismos en razón de errores metodológicos propios de cada disciplina en particular, pues no es igual la cadena de custodia de muestras biológicas que la de armas o documentos impresos o virtuales. Por ejemplo, un acta de secuestro es un elemento genérico, pero el asegurar la integridad de la prueba mediante un digesto (Hash) sobre un archivo secuestrado es un elemento propio de la cadena de custodia informático-forense.

La prueba documental informática tiene características particulares que requieren tratamiento particular en la recolección, la preservación y el traslado. Estos son:

1. Consiste en indicios digitalizados, codificados y resguardados en un contenedor digital específico, es decir, toda información es almacenada (aun durante su desplazamiento por una red, está almacenada en una onda electromagnética).

2. Hay diferencias entre el objeto que contiene la información (discos magnéticos, ópticos, cuánticos, ADN, proteínas, etc.) y su contenido —la información almacenada—. Para este caso consideramos:

a. Información: Todo conocimiento referido a un objeto o hecho, susceptible de codificación y almacenamiento.

b. Objeto: Conjunto físicamente determinable o lógicamente definible.

3. La información puede presentarse en uno de los siguientes estados:

a. En almacenamiento: se encuentra en un reservorio a la espera de ser accedida (almacenamiento primario, secundario o terciario). Es un estado estático y conforma la mayoría de las recolecciones posibles; sin embargo, difiere de la mayoría de los indicios recolectables a la que puede accederse por medios locales o remotos.

b. En desplazamiento, es decir, viajando en un elemento físico determinado (cable, microonda, láser, etc.). Es susceptible de recolección mediante interceptación de dicho elemento y está condicionada por las mismas cuestiones legales que la escucha telefónica o la violación de correspondencia.

c. En procesamiento: es el caso más complicado y constituye la primera decisión que debe tomar el recolector. Ante un equipo en funcionamiento, donde la información está siendo procesada, es decir, modificada, actualizada y nuevamente resguardada, debe decidir si apaga o no el equipo. Esta decisión es crítica y puede implicar la pérdida de información y la destrucción de la prueba documental informática pretendida. *Es una decisión incierta. Si se decide mantener el equipo encendido, se corre el riesgo de haber sido detectado durante su aproximación al mismo, y que en realidad la actividad del mismo esté consistiendo en borrar de manera segura cualquier información almacenada (usando técnicas específicas de eliminación de la información que la hacen irrecuperable a los métodos informático-forenses), con lo que cuanto más tiempo permanezca el equipo funcionando mayor será el daño producido. Si, por el contrario, se decide apagar el equipo, es posible que el mismo tenga un mecanismo de seguridad ante estos eventos que dispare las mismas acciones de borrado detalladas, sobre los equipos remotos, eliminando enlaces y reservorios dentro de la misma red o en redes externas (es muy común que, con fines delictivos o no, la información sea almacenada en un reservorio remoto, lo que aumenta la seguridad y confiabilidad de la misma, ya que está exenta de los riesgos edilicios, físicos y lógicos, del local donde se utiliza). La mejor manera de solucionar este problema es la labor de inteligencia previa (ataques pasivos, consistentes en intercepción, escucha o análisis de tráfico, por medios remotos). Esta tarea resuelve el problema, pero demanda recursos técnicos y, sobre todo, humanos sumamente escasos. Por otra parte, debe ser autorizada judicialmente y la práctica nos indica que la mayoría de los Juzgados, por muy diversas causas, son sumamente reacios a autorizar estar intervenciones (lo mismo ocurre con las clásicas y siempre restringidas medidas previas o preliminares, aunque constituyan prueba anticipada y reúnan las condiciones requeridas para la misma: peligro en la demora, credibilidad del derecho invocado* —fumus bonis iuris— *y contracautela de privacidad).* La solución por medio del acceso remoto, indetectable por el accedido, es un tema que aún no se encuentra en discusión en nuestro país. *(Con los medios adecuados es perfectamente posible acceder a un equipo remoto y recolectar la información pretendida, preservando las condiciones legalmente establecidas en la Constitución Nacional y sus normas derivadas. Sin embargo, en un ambiente donde la diferencia entre el delito informático impropio (delitos clásicos cometidos utilizando medios informáticos) tipificado en la Ley 26.388 y el delito informático propio (que afecta al bien jurídico protegido: "información", algo que ni siquiera está contemplado en nuestro Código Penal) es un que solo manejan algunos*

ISSN 2027-8101, No. 3, enero-junio 2012

operadores del derecho especializados en derecho de alta tecnología, parece utópico esperar comprensión real de las particularidades que identifican al lugar del hecho virtual (propio e impropio) respecto del lugar del hecho real, en el campo jurídico en el mediano plazo).

El significado de la prueba depende de su inserción como elemento pertinente y conducente a la argumentación presentada como sustento de la pretensión jurídica manifestada. Esto sugiere que constituye un documento más, diferente de la prueba documental clásica (bibliográfica, foliográfica y pictográfica) únicamente en el soporte (digital vs. papel). Sin embargo, es necesario tener en cuenta que un bit no es similar, sino idéntico a otro bit. De ahí que una copia bit a bit de un archivo digital es indiferenciable de su original, esto significa que no puede establecerse cuál es el original y cuál su copia, salvo que hayamos presenciado el proceso de copiado y tengamos conocimiento sobre cuál era el contenedor del original y cuál el de la copia (método indirecto e independiente de los archivos considerados). Esto no resulta un inconveniente, sino más bien una ventaja desde el punto de vista de la cadena de custodia, ya que permite preservar las copias, manteniendo el valor probatorio del original y evitando riesgos para el mismo. Se puede entregar al perito una copia de los archivos debitados y preservar los mismos en su reservorio original en el local del tribunal y con las seguridades que este pueda ofrecerle (caja fuerte, por ejemplo). *(Si un documento en papel es reservado en secretaría, en la caja fuerte y luego se le debe realizar una pericia caligráfica, debe ser entregado al perito, porque sólo puede trabajar sobre originales. Esto implica la salida de la prueba, abandonando la protección del Tribunal, hasta que regrese al mismo, si durante ese desplazamiento es destruido en forma dolosa o culposa, la prueba se pierde. En cambio si la documental informática es resguardada en el tribunal (por ejemplo en un CD o DVD) y al perito se le entrega una copia de la misma, podrá realizar su tarea sin inconveniente y si su copia es destruida, en nada afecta al original resguardado en el Juzgado).*

Por el contrario, en la recolección física de prueba indiciaria tradicional, se secuestra el indicio y se lo traslada. En la recolección de documentación informática esta acción puede realizarse o no, ya que es suficiente con copiar bit a bit la prueba y luego trasladar dicha copia. Es una extensión del caso anterior, donde no es necesario entregar el original al perito, sino que alcanza con una copia. La recolección de prueba, mediante copia debidamente certificada, puede sustituir perfectamente al original; es aplicable a los casos en que la información esté almacenada en reservorios vitales para la operación de una determina entidad u organización estatal o privada.

Supongamos la necesidad de secuestrar información almacenada en uno de los servidores operativos del Banco Central, es evidente que el secuestro de dicho servidor, podría sacar de operación a la entidad con las consecuencias que dicho hecho implicaría, mientras que su copia, certificación mediante hash y ante la autoridad judicial, administrativa o notarial correspondiente, en nada afectaría a la continuidad del servicio y serviría perfectamente como elemento probatorio.

Los mecanismos de certificación digital (*hash*, firma electrónica, firma digital) son mucho más confiables y difíciles de falsificar que los mismos elementos referidos a la firma y certificación ológrafas. Sin embargo, el desconocimiento de los operadores del derecho ante el nuevo mundo virtual hace que tengan sensaciones de inseguridad sin sustento en la realidad matemática que brinda soporte a los mecanismos referidos. Por tal motivo, se adopta una actitud sumamente crítica y negativa frente a la seguridad que los mismos brindan, en parte como consecuencia de la necesidad implícita de confiar en algoritmos que no se conocen. Entender, comprender y analizar un algoritmo de cifrado por clave pública, es una tarea de expertos y que no está al alcance de una formación matemática básica como la que posee la mayoría de los operadores del derecho. Por otra parte, el individuo inserto en la sociedad

tiende más a confiar en la medicina (por eso no cuestiona los métodos del médico legista o del psiquiatra forense) que la matemática, con la que se relaciona mucho menos. *(Las posibilidades reales de ser engañados al comprar un libro por internet son mucho menores que sus similares ante un vendedor ambulante. Sin embargo, sentimos cierta aprensión al ingresar el código de seguridad de nuestra tarjeta de crédito para confirmar la compra, algo que ocurre mucho menos con los jóvenes y los adolescentes; es un problema generacional que se superará con el paso del tiempo).* Es un proceso lento de aceptación, que como todo en derecho seguramente llegará a posteriori del desarrollo social y tecnológico.

Como se indicó anteriormente, la cadena de custodia informático-forense tiene por objeto asegurar que la prueba ofrecida cumple con los requisitos exigibles procesalmente para la misma, y por ello debe garantizar:

1. Trazabilidad:
    a. Humana (determinación de responsabilidades en la manipulación de la prueba, desde su detección y recolección hasta su disposición final).
    b. Física (incluyendo la totalidad de los equipos locales o remotos involucrados en la tarea, sean estos de almacenamiento, procesamiento o comunicaciones).
    c. Lógica (descripción y modelización de las estructuras de distribución de la información accedida y resguardada).
2. Confiabilidad (integridad, autenticidad, confidencialidad, no repudio).

Cadena de custodia vs. privacidad

La cadena de custodia se constituye de hecho en un elemento que permite asegurar la confiabilidad de la información recolectada, que si bien implica la trazabilidad de la misma, no protege por sí sola al derecho a la privacidad. Este componente asegura que la prueba recolectada se pueda seguir metodológica y procesalmente desde su origen hasta su disposición final, pero nada dice respecto de la legalidad de la misma, mucho menos de su legitimidad.

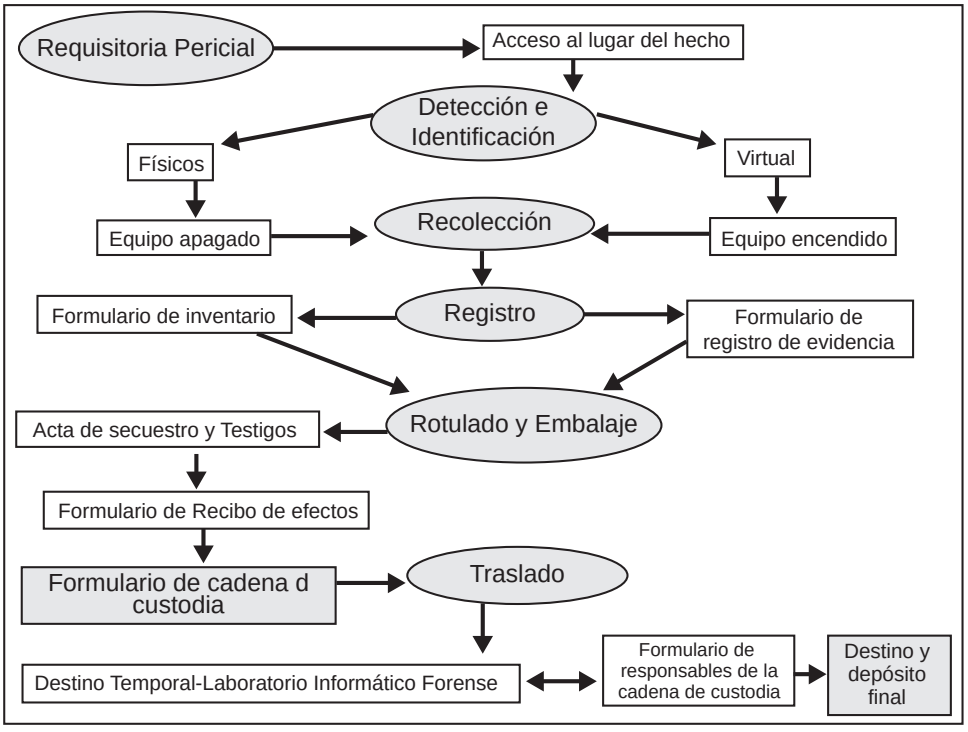
En efecto, la protección de la privacidad de la información no se conforma de manera exclusiva con la cadena de custodia. La privacidad requiere por supuesto confiabilidad, pero también respeto estricto de las normas procesales que resguardan el legítimo proceso asegurado constitucionalmente. Podríamos estar en presencia de una cadena de custodia bien realizada, con una trazabilidad adecuada, con preservación estricta criminalística, informática y procesal, pero que se haya realizado a partir de una acción ilegal o ilegítima. La condición de ilegalidad podría darse por falta de orden de allanamiento y secuestro previas a la recolección de prueba documental informática en una causa penal, y la ilegitimidad en el caso de la recolección de información propia, que excede los límites de lo permitido, accediendo no solo a la información estrictamente necesaria para asegurar la argumentación ofrecida, a efectos de justificar la pretensión litigada, resguardando otros elementos que nada tienen que ver con dicha cadena argumental-causal.

Protocolo para la cadena de custodia en la pericia informático-forense

La informática forense debe cumplir los requisitos generales establecidos en la inspección judicial en criminalística. En esta especialidad, los elementos dubitados pueden ser de tipo físico o virtual. En el caso de los elementos virtuales, la detección, la identificación y la recolección deberán efectuarse en tiempo real, es decir, en vivo, con el equipo encendido. La información es un elemento intangible que se encuentra almacenado en dispositivos que pueden ser volátiles o no. Con el fin de determinar la validez de la información contenida en los mencionados dispositivos será necesario efectuar la correspondiente certificación matemática por medio de un digesto o *hash*. Esta

comprobación es la que permitirá determinar la integridad de la prueba recolectada y su correspondencia con el elemento original.

El objetivo principal es preservar la evidencia. Por lo tanto, al acceder al lugar del hecho deberá: 1) identificar, 2) situar, 3) relacionar la información mediante un accionar metódico, sistemático y seguro, cuya consigna será: 1) rotular, 2) referenciar y 3) proteger.



Protocolo para la cadena de custodia en la pericia informático forense

En síntesis, la validez de la prueba informática depende del mantenimiento de la seguridad, de procurar el resguardo legal y del seguimiento de una metodología estricta. De este modo, en el lugar del hecho se deberá seguir una secuencia de pasos expresadas en el siguiente procedimiento que se considerará como etapa preliminar a la elaboración del formulario de la cadena de custodia, el cual debe ser considerado como información confidencial, clasificada y resguardada en un lugar seguro:

1. Detección, identificación y registro

En lo posible, debe identificarse la totalidad de los elementos informáticos dubitados —computadoras, red de computadoras, *netbook*, *notebook*, celular, iPad, GPS, etc.— y para ello realizar un inventario de hardware en la inspección y el reconocimiento judicial que quedarán consignados en el formulario registro de evidencia. Para ello, quien realice el procedimiento tendrá cuidado de:

a. Colocarse guantes.

b. Fotografiar el lugar del hecho o filmar todos los elementos que se encuentran en el área de inspección, desde la periferia hacia el área dubitada.

c. Fotografiar los elementos informáticos, determinando en cuál de ellos efectuar macro fotografía:

i. Pantallas del monitor del equipo dubitado.

ii. Vistas frontal, lateral y posterior, según corresponda.

iii. Números de series de los elementos informáticos, etiquetas de garantías.

iv. Periféricos, (teclados, mouse, monitor, impresoras, agendas PDA, videocámaras, video grabadora, PenDrive, dispositivos de almacenamiento en red, unidades de Zip o Jazz, celulares, iPod, etc.).

v. Material impreso en la bandeja de la impresora o circundante.

vi. Cableado.

vii. Dispositivos de conectividad, alámbricos e inalámbricos.

viii. Diagramas de la red y topologías.

d. Inventariar todos los elementos utilizando una planilla de registro del hardware, identificando: tipo, marca, número de serie, registro de garantía, estado (normal, dañado), observaciones particulares. *(Cfr. Inventario del hardware de la inspección judicial y el reconocimiento judicial – formulario de registro de evidencia de la computadora)*. Efectuar un croquis del lugar del hecho, especificando el acceso al lugar, la ubicación del o los equipos informáticos y de cualquier otro elemento, mobiliario, *racks*, cableado, existentes en el área a inspeccionar, para luego representarlo con cualquier herramienta de diseño.

2. Recolección de los elementos informáticos dubitados físicos o virtuales

El perito informático forense deberá recolectar la evidencia procediendo de manera acorde al origen del requerimiento de la pericia informático-forense, a saber:

1. Por orden judicial, cuyo texto indica:

   a. Secuestrar la evidencia para su posterior análisis en el laboratorio, el perito informático-forense procederá a:

      i. Certificar matemáticamente la evidencia.

      ii. Identificar y registrar la evidencia.

      iii. Elaborar un acta ante testigos.

      iv. Iniciar la cadena de custodia.

      v. Transportar la evidencia al laboratorio.

   b. Efectuar la copia de la evidencia para su posterior análisis en el laboratorio, el perito informático forense procederá a:

      i. Certificar matemáticamente la evidencia.

      ii. Duplicar la evidencia.

      iii. Identificar y registrar la evidencia y la copia.

      iv. Elaborar un acta ante testigos.

      v. Transportar la copia o duplicación de la evidencia al laboratorio.

2. Por solicitud particular de una persona específica, de una consultora, empresa, institución, organismo o por otros profesionales, el perito informático forense procederá a:

   a. Concurrir al lugar del hecho con un escribano público.

   b. Certificar matemáticamente la evidencia ante el escribano público.

   c. Duplicar la evidencia ante escribano público.

d. Solicitar al escribano que deje constancia en el acta de los motivos del secuestro, de los datos de la o las personas que solicitaron la pericia, las razones argumentadas y los fines pretendidos.

e. Solicitar una copia del acta realizada por el escribano.

f. Transportar la copia de la evidencia para su posterior análisis en el laboratorio

a. *Duplicación y autenticación de la prueba*

En ciertas situaciones el perito informático forense no podrá trasladar el equipamiento que contiene la información dubitada, por lo tanto deberá en el lugar del hecho efectuar la duplicación de la información contenida en su repositorio original. Esta tarea se deberá realizar de manera tal que la duplicación o copia generada preserve la validez de su contenido original.

A continuación se enuncian los pasos para efectuar la autenticación y duplicación de la prueba, el perito informático forense llevará en su maletín los dispositivos de almacenamiento limpios y desinfectados y el dispositivo de arranque (disco rígido externo, CD ROM, DVD, disquete) o inicio en vivo protegido contra escritura, que contiene el software de base seleccionado para la tarea y el software de autenticación y duplicación.

Las imágenes de los discos se deben realizar bit a bit para capturar la totalidad del disco rígido los espacios libres, no asignados y los archivos de intercambio, archivos eliminados y ocultos. Acorde a lo expresado por el NIST (National Institute of Standard and Technology), la herramienta utilizada para la generación de la imagen debe reunir ciertas especificaciones, como:

1. La herramienta deberá efectuar una imagen bit a bit de un disco original o de una partición en un dispositivo fijo o removible.

2. La herramienta debe asegurar que no alterará el disco original.

3. La herramienta podrá acceder tanto a discos SCSI como IDE.

4. La herramienta deberá verificar la integridad de la imagen de disco generada.

5. La herramienta deberá registrar errores tanto de entrada como de salida e informar si el dispositivo de origen es más grande que el de destino.

6. Se debe utilizar un bloqueador de escritura, preferiblemente por hardware, para asegurar la inalterabilidad del elemento de almacenamiento accedido.

La documentación de la herramienta deberá ser consistente para cada uno de los procedimientos. Esta imagen del disco se utilizará en la computadora del laboratorio para efectuar el análisis correspondiente.

1. Apagar el equipo desconectando el cable de alimentación eléctrica.

2. Retirar disquete, PenDrive, Zip.

3. Descargar la propia electricidad estática, tocando alguna parte metálica y abrir el gabinete.

4. Desconectar la interfaz o manguera de datos, puede ser IDE o SCSI.

5. Desconectar la alimentación eléctrica del dispositivo de disco rígido

6. Ingresar al CMOS (complementary metal oxide Semiconductor) o configuración del BIOS (sistema de entrada y salida de la computadora):

   i. Encender la computadora.

   ii. Oprimir el conjunto de teclas que se muestra en el monitor cuando se inicia la computadora para acceder al CMOS.

   iii. Verificar la fecha y hora del CMOS y registrarla en el formulario de recolección de evidencia. y documentar todo tipo de dato

que el perito informático forense considere relevante.

iv. Modificar la unidad de inicio o arranque del sistema operativo, es decir, seleccionar la unidad de disquete, CD-ROM / DVD o zip.

v. Guardar los cambios al salir.

8. Verificar la existencia de discos CD-ROM o DVD:

   a. Abrir la lectora o grabadora de CD-ROM o de DVD y quitar el disco pertinente.

9. Colocar la unidad de arranque, disquete, CD-ROM/DVD o zip en el dispositivo de hardware pertinente.

10. Verificar el inicio desde la unidad seleccionada.

11. Apagar el equipo.

12. Asegurar el dispositivo de almacenamiento secundario original —generalmente está configurado en el CMOS como master (maestro o primario) con protección de solo lectura—, mediante la configuración de los *jumpers* que indique el fabricante del disco o mediante el hardware bloqueador de lectura.

13. Conectar el cable plano al disco rígido, puede ser IDE o SCSI.

14. Conectar la alimentación eléctrica del dispositivo de disco rígido master.

15. Conectar el dispositivo que se utilice como destino para hacer la duplicación del disco rígido dubitado como *slave* —esclavo o secundario—, ya sea una controladora SCSI, un disco IDE esclavo o una unidad de cinta, o cualquier otro hardware utilizado para la duplicación de tamaño superior al disco original o dubitado. Si el almacenamiento secundario original es demasiado grande o es un arreglo de discos, efectuar la copia en cintas.

16. Verificar que en el dispositivo de arranque seleccionado se encuentren los controladores del hardware para la duplicación, en caso de que sean requeridos.

17. Encender la computadora iniciando desde la unidad de arranque configurada en el CMOS.

18. Efectuar la certificación matemática del dispositivo dubitado.

19. Guardar el resultado en un dispositivo de almacenamiento.

20. Registrar el resultado en el formulario verificación de la evidencia.

21. Duplicar el dispositivo de los datos con la herramienta de software y hardware seleccionada.

22. Efectuar, acorde al requerimiento de la pericia una o dos copias de la evidencia. En el caso de realizar dos copias, una se deja en el lugar del hecho, para permitir la continuidad de las actividades, otra copia se utiliza para el análisis en el laboratorio del perito informático forense y el original se deja en depósito judicial o si la pericia ha sido solicitada por un particular, registrarlo ante escribano público y guardarlo, según lo indicado por el solicitante de la pericia y el escribano público.

23. Efectuar la certificación matemática de la o las copias del dispositivo dubitado.

24. Guardar el resultado generado por las copias duplicadas en un dispositivo de almacenamiento.

25. Registrar el resultado generado por las copias duplicadas en el formulario de recolección de la evidencia.

26. Apagar el equipo.

27. Retirar los tornillos de sujeción del dispositivo de disco rígido.

28. Retirar el disco rígido con cuidado de no dañar el circuito electrónico.

3. Recolección y registro de evidencia virtual

a. Equipo encendido**:** En el caso de que se deba acceder a un equipo encendido, se debe considerar la obtención de los datos en tiempo real y de los dispositivos de almacenamiento volátil. Los dispositivos de almacenamiento volátil de datos pierden la información luego de interrumpirse la alimentación eléctrica, es decir al apagar la computadora la información almacenada se pierde.

Los datos que se encuentran en el almacenamiento volátil muestran la actividad actual del sistema operativo y de las aplicaciones, como por ejemplo: procesos en el estado de ejecución, en el estado de listo o bloqueado, actividad de la impresora (estado, cola de impresión), conexiones de red activas, puertos abiertos, (puerto es una estructura a la que los procesos pueden enviar mensajes o de la que pueden extraer mensajes, para comunicarse entre sí, siempre está asociado a un proceso o aplicación, por consiguiente sólo puede recibir de un puerto un proceso, recursos compartidos, estado de los dispositivos como discos rígidos, disqueteras, cintas, unidades ópticas.

Los datos volátiles están presentes en los registros de la unidad central de procesamiento del microprocesador, en la memoria caché, en la memoria RAM o en la memoria virtual.

Conjunto de tareas a realizar en el acceso a los dispositivos de almacenamiento volátil

1. Ejecutar un intérprete de comandos confiable o verificado matemáticamente.
2. Registrar la fecha, hora del sistema, zona horaria.
3. Determinar quién o quienes se encuentran con una sesión abierta, ya sea usuarios locales o remotos.
4. Registrar los tiempos de creación, modificación y acceso de todos los archivos.
5. Verificar y registrar todos los puertos de comunicación abiertos.
6. Registrar las aplicaciones relacionadas con los puertos abiertos.
7. Registrar todos los procesos activos.
8. Verificar y registrar las conexiones de redes actuales y recientes.
9. Registrar la fecha y hora del sistema
10. Verificar la integridad de los datos.
11. Documentar todas las tareas y comandos efectuados durante la recolección.

Posteriormente, en lo posible, se debe realizar una recolección más detallada de los datos existentes en el almacenamiento volátil, efectuando las siguientes tareas:

1. Examinar y extraer los registros de eventos.
2. Examinar la base de datos o los módulos del núcleo del sistema operativo.
3. Verificar la legitimidad de los comandos del sistema operativo.
4. Examinar y extraer los archivos de claves del sistema operativo.
5. Obtener y examinar los archivos de configuración relevantes del sistema operativo.
6. Obtener y examinar la información contenida en la memoria RAM del sistema.

Procedimiento

En la computadora, con el equipo encendido, acceder al recurso acorde al orden de volatilidad de la información, con las herramientas forenses almacenadas en disquete o cd-rom y de acceso de solo lectura:

1. Ejecutar un intérprete de comandos legítimo.
2. Obtener y transferir el listado de comandos

utilizados en la computadora, antes de la recolección de datos.

3. Registrar fecha y hora del sistema.
4. Recolectar, transferir a la estación forense o medio de recolección forense y documentar.
   a. Fecha y hora del sistema.
   b. Memoria principal.
   c. Usuarios conectados al sistema.
   d. Registro de modificación, creación y tiempos de acceso de todos los archivos.
   e. Listado de puertos abiertos y de aplicaciones escuchando en dichos puertos.
   f. Listado de las aplicaciones asociadas con los puertos abiertos.
   g. Tabla de procesos activos.
   h. Conexiones de red actuales o recientes.
   i. Recursos compartidos.
   j. Tablas de ruteo.
   k. Tabla de ARP.
   l. Registros de eventos de seguridad, del sistema, de las aplicaciones, servicios activos.
   m. Configuración de las políticas de auditoría del sistema operativo.
   n. Estadísticas del núcleo del sistema operativo.
   o. Archivos de usuarios y contraseñas del sistema operativo.
   p. Archivos de configuración relevantes del sistema operativo.
   q. Archivos temporales.
   r. Enlaces rotos.
   s. Archivos de correo electrónico.
   t. Archivos de navegación en internet.
   u. Certificación matemática de la integridad de los datos.
   v. Listado de los comandos utilizados en la computadora, durante la recolección de datos.
   w. Recolectar la topología de la red.

4. Si es factible, apagar el equipo.

b. Equipo apagado: En el caso que el perito informático forense efectúe la recolección de la evidencia en un equipo apagado, deberá previamente asegurarse que el dispositivo de inicio del equipo no se realice a través del disco rígido o dispositivo de almacenamiento secundario dubitado. Así mismo, deberá utilizar dispositivos de arranque en el modo solo lectura, con herramientas informáticas forenses para realizar la detección, recolección y registro de indicios probatorios.

Procedimiento

7. Apagar el equipo desconectando el cable de alimentación eléctrica
8. Retirar disquetes, PenDrive, Zip.
9. Descargar la propia electricidad estática, tocando alguna parte metálica y abrir el gabinete.
10. Desconectar la interfaz o manguera de datos, puede ser IDE o SCSI.
11. Desconectar la alimentación eléctrica del dispositivo de disco rígido.
12. Ingresar al CMOS (complementary metal oxide semiconductor) o configuración del BIOS (sistema de entrada y salida de la computadora):

a. Encender la computadora

b. Oprimir el conjunto de teclas que se muestra en el monitor cuando se inicia la computadora para acceder al CMOS.

c. Verificar la fecha y hora del CMOS y registrarla en el formulario de recolección de evidencia. y documentar todo tipo de dato que el perito informático forense considere relevante y documentarlo con fotografía, filmadora o en la lista de control.

d. Modificar la unidad de inicio o arranque del sistema operativo, es decir seleccionar la unidad de disquete, CD-ROM/DVD o ZIP de solo lectura con las herramientas informáticas forenses.

e. Guardar los cambios al salir.

8. Colocar la unidad de arranque, disquete, cd-rom/dvd o zip en el dispositivo de hardware pertinente.

9. Verificar el inicio desde la unidad seleccionada.

10. Apagar el equipo.

11. Acorde a la decisión del perito informático forense o a lo solicitado en la requisitoria pericial, se podrá realizar el *Procedimiento de duplicación y autenticación de la prueba,* explicado anteriormente o continuar con la lectura del dispositivo original, configurando el mismo con los jumpers que el fabricante indique como solo lectura o colocando un dispositivo de hardware de bloqueo de escritura.

12. Conectar el cable plano al disco rígido, puede ser IDE o SCSI.

13. Conectar la alimentación eléctrica del dispositivo de disco rígido.

14. Encender la computadora iniciando desde la unidad de arranque configurada en el CMOS.

15. Colocar el dispositivo de almacenamiento forense.

16. Efectuar la certificación matemática del dispositivo dubitado.

17. Guardar el resultado en un dispositivo de almacenamiento forense.

18. Registrar el resultado en el formulario de recolección de la evidencia.

19. Por medio del conjunto de herramientas informático forense, obtener la siguiente información del disco dubitado, documentarla y almacenarla en dispositivos de almacenamiento forense, para su posterior análisis, ya sea en el lugar del hecho o en el laboratorio:

a) Tipo de sistema operativo

b) Fecha, hora y zona horaria del sistema operativo

c) Versión del sistema operativo

d) Número de particiones

e) Tipo de particiones

f) Esquema de la tabla de particiones

g) Listado de todos los nombre de archivos, fecha y hora

h) Registro del espacio descuidado o desperdiciado.

i. Incluido el MBR

ii. Incluida la tabla de particiones

iii. Incluida la partición de inicio del sistema y los archivos de comandos

i) Registro del espacio no asignado

j) Registro del espacio de intercambio

k) Recuperación de archivos eliminados

l) Búsqueda de archivos ocultos con las palabras claves en el:

i. espacio desperdiciado

ii. espacio no asignado

iii. espacio de intercambio

iv. MBR y tabla de particiones

m) Listado de todas las aplicaciones existentes en el sistema

n) Búsqueda de programas ejecutables sospechosos

o) Identificación de extensiones de archivos sospechosas.

p) Listado de todos los archivos protegidos con claves.

q) Listado del contenido de los archivos de cada usuario en el directorio raíz y si existen, en los subdirectorios

r) Verificación del comportamiento del sistema operativo:

i. Integridad de los comandos

ii. Integridad de los módulos

iii. Captura de pantallas

20. Generar la autenticación matemática de los datos a través del algoritmo de hash al finalizar la detección, recolección y registro.

21. Conservar las copias del software utilizado

22. Apagar o dejar funcionando el equipo, esto dependerá de la requisitoria pericial.

Procedimiento para el resguardo de la prueba y preparación para su traslado

1. Disponer, según sea el caso, las pruebas obtenidas en una zona despejada, para su posterior rotulado y registro.

2. Registrar en el formulario de registro de la evidencia cada uno de los elementos dubitados, acorde a lo especificado en dicho formulario y agregando cualquier otra información que considere pertinente el perito informático forense.

3. Proteger:

   a. en bolsas antiestáticas los elementos informáticos de almacenamiento secundario, registrando: Fecha y hora del secuestro, tipo, número de serie del elemento si se puede obtener, capacidad de almacenamiento, apellido, nombre y documento de identidad del perito informático forense, firma del perito informático forense.

   b. en bolsas manufacturadas con filamentos de cobre y níquel para prevenir la interferencia de señales inalámbricas —celulares, GPS, etc.—

4. Proteger con plástico o con bolsas estériles cualquier otro elemento que considere relevante el perito informático forense y rotularlos con los datos pertinentes al elemento, apellido, nombre y documento de identidad del perito informático forense, firma del perito informático forense.

5. Elaborar el acta de secuestro acorde al formulario del recibo de efectos.

6. Colocar los elementos identificados y registrados en una caja o recipiente de traslado que asegure la suficiente rigidez, aislamiento térmico, electromagnético y protección para evitar daños accidentales en el traslado de los elementos probatorios.

7. Trasladar, en lo posible, los elementos secuestrados reunidos en un único recipiente, evitando la confusión, separación o pérdida durante su almacenamiento posterior.

5. Traslado de la evidencia de informática forense

El traslado de la evidencia tendrá como destino el laboratorio de informática forense correspondiente al organismo establecido en la requisito-

ria pericial. La permanencia en este laboratorio puede ser temporal, pero será necesario mantener la cadena de custodia mientras la prueba sea analizada por las entidades involucradas. Acorde a la evolución del proceso judicial donde se encuentra involucrada la prueba de informática forense, la prueba podrá ser posteriormente entregada y resguardada en un lugar o destino específico para su resguardo y depósito final o definitivo.

Nota importante: Es sumamente importante considerar que si bien la prueba documental informática constituye una especie del género prueba documental clásica (bibliográfica, foliográfica y pictográfica), de la cual solo difiere en el soporte (papel vs. digital), no significa que por esto escape a las consideraciones generales que le aporta la criminalística en su sentido más amplio.

Conclusiones

Suele ocurrir que como la realización de la certificación *in situ* por digesto matemático de los discos secuestrados (*hash*) es una tarea que consume mucho tiempo, se prefiere secuestrar los equipos, clausurarlos y dejar la tarea de validación y *hash* para un momento posterior, generalmente en el laboratorio pericial. Sin embargo, se suele preservar la prueba en las mismas condiciones en que fue encontrada en el momento de la recolección. Este criterio hace que al secuestrar equipos informáticos, se mantenga el disco conectado a su fuente de alimentación y a su cable de datos para *"no modificar la prueba y preservar las condiciones de secuestro"*.

Sin embargo, este es un error, pues pone en riesgo la integridad de los datos recolectados en el disco referido. En efecto, si el aislamiento posterior del equipo con las correspondientes fajas de clausura, deja resquicios accesibles, cualquier persona de manera intencional o accidental podrá acceder al disco y modificar su contenido. La experiencia indica que muchas veces es posible incluso retirar el disco o acceder al mismo sin romper las fajas de clausura colocadas. De ahí que sea preferible abrir el gabinete y desconectar físicamente el disco (alimentación y datos) —hecho que debe ser registrado en el acta de secuestro—, para protegerlo de accesos indeseados hasta el momento de la ruptura formal de las fajas, para realizar las tareas técnico-periciales encomendadas.

Esta apertura debe ser ejecutada con todos los requisitos procesales pertinentes: acta de apertura, presencia de testigos, comprobación de integridad de las fajas de clausura y desconexión de los discos insertos en el gabinete, todo lo cual debe quedar registrado en un acta de apertura, que constituye la contrapartida del acta de secuestro. Al finalizar la labor pericial, debe desconectarse nuevamente el disco y dejar registro de esta circunstancia en el acta que corresponda (tareas periciales efectuadas, registro, comprobación, etc.).

Haciendo una analogía, cuando se secuestra un arma, se privilegia la seguridad sobre la protección de la prueba, es decir, se descarga y se envían por separado los proyectiles, las vainas y la munición intacta, en especial para evitar accidentes; esto en nada afecta a la prueba. La misma atención se debe aplicar a la prueba documental informática resguardada en el disco: se debe privilegiar la protección de los datos sobre el mantenimiento de las condiciones de recolección a ultranza; basta con aclarar la acción efectuada para que el juez tenga conocimiento de lo ocurrido y su razón de ser técnica y procesal.

Algunas definiciones pertinentes

En referencia a estos actos, téngase en cuenta el correcto empleo de los siguientes vocablos o palabras claves para fines de lo explicado aquí:

> ***Expropiar*** (paras. de propio): Desposeer legalmente (de una cosa) a su propietario por razón de interés público.
>
> ***Confiscar:*** Apropiarse las autoridades competentes de lo implicado en algún delito: *"confiscar mercadería de contrabando"*.

Secuestrar: Ordenar el juez el embargo o retirada de la circulación de una cosa: *"secuestrar la edición de un periódico"*.

Decomisar: Incautarse el Estado como pena de las mercancías procedentes de comercio ilegal o los instrumentos del delito: *"se ha decomisado un kilo de heroína"*.

Incautar(se) (no existe el verbo incautar): (de *in* y *cautum*, multa) Dicho de una autoridad judicial o administrativa. Privar a alguien de sus bienes como consecuencia de la relación de estos con un delito, falta o infracción administrativa. Cuando hay condena firma se sustituye por la pena accesoria de comiso.

Referencias

[1] Arellano, Enrique y Darahuge, María E. (2011). Manual de informática forense. Buenos Aires: Errepar.

[2] Borghello, Cristian (2001). Seguridad informática. Implicancias e implementación. [versión electrónica] Disponible en: http://www.segu-info.com.ar/tesis/ [Consultado: octubre, 2012].

[3] Castañeda, Carlos M. (2012) Cibercriminal. s.l., s.e.

[4] Lucena, Manuel J. (2000). Criptografía y seguridad para computadores. 3ª. ed., [PDF] Disponible en: http://iie.fing.edu.uy/ense/asign/seguro/Criptografia.pdf [Consultado: octubre, 2012].

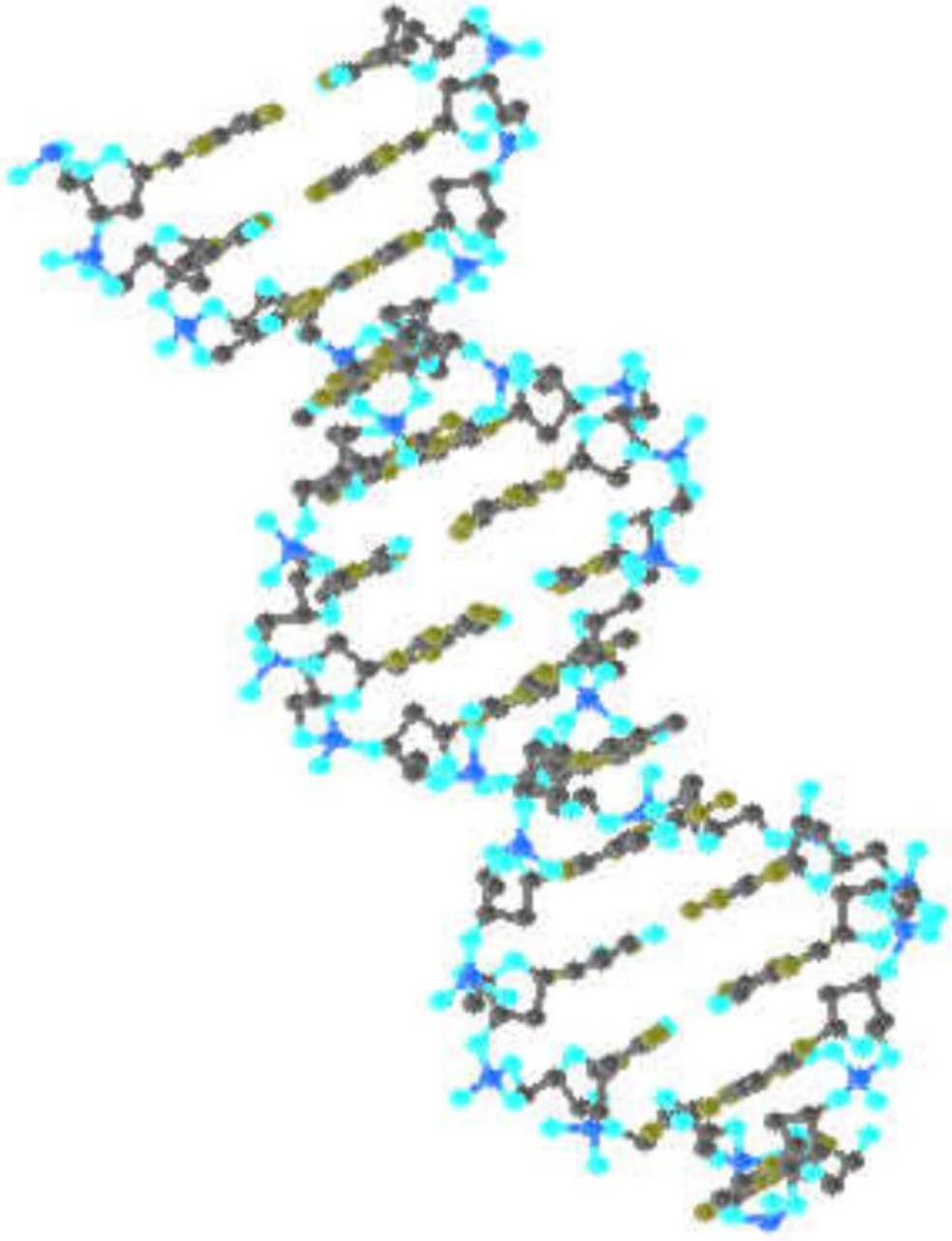
[5] Sies, John (2011). Delitos emergentes. s.l., s.e.

UNIDAD II: INFORMATICA FORENSE

2.- Análisis Forense Digital - Miguel López Delgado.

Análisis Forense Digital

Miguel López Delgado



Hackers & Seguridad

Edición 2ª - junio 2007

LICENCIA

Análisis Forense Digital
Computer Forensics

"Análisis Forense Digital"

Segunda Edición: **junio 2007, revisada y adaptada para su publicación en CriptoRed**
Primera Edición: **junio 2.006**

Autor: **Miguel López Delgado**
Ingeniero Técnico Industrial
Experto Profesional en Seguridad Informática
Web: www.codemaster.es
e-mail: codemaster@telefonica.net

A mis hijos Manuel y Paula, por ser una fuente constante de inspiración.

1
Índice

2
Introducción

Antecedentes

Un jueves por la tarde comienza a circular por Internet un nuevo "gusano". Éste aprovecha una vulnerabilidad de Microsoft Windows XP que había sido publicada oficialmente un par de semanas atrás y que se acompañó del correspondiente "parche". Se conoce que el "gusano" se extiende auto enviándose por e-mail usando todas las direcciones que encuentra en el sistema infectado, además está programado para generar diferentes nombres de archivos adjuntos y sus extensiones pueden variar, al tiempo que elige entre un centenar de asuntos y cuerpos de mensaje diferentes. Cuando el "gusano" infecta un sistema realiza una escalada de privilegios hasta obtener derechos de Administrador, realizando entonces la descarga, desde diferentes direcciones IP y vía FTP, de un agente para la ejecución de ataques de denegación de servicio distribuido (DDoS). Aunque los fabricantes de software antivirus alertan inmediatamente del "gusano" su expansión ha sido muy rápida y aún no se dispone de su firma. *Su organización ya ha sufrido una infección importante por la ejecución del "gusano" unas tres horas antes de que dispusiese de la firma para su antivirus y este se encuentra activo en algunos sistemas de su red.*

Ante un escenario de este tipo, podríamos hacernos las siguientes preguntas:

- ✓ ¿Tiene su organización un equipo de respuesta a incidentes como parte de su política de seguridad?
- ✓ ¿Es capaz de identificar los sistemas infectados y proceder a su desconexión y recuperación?
- ✓ ¿Podría informar y justificar a sus empleados una anulación temporal de sus cuentas de correo electrónico para su investigación?
- ✓ Si el ataque DDoS está programado para atacar al servidor Web de otra organización, por ejemplo a la mañana siguiente, ¿sería capaz de manejar una situación en la que dicha organización le pidiese responsabilidades tras detectar que el ataque se ha producido desde direcciones IP suyas?

Este tipo de situaciones no son ni mucho menos casos aislados o anecdóticos, según un estudio realizado por McAfee, compañía centrada en soluciones de prevención de intrusiones y de gestión de riesgos, revela el grado de desprotección de las organizaciones a la hora de gestionar su seguridad. Casi la mitad (el 45 por ciento) de los 600 ejecutivos TI europeos pertenecientes a compañías de más de 250 empleados encuestados durante el 2.005, afirmaron que su infraestructura informática nunca está protegida al 100 por cien frente a las vulnerabilidades.

La inclusión en la política de seguridad de procedimientos capaces de recibir, analizar y posteriormente responder a este tipo de incidentes, ya sean inminentes o en curso, se convierte en un componente indispensable de la infraestructura de los sistemas informáticos de la

organización, pues los ataques a dichos sistemas no sólo ha aumentado en número sino que también lo han hecho en variedad y capacidad destructiva.

Veremos a lo largo del presente trabajo, como la aplicación de técnicas forenses al análisis de sistemas proporciona una metodología adecuada en el proceso de respuesta ante incidentes.

Conceptos y terminología

Organizar un equipo de respuesta a incidentes requiere establecer, entre otros aspectos, unos procedimientos y métodos de análisis que nos permitan identificar, recuperar, reconstruir y analizar evidencias de lo ocurrido y una de las ciencias que cubren estas necesidades es la Ciencia Forense, la cual nos aporta las técnicas y principios necesarios para realizar nuestra investigación, ya sea criminal o no.

Si llevamos al plano de los sistemas informáticos a la Ciencia Forense, entonces hablamos de ***Computer Forensics***, o para nosotros **Análisis Forense Digital**. Esta disciplina es relativamente nueva y se aplica tanto para la investigación de delitos "tradicionales", (homicidios, fraude financiero, narcotráfico, terrorismo, etc.), como para los propiamente relacionados con las tecnologías de la información y las comunicaciones, entre los que destacan piratería de software y comunicaciones, distribución de pornografía infantil, intrusiones y "hacking" en organizaciones, spam, phishing, etc.

De manera más formal podemos definir el Análisis Forense Digital como un conjunto de principios y técnicas que comprende el proceso de adquisición, conservación, documentación, análisis y presentación de evidencias digitales y que llegado el caso puedan ser aceptadas legalmente en un proceso judicial. Por evidencia digital se entiende al conjunto de datos en formato binario, esto es, comprende los ficheros, su contenido o referencias a éstos (metadatos) que se encuentren en los soportes físicos o lógicos del sistema atacado.

Dentro del Análisis Forense Digital (en adelante AFD), podemos destacar las siguientes fases, que serán desarrolladas con más detalle a lo largo deeste documento:

1ª. Identificación del incidente.
2ª. Recopilación de evidencias.
3ª. Preservación de la evidencia.
4ª. Análisis de la evidencia.
5ª. Documentación y presentación de los resultados.

Por otro lado, hay que definir otro concepto importante, el de Incidente de Seguridad Informática, pues éste ha evolucionado en los últimos tiempos. En principio un incidente de este tipo se entendía como cualquier evento anómalo que pudiese afectar a la seguridad de la información, como podría ser una pérdida de disponibilidad, su integridad o confidencialidad, etc. Pero la aparición de nuevos tipos de incidentes ha hecho que este concepto haya ampliado su definición. Actualmente un **Incidente de Seguridad Informática** puede considerarse como una violación o intento de violación de la política de seguridad, de la política de uso adecuado o de las buenas prácticas de utilización de los sistemas informáticos.

Tras esta definición cabe ahora una categorización de dichos incidentes que nos aporte una base para su valoración y nos de una visión de cómo afrontarlos. Aunque se han propuesto varios tipos de clasificaciones sobre taxonomías de incidentes, no existe ningún consenso al respecto y ni mucho menos sobre cual de ellas es la más acertada. La que se propone a continuación tiene la finalidad de ayudar a una mejor comprensión de apartados siguientes del documento:

Incidentes de Denegación de Servicios (DoS): Son un tipo de incidentes cuya finalidad es obstaculizar, dañar o impedir el acceso a redes, sistemas o aplicaciones mediante el agotamiento de sus recursos.

Incidentes de código malicioso: Cualquier tipo de código ya sea, virus, gusano, "caballo de Troya", que pueda ejecutarse en un sistema e infectarlo.

Incidentes de acceso no autorizado: Se produce cuando un usuario o aplicación accede, por medio de hardware o software, sin los permisos adecuados a un sistema, a una red, a una aplicación o los datos.

Incidentes por uso inapropiado: Se dan cuando los usuarios se "saltan" la política de uso apropiado de las sistemas (por ejemplo ejecutando aplicaciones P2P en la red interna de la organización para la descarga de música).

Incidente múltiple: Se produce cuando el incidente implica varios de los tipos anteriores.

La mayoría de los incidentes que se dan en la realidad, pueden enmarcarse en varias de las categorías expuestas, por lo que una buena forma de identificarlos es por el **mecanismo de transmisión empleado**. Por ejemplo un virus que crea en el sistema atacado una puerta trasera debe ser manejado como un incidente de *código malicioso* y no como un acceso no autorizado, ya que el virus es el mecanismo de transmisión.

Prevención de ataques a sistemas

Detectar un ataque a sus sistemas informáticos antes de que se produzca, o en el peor de los casos en el instante en el que comienza, siempre será mejor que tener que recuperar el sistema recurriendo a sus copias de seguridad... por que las hace ¿verdad?.

Piense que es muy importante para proteger su actividad productiva, mantener el número de incidentes razonablemente bajo. Si sus controles de seguridad son insuficientes y sufre continuos ataques a sus sistemas, éstos pueden repercutir negativamente en sus actividad, tanto desde el punto de vista económico como el de imagen.

Existen multitud de libros y artículos que le proporcionarán información sobre como asegurar sus sistemas, y dado que este aspecto queda fuera del alcance del trabajo, se van a exponer de forma breve algunas recomendaciones para asegurar sus sistemas, redes, aplicaciones y datos.

- ✓ Disponer de una correcta gestión de parches y actualizaciones de su hardware y software, ya que gran parte de los ataques se basan en explotar un número reducido de vulnerabilidades en sistemas y aplicaciones.

- ✓ Asegurar los servidores basándose en el concepto de privilegio mínimo, esto es, configurarlos para que proporcionen un número limitado de servicios y con un nivel de acceso restringido según el tipo de usuario. Además deben evitarse configuraciones por defecto, como claves predefinidas, recursos compartidos, etc. También sería interesante disponer de medios de notificación al administrador cuando se produzcan accesos a niveles de privilegio no autorizados.
- ✓ Mantener la seguridad de la red, configurando un filtro perimetral en modo "paranoico", esto es, denegando cualquier tipo de acceso no autorizado expresamente, y manteniendo sólo el tráfico necesario para la actividad diaria normal. Esto incluirá instalación de cortafuegos, detectores de intrusos (IDS), monitores de red, uso de redes privadas virtuales (VPNs), uso de protocolos seguros (IPSec, SSL).
- ✓ Prevenir la ejecución de código malicioso (*malware*), utilizando programas antivirus capaces de parar este tipo de código como virus, caballos de Troya, gusanos y además "especies".
- ✓ Formar e informar a sus usuarios para que conozcan, acepten y sean capaces de aplicar las directrices de su política de seguridad. Hágales ver lo que ha ocurrido en otras organizaciones o entidades, cómo han "aprendido la lección", cómo ha afectado un incidente a sus actividades (y a sus sueldos). Informando y formando a los usuarios reducirá la frecuencia de los incidentes, sobre todo aquellos que impliquen la ejecución de código malicioso, o el saltarse la política de uso adecuado de los sistemas.

Preparación y respuesta ante incidentes

Si ya ha tomado las medidas descritas en el apartado anterior, y quizás alguna más, y aunque a nadie la agrade tener que preparar actuaciones ante desastres en sus sistemas informáticos, siendo realista, no estaría de más incluir dentro de su política de seguridad un **Plan de Respuesta ante Incidentes**. Éstos planes dependerán en gran medida de las características de su organización, y de su política, pero en base y sin extendernos en ello pues no es objetivo de este documento, deberían contener los siguientes puntos:

- ✓ Alcance, propósitos y objetivos del plan de acción.
- ✓ Estructura organizativa del equipo de respuesta a incidentes, responsabilidades, autoridad, departamentos implicados.
- ✓ Actuaciones para la contención del problema.
- ✓ Procedimientos de recuperación y restauración de sistemas SIN eliminación de posibles evidencias del ataque.
- ✓ Índices para la valoración de los daños, tanto desde el punto de vista económico como de imagen corporativa.
- ✓ Determinar en qué casos se tratará el incidente internamente y en qué casos se dará aviso a las Autoridades.
- ✓ Sopesar la contratación de personal externo para llevar a cabo la investigación.
- ✓ Establecer las fases de la investigación.
- ✓ Elaboración de informes y formularios tipo para comunicación del incidente tanto dentro como fuera de la organización si fuese necesario.

Por otro lado, y debido a que la recopilación de evidencias digitales puede llegar a ser una tarea bastante difícil, será necesario preparar sus sistemas para obtener buenos datos forenses. La implantación de procedimientos adecuados en la gestión de archivos, registros y

copias de seguridad pueden ayudar al quipo investigados en esta labor. Se exponen a continuación algunas recomendaciones:

- ✓ Conocer y monitorizar los parámetros de funcionamiento normal de los sistemas, tales como tráfico IP usual, carga de transacciones, ancho de banda consumido, usuarios conectados, etc.
- ✓ Utilizar un servidor de registros central y establecer una política de mantenimiento y retención de esos registros que permitan su estudio pasado el tiempo.
- ✓ Activar al máximo de detalle la información que contendrán los archivos de registro, lo que permitirá facilitar el proceso de reconstrucción de lo sucedido.
- ✓ Sincronizar todos los relojes de los servidores mediante, por ejemplo, el protocolo NTP (Network Time Protocol), permitiendo que los registros contengan todos la misma hora.
- ✓ Disponer de una base de conocimientos sobre incidentes, basta algo tan sencillo como enlaces páginas de software antivirus, o empresas y organizaciones especializadas en seguridad informática, así como suscribirse a sus listas e-mail de notificacionesde alertas y vulnerabilidades.
- ✓ Considere la experiencia como un factor irremplazable, esto le permitirá distinguir rápidamente un ataque de un simple problema técnico.

Aspectos legales

Si tras la realización de un primer análisis existen sospechas de que el incidente se ha provocado desde el interior de su red, tendrá que plantearse la posibilidad de llevar a cabo una investigación interna a la organización para depurar responsabilidades, bastará para este propósito recopilar información suficiente tanto en cantidad como calidad para poder tomar acciones disciplinarias posteriores, sin llegar a los tribunales. En esta situación además del equipo técnico de respuesta a incidentes, tendrá que contar con otros departamentos como el de Recursos Humanos e incluso con la Sección Sindical, pues no puede permitirse que por una mala gestión del caso el incidente se vuelva contra usted y acabe siendo acusado, por ejemplo, de despido improcedente.

Si los indicios llevan a su equipo forense a un ataque externo, habitualmente no merece la pena llevar a cabo acciones legales cuando los daños producidos son mínimos debido al alto coste económico que esto puede suponerle. Por ejemplo una deformación de su página Web corporativa que se subsana rápidamente o intentos de intrusión sin mayores consecuencias que algunas molestias para sus usuarios, pueden resolverse enviando un aviso de uso inapropiado al proveedor o proveedores de los servicios de conexión de los presuntos atacantes. Si documenta suficientemente bien su queja adjuntando históricos detallados de conexiones, del escaneado de sus equipos, etc., puede conseguir que el ISP desconecte o anule las cuentas de sus atacantes. La mayoría de los proveedores tienen direcciones de e-mail para estos casos y los más importantes suelen ser muy estrictos en cuanto a la política de uso de sus servicios.

Pero si el incidente, realizado por atacantes internos o externos, ha provocado daños importantes a su organización ya sean económicos, de imagen corporativa o su reputación ha quedado en entredicho, puede considerar abrir un proceso judicial contra sus atacantes. En este caso la investigación técnica deberá ser tratada como una investigación pericial técnica, incorporando procedimientos en materia de probatoria judicial, pues una evidencia digital no será considerada como prueba en un proceso judicial hasta que el juez así lo determine. Por

ello tendremos que convencerle de que hemos actuado de forma profesional, científica, veraz, con cautela e imparcial, y además explicárselo para que lo entienda pues es muy probable que el juez no tenga conocimientos avanzados en estos temas.

Para ampliar información sobre estos conceptos, en el Nuevo Código Penal, encontrará las siguientes referencias:

Ataques que se producen contra el derecho a la intimidad: Delito de descubrimiento y revelación de secretos mediante el apoderamiento y difusión de datos reservados registrados en ficheros o soportes informáticos. (Artículos del 197 al 201 del Código Penal).

Infracciones a la Propiedad Intelectual a través de la protección de los derechos de autor: Especialmente la copia y distribución no autorizada de programas de ordenador y tenencia de medios para suprimir los dispositivos utilizados para proteger dichos programas. (Artículos 270 y otros del Código Penal).

Falsedades: Concepto de documento como todo soporte material que exprese o incorpore datos. Extensión de la falsificación de moneda a las tarjetas de débito y crédito. Fabricación o tenencia de programas de ordenador para la comisión de delitos de falsedad. (Artículos 386 y ss. del Código Penal).

Sabotajes informáticos: Delito de daños mediante la destrucción o alteración de datos, programas o documentos electrónicos contenidos en redes o sistemas informáticos. (Artículo 263 y otros del Código Penal).

Fraudes informáticos: Delitos de estafa a través de la manipulación de datos o programas para la obtención de un lucro ilícito. (Artículos 248 y ss. del Código Penal).

Amenazas: Realizadas por cualquier medio de comunicación. (Artículos 169 y ss. del Código Penal).

Calumnias e injurias: Cuando se propaguen por cualquier medio de eficacia semejante a la imprenta o la radiodifusión. (Artículos 205 y ss. del Código Penal).

Pornografía infantil: Entre los delitos relativos a la prostitución al utilizar a menores o incapaces con fines exhibicionistas o pornográficos.

- La inducción, promoción, favorecimiento o facilitamiento de la prostitución de una persona menor de edad o incapaz. (art 187).
- La producción, venta, distribución, exhibición, por cualquier medio, de material pornográfico en en cuya elaboración hayan sido utilizados menores de edad o incapaces, aunque el material tuviere su origen en el extranjero o fuere desconocido. (art 189).
- El facilitamiento de las conductas anteriores (El que facilitare la producción, venta, distribución, exhibición, etc.) (art 189).
- La posesión de dicho material para la realización de dichas conductas.(art 189)

Fuente: Policía Nacional Española

Por otro lado, en cuanto a métodos de probatoria y demás tecnicismos legales se puede acudir a la Ley de Enjuiciamiento Criminal, La Nueva Ley de Enjuiciamiento Civil, etc.

3

Fases de un Análisis Forense Digital

Identificación del incidente: búsqueda y recopilación de evidencias

Una de las primeras fases del análisis forense comprende el proceso de identificación del incidente, que lleva aparejado la búsqueda y recopilación de evidencias.

Si sospecha que sus sistemas han sido comprometidos lo primero que tiene que hacer es ¡NO PERDER LA CALMA!, piense que no es el primero y que menos aún va a ser el último al que le ocurre. Antes de comenzar una búsqueda desesperada de señales del incidente que lo único que conlleve sea una eliminación de "huellas", actúe de forma metódica y profesional.

Asegúrese primero que no se trata de un problema de hardware o software de su red o servidor, no confunda un "apagón" en su router con un ataque DoS.

Descubrir las señales del ataque

Para iniciar una primera inspección del equipo deberá tener en mente la premisa de que debe conservar la evidencia, por ello NO HAGA NADA QUE PUEDA MODIFICARLA. Deberá utilizar herramientas que no cambien los sellos de tiempo de acceso (*timestamp*), o provoquen modificaciones en los archivos, y por supuesto que no borren nada.

Un inciso importante es que si no hay certeza de que las aplicaciones y utilidades de seguridad que incorpora el Sistema Operativo, o las que se hayan instalado se mantienen intactas deberemos utilizar otras alternativas. Piense que en muchos casos los atacantes dispondrán de herramientas capaces de modificar la información que el administrador verá tras la ejecución de ciertos comandos. Por ejemplo podrán ocultarse procesos o puertos TCP/UDP en uso. Cuestione siempre la información que le proporcionen las aplicaciones instaladas en un sistema que crea comprometido.

No estría de más en este momento crear un CD o DVD como parte de sus herramientas para la respuesta a incidentes, y si trabaja en entornos mixtos UNIX/Linux y Windows, tendrá que preparar uno para cada plataforma. Aunque existen gran cantidad de utilidades a continuación propongo una relación de aquellas que considero debería incluir en su ToolKit, y que le permitan, al menos, realizar las siguientes tareas:

- ✓ Interpretar comandos en modo consola (`cmd, bash`)
- ✓ Enumerar puertos TCP y UDP abiertos y sus aplicaciones asociadas (`fport, lsoft`)
- ✓ Listar usuarios conectados local y remotamente al sistema
- ✓ Obtener fecha y hora del sistema (date, time)
- ✓ Enumerar procesos activos, recursos que utilizan, usuarios o aplicaciones que los lanzaron (`ps, pslist`)

- ✓ Enumerar las direcciones IP del sistema y mapear la asignación de direcciones físicas MAC con dichas IP (`ipconfig, arp, netstat, net`)
- ✓ Buscar ficheros ocultos o borrados (`hfind, unrm, lazarus`)
- ✓ Visualizar registros y logs del sistema (`reg, dumpel`)
- ✓ Visualizar la configuración de seguridad del sistema (`auditpol`)
- ✓ Generar funciones hash de ficheros (`sah1sum, md5sum`)
- ✓ Leer, copiar y escribir a través de la red (`netcat, crypcat`)
- ✓ Realizar copias bit-a-bit de discos duros y particiones (`dd, safeback`)
- ✓ Analizar el tráfico de red (`tcpdump, windump`)

Supongamos que ya dispone de su ToolKit, ahora se hará la siguiente pregunta ¿dónde puedo buscar indicios de un ataque?. Evidentemente, uno de los primeros lugares donde comenzar la búsqueda de indicios es en los equipos que consideremos comprometidos pero no se limite sólo a éstos, piense que sus atacantes han podido borrar algunos registros locales en esos equipos, pero aún así, puede haber indicios en otras máquinas próximas tales como escaneado de puertos o tráfico inusual en cortafuegos y routers de la red.

Al iniciar la investigación nunca sabremos con qué nos vamos a topar, de hecho al principio puede que no se aprecie, a simple vista ninguna huella o indicio del ataque especialmente si para realizarlo han empleado e instalado en sus equipos un rootkit.

Como primera opción de búsqueda podemos realizar una verificación de integridad de los ficheros del sistema, utilidades como Tripwire o AIDE (Advance Intrusion Detection Enviroment) podrán arrojar algo de luz sobre sus sospechas. Otra opción es realizar una serie de verificaciones sobre del equipo.

Primero sería interesante conocer los procesos que se están ejecutando actualmente en el equipo, en busca de alguno que le resulte extraño, deberán llamarnos la atención aquellos que consuman recursos en exceso, con ubicaciones poco frecuentes en el sistema de archivos, que mantengan conexiones de red en puertos TCP o UDP no habituales, etc.

Este último punto nos llevará a realizar otra comprobación de interés, listar todos los puertos TCP y UDP abiertos además de los procesos (PID), usuarios y aplicaciones que los utilizan, siempre con la idea de identificar actividad no usual, recuerde la importancia de que el administrador conozca muy bien los parámetros de actividad normal del sistema. La aparición en el listado de procesos sin nombre o que emplean puertos altos (por encima del 1024) pueden ser indicios de la ejecución de un *troyano* o puerta trasera (backdoor) en el equipo. Una buena opción sería buscar en Internet (especialmente en Google) alguna referencia sobre el puerto o proceso que le resulta sospechoso.

Si tras estas consultas sus temores aumentan, pase ahora a editar los archidos de registro del sistema y logs en busca de entradas y avisos sobre fallos de instalación, accesos no autorizados, conexiones erróneas o fallidas, etc. Dependiendo de la plataforma que emplee encontrará estos archivos en distintas ubicaciones.

> **Microsoft Windows:** Este sistema operativo le proporciona un entorno para realizar estas pesquisas puede consultar, si considera que se trata aún de una aplicación segura, dentro del menú Herramientas administrativas, el Visor de sucesos, el de Servicios o el de la Directiva de seguridad local. Si no entiende bien la información que estos visores le

aporten puede consultar la base de datos de ayuda de Microsoft. Otro lugar donde se esconde gran cantidad información es el registro de Windows. La aplicación del sistema `regedit.exe` puede ayudarle en esta tarea, pero si no se fía de ella use las herramientas de su CD tales como `reg` (permite hacer consultas al registro sin modificarlo), o `regdmp` (exporta el registro en formato de texto plano, .txt), para su posterior consulta. En estos archivos tendrá que buscar "una aguja en un pajar", debido a la ingente cantidad de información que almacena y que se mezcla. Un punto de partida podría ser buscar en las claves del registro Run, RunOnce, RunOnceEx, RunServices, RunServicesOnce, Winlogon, pues bajo estas claves se encuentran los servicios, programas y aplicaciones que se cargarán en el inicio del sistema. Si ve algo raro, acuda nuevamente a Google.

UNIX/Linux: En este tipo de sistemas se dispone de una serie de archivos de registro (logs), que podremos encontrar habitualmente bajo el directorio `/var/log`, siendo los más importantes los que se detallan a continuación:

`/var/log/messages`	contiene los mensajes generales del sistema
`/var/log/secure`	guarda los sistemas de autenticación y seguridad
`/var/log/wmtp`	guarda un historial de inicio y cierres de sesión pasadas
`/var/run/utmp`	guarda una lista dinámica de quien ha iniciado la sesión
`/var/log/btmp`	guarda cualquier inicio de sesión fallido o erróneo (sólo para Linux)

Además los programas y aplicaciones crean normalmente sus propios archivos de registro, que podrá encontrar bajo el directorio `/var`. Todos estos archivos están en modo texto, por lo que podrá utilizar cualquier editor o visor de texto para buscar indicios del ataque. Observe el siguiente fragmento de un archivo `/var/log/messages`, en una máquina comprometida:

```
.....
Aug 22 23:37:55 localhost ftpd[7020]: FTP session closed
Aug 23 00:12:15 localhost ftpd[7045]: FTP session closed
Aug 23 00:19:19 localhost ftpd[7046]: FTP session closed
Aug  22  22:21:05  localhost  ftpd[7049]:  Anonymous  FTP  login  from
200.47.186.114 [200.47.186.114], mozilla@
Aug  22  22:22:48  localhost  ftpd[7052]:  Anonymous  FTP  login  from
200.47.186.114 [200.47.186.114], mozilla@
Aug 23 00:25:03 localhost kernel: Kernel logging (proc) stopped.
Aug 23 00:25:03 localhost kernel: Kernel log daemon terminating.
.....
```

¿No aprecia nada raro?, fíjese en la 4ª y 5ª entradas del archivo, éste parece haber sido modificado pues aparece un salto en la secuencia de fechas, con dos entradas fechadas el 22 de agosto tras dos entradas con fecha 23 de agosto. Este tipo de detalles, aunque no son determinantes, si pueden ser síntomas de que han estado "trasteando" en sus sistemas.

Además de estos archivos de registro, también pueden contener indicios los archivos de claves, usuarios y grupos, podrá encontrarlos en `/etc/passwd`, `/etc/shadow`,

`/etc/group`. También pude encontrar indicios de actividad anómala al editar el archivo `/root/.bash_history` que contiene los comandos ejecutados por el usuario roo el intérprete vas.

Para el propósito inicial de confirmación del ataque o compromiso de sus sistemas estas primeras pesquisas serán suficientes, aunque tendrá que volver a utilizar de forma más exhaustiva estos datos tal y como veremos en el apartado de análisis de evidencias.

Recopilación de evidencias

Bien, ya está seguro de que sus sistemas informáticos han sido atacados. En este punto deberá decidir cuál es su prioridad:

A.- Tener nuevamente operativos sus sistemas rápidamente.
B.- Realizar una investigación forense detallada.

Piense que la primera reacción de la mayoría de los administradores será la de intentar devolver el sistema a su estado normal cuanto antes, pero esta actitud sólo hará que pierda casi todas las evidencias que los atacantes hayan podido dejar en "la escena del crimen", eliminando la posibilidad de realizar un análisis forense de lo sucedido que le permita contestar a las preguntas de ¿qué?, ¿cómo?, ¿quién?, ¿de dónde? y ¿cuándo? se comprometió el sistema, e impidiendo incluso llevar a cabo acciones legales posteriores si se diese el caso. Esto también puede que le lleve a volver a trabajar con un sistema vulnerable, exponiéndolo nuevamente a otro ataque.

Si no está seguro de lo que está haciendo, ¡NO HAGA NADA!, y póngase en contacto con expertos en la materia.

Asumamos que elige el *"Plan B"*, que el análisis forense es su prioridad y que está capacitado para realizarlo, así que a partir de ahora tendrá que seguir una serie de pasos encaminados a **recopilar evidencias** que le permitan determinar el método de entrada al sistema, la actividad de los intrusos, su identidad y origen, duración del compromiso y todo ello extremando las precauciones para evitar alterar las evidencias durante el proceso de recolección.

Este es un buen momento para hacerse con un cuaderno donde comenzar a tomar apuntes detallados de todas las operaciones que realice sobre los sistemas atacados, no se fíe de su memoria, anote la fecha y hora de inicio y fin de cada uno de los pasos que dé, anote también características como números de serie de cada equipo, de sus componentes, de su S.O., etc. No escatime en la recopilación de datos incluso haga fotografías de los equipos y del entorno, nunca se sabe si tendrá que vérselas con sus atacantes en un juicio, y cualquier evidencia puede ser definitiva. También sería recomendable que le acompañase otra persona durante el proceso de recopilación de evidencias, ésta actuaría como testigo de sus acciones, así que si es alguien imparcial mejor, y si puede permitirse que le acompañe un Notario mejor que mejor, recuerde los requisitos legales para que una evidencia pase a ser considerada como prueba en un juicio. No sería la primera vez que un excelente análisis técnico de un incidente es rechazado en un juicio por no guardar las debidas garantías procesales.

Ahora que ya está preparado para la recolección de evidencias tendrá que decidir si comienza a tomar muestras sobre el sistema "vivo" o "muerto". Tenga presente que en el sis-

tema habrá pruebas ocultas con diferentes niveles de volatilidad, como los registros del procesador, estructuras de datos en la memoria RAM o memoria de tipo caché, conexiones de red activas, usuarios y procesos actuales, sistema de archivos, etc. Será muy difícil reunir toda esta información a la vez y gran parte de esta se perderá si decide apagar el equipo de la forma habitual, ya que en este proceso se realizan una serie de pasos programados para cerrar el sistema de forma limpia, pero si además el atacante ha instalado las herramientas adecuadas éste podría eliminar, modificar y sustituir ficheros a su antojo durante el apagado, y se "limpiarán" también del equipo las huellas de su atacante. Además si el atacante sigue on-line, puede detectar su actividad y actuar con una acción evasiva o, peor aún, destructiva eliminando todo tipo de información. Pero si por la severidad del ataque o por la importancia de los datos comprometidos decide apagar el equipo, no lo dude ¡DESCONÉCTELO DIRECTAMENTE DE LA RED ELÉCTRICA!, si ha leído bien, de esta forma perderá la información volátil de la RAM, micro, etc. Pero conservará aún bastante información sobre el ataque.

Supongamos que puede mantener su equipo "vivo" un poco más, comience a recopilar evidencias siguiendo el orden de mayor a menor volatilidad. Este proceso se describe muy bien e el RFC 3227, .Estableceremos el siguiente orden de volatilidad y por tanto de recopilación de evidencias:

- ✓ Registros y contenidos de la caché.
- ✓ Contenidos de la memoria.
- ✓ Estado de las conexiones de red, tablas de rutas.
- ✓ Estado de los procesos en ejecución.
- ✓ Contenido del sistema de archivos y de los discos duros.
- ✓ Contenido de otros dispositivos de almacenamiento.

Observe que los cuatro primeros puntos representan un tipo de datos, volátil, que se perderán o modificarán si apaga o reinicia el sistema, es por tanto muy fácil eliminar evidencias de forma inadvertida.

Dentro de las evidencias volátiles será de interés recuperar los siguientes datos del sistema en tiempo real:

- ✓ Fecha y hora.
- ✓ Procesos activos.
- ✓ Conexiones de red.
- ✓ Puertos TCP/UDP abiertos y aplicaciones asociadas "a la escucha".
- ✓ Usuarios conectados remota y localmente.

Durante este proceso de recopilación de evidencias, tendrá que hacer uso de su Tool-Kit, pero como se indicó anteriormente, deberá tener precaución pues el atacante aún puede estar fisgoneando por sus sistemas. Con un buen entrenamiento será capaz de recopilar toda esta información con un número de comandos mínimo, haciendo su labor casi desapercibida, incluso sería recomendable que tuviese preparado un script en Perl para sistemas UNIX/Linux o un archivo de proceso por lotes para entornos Windows que realizase todas estas operaciones de forma automatizada y que, además, enviase la información a un lugar seguro.

Y ahora viene otra cuestión , a la hora de recopilar estas evidencias volátiles, ¿dónde las almacenamos?, ¿dónde está ese lugar seguro?. Las salidas de algunos comandos pueden ocupar poco espacio, pero otros pueden generar tal cantidad de información que sea necesario

el uso de medios de almacenamiento con una capacidad considerable (desde cientos de Mbytes hasta decenas de Gbytes). Una Opción interesante sería usar discos externos USB, muy económicos y que le permiten gran flexibilidad de manejo y transporte de grandes cantidades de información. Otra opción es emplear herramientas de transmisión de datos por la red tipo `netcat`, que le permitiría enviar toda la información recopilada a un sistema seguro, como por ejemplo un equipo conectado en la misma red o un portátil conectado directamente al sistema afectado.

En cualquier caso tenga en cuenta el siguiente consejo, NUNCA almacene la información volátil en el equipo comprometido con la idea de recuperarla más tarde para su análisis... ¡puede que ya no esté ahí cuando vuelva a buscarla!.

Tan pronto como haya obtenido toda la información volátil del sistema tendremos que recopilar la información contenida en los discos duros, teniendo en cuenta que estos dispositivos no sólo contienen las particiones, los archivos, directorios, etc. Sino que también contienen otro tipo de datos que hacen referencia a los propios archivos y a flujos de información, son los metadatos que serán de gran importancia en el análisis forense.

En este punto cabe hacer una aclaración muy importante, cuando se realiza una **copia de seguridad** de un disco o soporte en general se procede a copiar los archivos tal cual el sistema operativo los “ve”, perdiéndose gran cantidad de información oculta en el disco. Por el contrario si realizamos una **imagen del disco**, creamos una copia bit-a-bit del disco original preservando toda la información que contenga, incluyendo los bloques de los ficheros eliminados, espacio libre tras cada bloque, inodos (metadatos), etc.

Como norma general, obtendremos siempre imágenes de los discos duros para su posterior análisis y, siempre sobre medios de sólo lectura.

Una de las herramientas más empleadas en entornos UNIX/Linux es `dd`, ésta permite crear imágenes de discos bit-a-bit, además de ofrecer otras opciones como obtención del hash MD5 de la copia, etc. Si además la combinamos con la herramienta `netcat`, podríamos transferir las imágenes completas a través de la red.

Preservación de la evidencia

Aunque el primer motivo que le habrá llevado a la recopilación de evidencias sobre el incidente sea la resolución del mismo, puede que las necesite posteriormente para iniciar un proceso judicial contra sus atacantes y en tal caso deberá documentar de forma clara cómo ha sido preservada la evidencia tras la recopilación. En este proceso, como se expondrá a continuación, es imprescindible definir métodos adecuados para el almacenamiento y etiquetado de las evidencias.

Muy bien, ya tenemos la **evidencia del ataque**, ahora veremos que ha de continuar siendo metódico y sobre todo conservando intactas las “huellas del crimen”, debe asegurar esa evidencia a toda costa, por lo tanto ¡NI SE LE OCURRA COMENZAR EL ANÁLISIS SOBRE ESA COPIA!.

Como primer paso deberá realizar dos copias de las evidencias obtenidas, genere una suma de comprobación de la integridad de cada copia mediante el empleo de funciones *hash*

tales como MD5 o SHA1. Incluya estas firmas en la etiqueta de cada copia de la evidencia sobre el propio CD o DVD, incluya también en el etiquetado la fecha y hora de creación de la copia, nombre cada copia, por ejemplo "COPIA A", "COPIA B" para distinguirlas claramente del original. Traslade estos datos a otra etiqueta y péguela en la caja contenedora del soporte, incluso sería conveniente precintar el original para evitar su manipulación inadecuada.

Si además decide extraer los discos duros del sistema para utilizarlos como evidencia, deberá seguir el mismo procedimiento, coloque sobre ellos la etiqueta "EVIDENCIA ORIGINAL", incluya además las correspondientes sumas *hash*, fecha y hora de la extracción del equipo, datos de la persona que realizó la operación, fecha, hora y lugar donde se almacenó, por ejemplo en una caja fuerte. Piense, además, que existen factores externos como cambios bruscos de temperatura o campos electromagnéticos que pueden alterar la evidencia. Toda precaución es poca, incluso si decide enviar esos discos a que sean analizados por empresas especializadas solicite que los aseguren por un importe similar a los daños causados en sus equipos.

Otro aspecto a tener en cuenta, y que está relacionado con el comentario anterior, es el proceso que se conoce como la **cadena de custodia**, donde se establecen las responsabilidades y controles de cada una de las personas que manipulen la evidencia. Deberá preparar un documento en el que se registren los datos personales de todos los implicados en el proceso de manipulación de las copias, desde que se tomaron hasta su almacenamiento. Sería interesante documentar:

- ✓ Dónde, cuándo y quién manejo o examinó la evidencia, incluyendo su nombre, su cargo, un número identificativo, fechas y horas, etc.
- ✓ Quién estuvo custodiando la evidencia, durante cuanto tiempo y dónde se almacenó.
- ✓ Cuando se cambie la custodia de la evidencia también deberá documentarse cuándo y como se produjo la transferencia y quién la transportó.

Todas estas medidas harán que el acceso a la evidencia sea muy restrictivo y quede claramente documentado, posibilitando detectar y pedir responsabilidades ante manipulaciones incorrectas a intentos de acceso no autorizados.

Análisis de la evidencia

Una vez que disponemos de las **evidencias digitales** recopiladas y almacenadas de forma adecuada, pasemos a la fase quizás más laboriosa, el Análisis Forense propiamente dicho, cuyo objetivo es reconstruir con todos los datos disponibles la línea temporal del ataque o *timeline*, determinando la cadena de acontecimientos que tuvieron lugar desde el instante inmediatamente anterior al inicio del ataque, hasta el momento de su descubrimiento.

Este análisis se dará por concluido cuando conozcamos cómo se produjo el ataque, quién o quienes lo llevaron a cabo, bajo qué circunstancias se produjo, cuál era el objetivo del ataque, qué daños causaron, etc.

En el siguiente apartado se describirá este **proceso de análisis** empleando las herramientas propias del sistema operativo que se emplee como anfitrión y las que recopiló en su ToolKit, de esta forma se pretende dar una visión amplia del proceso que ayudará a compren-

der mejor el funcionamiento de las herramientas específicas para el análisis forense de sistemas que se expondrán más adelante.

Preparación para el análisis: El entorno de trabajo

Antes de comenzar el **análisis de las evidencias** deberá acondicionar un entorno de trabajo adecuado al estudio que desee realizar. Si se decanta por no tocar los discos duros originales ¡muy recomendable!, y trabajar con las imágenes que recopiló como evidencias, o mejor aún con una copia de éstas, tenga en cuenta que necesitará montar esas imágenes tal cual estaban en el sistema comprometido.

Si dispone de recursos suficientes prepare dos estaciones de trabajo, en una de ellas, que contendrá al menos dos discos duros, instale un sistema operativo que actuará de anfitrión y que le servirá para realizar el estudio de las evidencias . En ese mismo ordenador y sobre un segundo disco duro, vuelque las imágenes manteniendo la estructura de particiones y del sistema de archivos tal y como estaban en el equipo atacado. En el otro equipo instale un sistema operativo configurado exactamente igual que el del equipo atacado, además mantenga nuevamente la misma estructura de particiones y ficheros en sus discos duros. La idea es utilizar este segundo ordenador como "conejillo de Indias" y realizar sobre él pruebas y verificaciones conforme vayan surgiendo hipótesis sobre el ataque.

Si no dispone de estos recursos, puede utilizar software como VMware, que le permitirá crear una plataforma de trabajo con varias máquinas virtuales (varios equipos lógicos independientes funcionando sobre un único equipo físico). También puede decantarse por una versión LIVE de sistemas operativos como Linux, que le permitirá interactuar con las imágenes montadas pero sin modificarlas. Pero si tuvo la "feliz idea" de hacer que su ToolKit en CD o DVD fuese autoarrancable, ahora es el momento de utilizarlo.

Si está muy seguro de sus posibilidades y de lo que va a hacer, puede conectar los discos duros originales del sistema atacado a una estación de trabajo independiente para intentar hacer un análisis "en caliente" del sistema, deberá tomar la precaución de montar los dispositivos en modo sólo lectura, esto se puede hacer con sistemas anfitriones UNIX/Linux, pero no con entornos Windows.

Reconstrucción de la secuencia temporal del ataque

Supongamos que ya tenemos montadas las imágenes del sistema comprometido en nuestra estación de trabajo independiente y con un sistema operativo anfitrión *de confianza*. El primer paso que deberá dar es crear una línea temporal de sucesos o *timeline*, para ello recopile la siguiente información sobre los ficheros:

- ✓ Inodos asociados.
- ✓ Marcas de tiempo MACD (fecha y hora de modificación, acceso, creación y borrado).
- ✓ Ruta completa.
- ✓ Tamaño en bytes y tipo de fichero.
- ✓ Usuarios y grupos a quien pertenece.
- ✓ Permisos de acceso.
- ✓ Si fue borrado o no.

Sin duda esta será la información que más tiempo le llevará recopilar, pero será el punto de partida para su análisis, podría plantearse aquí dedicar un poco de tiempo a preparar un *script* que automatizase el proceso de creación del *timeline*, empleando los comandos que le proporciona el sistema operativo y su ToolKit.

Para comenzar ordene los archivos por sus fechas MAC, esta primera comprobación, aunque simple, es muy interesante pues la mayoría de los archivos tendrán la fecha de instalación del sistema operativo, por lo que un sistema que se instaló hace meses y que fue comprometido recientemente presentará en los ficheros nuevos, inodos y fechas MAC muy distintas a las de los ficheros más antiguos.

La idea es buscar ficheros y directorios que han sido creados, modificados o borrados recientemente, o instalaciones de programas posteriores a la del sistema operativo y que además se encuentren en rutas poco comunes. Piense que la mayoría de los atacantes y sus herramientas crearán directorios y descargarán sus "aplicaciones" en lugares donde no se suele mirar, como por ejemplo en los directorios temporales.

A modo de guía céntrese primero en buscar los archivos de sistema modificados tras la instalación del sistema operativo, averigüe después la ubicación de los archivos ocultos y écheles un vistazo a ver dónde están y de qué tipo son, busque también los archivos borrados o fragmentos de éstos, pues pueden ser restos de logs y registros borrados por sus atacantes. Aquí cabe destacar nuevamente la importancia de realizar imágenes de los discos pues podremos acceder al espacio residual que hay detrás de cada archivo, (recordemos que los ficheros suelen almacenarse por bloques cuyo tamaño de *clúster* depende del tipo de sistema de archivos que se emplee), y leer en zonas que el sistema operativo *no ve*.

Piense que está buscando "una aguja en un pajar", por lo que deberá ser metódico, vaya de lo general a lo particular, por ejemplo parta de los archivos borrados, intente recuperar su contenido, anote su fecha de borrado y cotéjela con la actividad del resto de los archivos, puede que en esos momentos se estuviesen dando los primeros pasos del ataque.

Sin perder de vista ese *timestamp* anterior, comience a examinar ahora con más detalle los ficheros *logs* y de registros que ya ojeó durante la búsqueda de indicios del ataque, intente buscar una correlación temporal entre eventos. Piense que los archivos log y de registro son generados de forma automática por el propio sistema operativo o por aplicaciones específicas, conteniendo datos sobre accesos al equipo, errores de inicialización, creación o modificación de usuarios, estado del sistema, etc. Por lo que tendremos que buscar nuevamente entradas anómalas y compararlas con la actividad de los ficheros. Edite también el archivo de contraseñas y busque la creación de usuarios y cuentas extrañas sobre la hora que considere se inició el compromiso del sistema

Siguiendo con el ejemplo que se expuso en el apartado 3.1.1., en el fragmento del archivo `/var/log/messages` se detectaron dos accesos FTP, al examinar la actividad de los ficheros se descubrió que sobre esa fecha y hora se crearon varios archivos bajo el directorio `/var/ftp` de la máquina comprometida (directorio raíz del servicio ftp en sistemas UNIX/Linux), que además había sido borrado por el atacante. Al ser recuperado, se encontró la descarga de archivos que eran propiedad de usuario root (administradores del sistema) surgiendo la pregunta ¿qué hacía el administrador descargando archivos a esas horas?, el archivo recuperado era un conocido *rootkit*, se comprobó mediante el estudio del archivo de registro, que momentos después el atacante descomprimió, compiló y ejecutó sus "herramientas", acto

seguido (segundos después) se observa que un gran número de archivos de comandos del sistema operativo son modificados.

Este pequeño ejemplo es representativo de cómo ha de utilizar el *timestamp* para hacerse una idea más o menos certera de la cadena de eventos que se produjo.

Determinación de cómo se realizó el ataque

Una vez que disponga de la cadena de acontecimientos que se han producido, deberá determinar cuál fue la vía de entrada a su sistema, averiguando qué vulnerabilidad o fallo de administración causó el agujero de seguridad y que herramientas utilizó el atacante para aprovecharse de tal brecha. Estos datos, al igual que en el caso anterior, deberá obtenerlos de forma metódica, empleando una combinación de consultas a archivos de logs, registro, claves, cuentas de usuarios, etc.

Un buen punto de partida es repasar los servicios y procesos abiertos que recopiló como evidencia volátil, así como los puertos TCP/UDP y conexiones que estaban abiertas cuando el sistema estaba aún "vivo". Examine con más detalle aquellas circunstancias que le resultaron sospechosas cuando buscó indicios sobre el ataque, y realice con ellos un búsqueda de vulnerabilidades a través de Internet, emplee Google o utilice páginas específicas donde encontrará perfectamente documentadas cientos de vulnerabilidades, como por ejemplo el CERT, www.cert.org o en la base bugtraq en www.securityfocus.com.

Siguiendo con el ejemplo anterior, se sospechaba que al ataque se inició a través del servicio FTP que ejecutaba la máquina comprometida, se conocía una vulnerabilidad en dicho servicio y al realizar la consulta correspondiente se descubrió que efectivamente, ésta máquina era vulnerable pues no había sido instalado el parche de seguridad correspondiente, ¿recuerda el punto 1 del apartado Prevención de ataques a sistemas?. Pero no se confíe piense que si existía esa vulnerabilidad puede que haya otras, realice el proceso de búsqueda cuantas veces crea necesario, se imagina que ocurriría si volviese a instalar el sistema y dejase otra brecha de seguridad.

Si ya tiene claro cuál fue la vulnerabilidad que dejó su sistema "al desnudo", vaya un paso más allá y busque en Internet algún *exploit* anterior a la fecha del compromiso, que utilice esa vulnerabilidad. Generalmente lo encontrará en forma de rootkit y un buen lugar donde comenzar su búsqueda es, nuevamente, Google aunque también le será de utilidad anotar la siguiente dirección www.packetstormsecurity.org.

En este punto es muy importante que sea metódico, refuerce cada una de sus hipótesis empleando una formulación causa-efecto, también es el momento de arrancar y comenzar a utilizar nuestra máquina "conejillo de Indias". Pruebe sobre ella los exploits que ha encontrado, si he leído bien, NO TENGA MIEDO, recuerde que en el análisis forense una premisa es que los hechos han de ser reproducibles y sus resultados verificables, por lo tanto compruebe si la ejecución de ese exploit sobre una máquina igual que la comprometida y en perfecto estado (causa posible), genera los mismos eventos que ha encontrado entre sus evidencias (efecto verificable).

Si no es tan atrevido, puede recurrir a las bases de datos sobre ataques de los *honeypots*, herramientas de seguridad informática (implantadas por hardware o por software), cuya intención es atraer a crackers o spammers, simulando ser sistemas vulnerables o débiles a los

ataques, permitiendo recoger información sobre los atacantes y sus técnicas, permitiendo un examen en profundidad del atacante, durante y después del ataque al honeypot.

Identificación del autor o autores del incidente

Si ya ha logrado averiguar cómo entraron en sus sistemas, ahora le toca saber quién o quiénes lo hicieron. Para este propósito le será de utilidad consultar nuevamente algunas evidencias volátiles que recopiló en las primeras fases, revise las conexiones que estaban abiertas, en qué puertos y qué direcciones IP las solicitaron, además busque entre las entradas a los logs de conexiones. También puede indagar entre los archivos borrados que recuperó por si el atacante eliminó alguna huella que quedaba en ellos.

La **identificación de sus atacantes** será de especial importancia si tiene pensado llevar a cabo acciones legales posteriores o investigaciones internas a su organización. Si no va a seguir estos pasos, puede saltarse esta fase y dedicar ese tiempo a otros menesteres, como por ejemplo recuperar completamente el sistema atacado y mejorar su seguridad.

Pero si decide perseguir a sus atacantes, deberá realizar algunas pesquisas como parte del proceso de identificación. Primero intente averiguar la dirección IP de su atacante, para ello revise con detenimiento los registros de conexiones de red y los procesos y servicios que se encontraban a la escucha. También podría encontrar esta información en fragmentos de las evidencias volátiles, la memoria virtual o archivos temporales y borrados, como restos de e-mail, conexiones fallidas, etc.

Si cree tener una IP sospechosa, compruebe en el registro RIPE NCC (www.ripe.net) a quién pertenece. Pero ojo, no saque conclusiones prematuras, muchos atacantes falsifican la dirección IP con técnicas de *spoofing*. Suponga que encuentra una dirección IP y tras consultar el registro RIPE, le aparece que está asignada a una importante entidad bancaria ¿cree sinceramente que un empleado de banca le ha atacado?. Otra técnica de ataque habitual consiste en utilizar “ordenadores zombis”, éstos son comprometidos en primera instancia por el atacante y posteriormente son utilizados como lanzaderas del ataque final sin que sus propietarios sepan que están siendo cómplices de tal hecho. Por ello, para identificar a su atacante tendrá que verificar y validar la dirección IP obtenida.

También puede emplear **técnicas hacker**, eso sí ¡DE FORMA ÉTICA!, para identificar a su atacante, piense que si este dejó ejecutándose en el equipo comprometido “un regalito” como una puerta trasera o un troyano, está claro que en el equipo del atacante deberán estar a la escucha esos programas y en los puertos correspondientes, bien esperando noticias o buscando nuevas víctimas. Aquí entra en juego nuevamente nuestro ordenador “conejillo de indias”.

Si procede de esta forma, use una de las herramientas más impresionantes y baratas que encontrará `nmap`, este “mapeador de redes” es una utilidad de código abierto (por lo tanto gratuita) para exploración de redes y auditoría de seguridad. Se diseñó para analizar rápidamente grandes redes, aunque funciona muy bien contra equipos individuales. Nmap utiliza paquetes IP "crudos" de forma novedosa, para determinar qué equipos se encuentran disponibles en una red, qué servicios (nombre y versión de la aplicación) ofrecen, qué sistemas operativos (y sus versiones) ejecutan, qué tipo de filtros de paquetes o cortafuegos se están utilizando y así hasta como docenas de características.... Una auténtica joya para los analistas de sistemas.

En este apartado también cabe la posibilidad de adentrarse en los "bajos fondos" de Internet para intentar buscar a sus atacantes, pues en ocasiones algunos de ellos se jactan de sus hazañas públicamente en foros y Chat, visite estos lugares y verá lo que uno puede llegar a aprender.

Otro aspecto que le interesaría averiguar es el perfil de sus atacantes, aunque sin entrar en detalles podrá encontrarse con los siguientes tipos de "tipos":

Hackers: Son los más populares y tienen hasta su propia película (*HACKERS* de Iain Softley, 1995). Se trata de personas con conocimientos en técnicas de programación, redes, Internet y sistemas operativos. Sus ataque suelen tener motivaciones de tipo ideológico (pacifistas, ecologistas, anti globalización, anti Microsoft, etc.) o simplemente lo consideran como un "desafío intelectual".

SciptKiddies: Son una nueva especie que ha saltado a la escena de la delincuencia informática recientemente. Se trata de jóvenes que con unos conocimientos aceptables en Internet y programación emplean herramientas ya fabricadas por otros para realizar ataques y "ver que pasa". Su nombre viene de su corta edad y del uso intensivo que haces de los scrpts (guiones) de ataque que encuentran por Internet.

Profesionales: Son personas con muchísimos conocimientos en lenguajes de programación, en redes y su equipamiento (routers, firewall, etc.), Internet y sistemas operativos tipo UNIX. Suelen realizar los ataques taques bajo encargo, por lo que su forma de trabajar implica una exhaustiva preparación del mismo, realizando un estudio meticuloso de todo el proceso que llevará a cabo, recopilando toda la información posible sobre sus objetivos, se posicionará estratégicamente cerca de ellos, realizará un tanteo con ataques en los que no modificará nada ni dejará huellas... cuando lo tenga todo bien atado entonces atacará... pero tranquilo, este tipo de atacantes se encuentra muy poco y además se dedica a dar grandes golpes.

Evaluación del impacto causado al sistema

Para poder evaluar el impacto causado al sistema, el análisis forense le ofrece la posibilidad de investigar qué es lo que han hecho los atacantes una vez que accedieron a sus sistemas. Esto le permitirá evaluar el compromiso de sus equipos y realizar una estimación del impacto causado. Generalmente se pueden dar dos tipos de ataques:

Ataques pasivos: en los que no se altera la información ni la operación normal de los sistemas, limitándose el atacante a fisgonear por ellos.
Ataques activos, en los que se altera, y en ocasiones seriamente, tanto la información como la capacidad de operación del sistema.

Deberá tener en cuanta, además otros aspectos del ataque como los efectos negativos de tipo técnico que ha causado el incidente, tanto inmediatos como potenciales además de lo crítico que eran los sistemas atacados. Por ejemplo ataques al cortafuegos, el router de conexión a Internet o Intranet, el servidor Web corporativo, los servidores de bases de datos, tendrán diferente repercusión según el tipo de servicio o negocio que preste su organización y las relaciones de dependencia entre sus usuarios. Piense que una manipulación de una Web corporativa que realiza funciones meramente publicitarias tendrá un impacto mucho menor

que si eso mismo ocurre por ejemplo en eBay, que su negocio está basado totalmente en las subastas por Internet y un parón en su servidor Web puede traducirse en miles de euros de pérdidas por cada hora.

Puede también recurrir a métodos como BIA (Bussines Impact Analysis) que le indicarán como determinar el impacto de eventos específicos, permitiéndole valorar los daños en cantidades monetarias, que podrá presentar dado el caso, a su compañía de seguros.

Pero no piense sólo en los daños y pérdidas actuales, sino que tendrá que pensar en daños potenciales, si no conoce qué actividades han llevado a cabo los atacantes, no sabrá hasta dónde han podido "fastidiarle" sus sistemas, o peor aún, hasta dónde pueden llegar, pues ¿qué ocurriría si desconoce que su atacante consiguió descargarse un archivo que contenía datos de carácter personal de sus empleados?, y peor aún, ¿qué pasaría si el atacante alardeando de su proeza publica esos ficheros en Internet?. Pues bien, el artículo 44.3.h de la Ley Orgánica 15/1999,de 13 de Diciembre, de Protección de Datos de Carácter Personal se lo aclarará rápidamente:

"Artículo 44. Tipos de infracciones

...

3. Son infracciones graves:

...

h) Mantener los ficheros, locales, programas o equipos que contengan datos de carácter personal sin las debidas condiciones de seguridad que por vía reglamentaria se determinen.

...."

Sólo comentar que las sanciones para este tipo de infracciones son de 60.000 a 600.000 €.

Documentación del incidente

Tan pronto como el incidente haya sido detectado, es muy importante comenzar a tomar notas sobre todas las actividades que se lleven a cabo. Cada paso dado debe ser documentado y fechado desde que se descubre el incidente hasta que finalice el proceso de análisis forense, esto le hará ser más eficiente y efectivo al tiempo que reducirá las posibilidades de error a la hora de gestionar el incidente.

Por otro lado, cuando se haya concluido el análisis y durante éste, tendrá que mantener informados a las personas adecuadas de la organización, por lo que será interesante que disponga de diversos métodos de comunicación. Además como se verá necesitará tener preparados una serie de formularios y presentar tras la resolución del incidente al menos dos tipos de informes uno Técnico y otro Ejecutivo.

Utilización de formularios de registro del incidente

Al hilo de lo comentado anteriormente, el empleo de formularios puede ayudarle bastante en este propósito. Éstos deberán ser rellenados por los departamentos afectados por el compromiso o por el propio equipo que gestionará el incidente. Alguno de los formularios que debería preparar serán:

- ✓ Documento de custodia de la evidencia.
- ✓ Formulario de identificación del equipos y componentes.
- ✓ Formulario de incidencias tipificadas.
- ✓ Formulario de publicación del incidente.
- ✓ Formulario de recogida de evidencias.
- ✓ Formulario de discos duros.

El Informe Técnico

Este informe consiste en una exposición detallada del análisis efectuado. Deberá describir en profundidad la metodología, técnicas y hallazgos del equipo forense. A modo de orientación, deberá contener, al menos, los siguientes puntos:

- ✓ Antecedentes del incidente.
- ✓ Recolección de los datos.
- ✓ Descripción de la evidencia.
- ✓ Entorno del análisis .
  - Descripción de las herramientas.
- ✓ Análisis de la evidencia .
  - Información del sistema analizado .
    - Características del SO.
    - Aplicaciones.
    - Servicios.
    - Vulnerabilidades.
    - Metodología.
- ✓ Descripción de los hallazgos.
  - Huellas de la intrusión.
  - Herramientas usadas por el atacante.
  - Alcance de la intrusión.
  - El origen del ataque
- ✓ Cronología de la intrusión.
- ✓ Conclusiones.
- ✓ Recomendaciones específicas.
- ✓ Referencias.

El Informe Ejecutivo

Este informe consiste en un resumen del análisis efectuado pero empleando una explicación no técnica, con lenguaje común, en el que se expondrá los hechos más destacables de lo ocurrido en el sistema analizado. Constará de pocas páginas, entre tres y cinco, y será de especial interés para exponer lo sucedido a personal no especializado en sistemas informáticos, como pueda ser el departamento de Recursos Humanos, Administración, e incluso algunos directivos. En este informe deberá, donde se describir, al menos, lo siguiente:

- ✓ Motivos de la intrusión.
- ✓ Desarrollo de la intrusión
- ✓ Resultados del análisis.
- ✓ Recomendaciones.

4

Herramientas para Análisis Forense Digital

Hasta ahora se han desarrollado las fases del análisis forense de sistemas centrándonos en la utilización bien herramientas del sistema operativo o las propias del ToolKit que creamos como parte de nuestro plan de respuestas ante incidentes, por lo que hemos realizado la investigación de forma manual. Pero habrá podido comprobar que una de las dificultades que se encontrará el investigador a la hora de analizar determinadas evidencias digitales es que los atacantes emplean cada vez herramientas más sigilosas y perfeccionadas para realizar sus asaltos. Por lo tanto no estará de más disponer de un conjunto de herramientas específicas para el análisis de evidencias que nos ayudaran a completar de forma más eficiente nuestra investigación.

Dejando a parte el software comercial, en el que podrá encontrar herramientas específicas como EnCase de la empresa Guidance Software, considerado un estándar en el análisis forense de sistemas, nos centraremos en herramientas de código abierto (Open Source) que podrá descargar libremente desde la página sus correspondientes autores o miembros del proyecto.

Software de Libre Distribución y Open Source

Vamos a comenzar con una recopilación de herramientas que necesitan ser ejecutadas bajo un sistema operativo anfitrión, bien sea MS Windows o UNIX/Linux.

The Forensic ToolKit

Se trata de una colección de herramientas forenses para plataformas Windows, creado por el equipo de Foundstone. Puede descargarlo desde www.foundstone.com, donde además encontrará gran cantidad de herramientas de seguridad. Este ToolKit le permitirá recopilar información sobre el ataque, y se compone de una serie aplicaciones en línea de comandos que permiten generar diversos informes y estadísticas del sistema de archivos a estudiar. Para poder utilizarlos deberá disponer de un intérprete de comandos como cmd.exe.

Comando	Función
`afind`	Realiza búsqueda de archivos por su tiempo de acceso, sin modificar la información de acceso al mismo.
`hfind`	Busca archivos ocultos en el Sistema Operativo.
`sfind`	Busca flujos de datos ocultos en el disco duro, éstos son distintos de los archivos ocultos y no aparecerán con herramientas normales del sistema operativo. Su importancia radica en que pueden usarse para ocultar datos o software dañino.
`filestat`	Ofrece una lista completa de los atributos del archivo que se le pase como argumento (uno cada vez).
`hunt`	Permite obtener información sobre un sistema que utiliza las opciones de sesión NULL, tal como usuarios, recursos compartidos y servicios.

The Sleuth Kit y Autopsy

Este conjunto, cuyo autor es Brian Carrier, consiste en una colección de herramientas forenses para entornos UNIX/Linux, que incluye algunas partes del conocido The Coroners ToolKit (TCT) de Dan Farmer. Puede analizar archivos de datos de evidencias generadas con utilidades de disco como por ejemplo dd. Pese a ser de libre distribución (puede descargarlo del sitio Web www.sleuthkit.org) ofrece más detalle que algunos programas de pago. Incluye funciones como registro de casos separados e investigaciones múltiples, acceso a estructuras de archivos y directorios de bajo nivel y eliminados, genera la línea temporal de actividad de los archivos (timestamp), permite buscar datos dentro de las imágenes por palabras clave, permite crear notas del investigador e incluso genera informes... y mucho más.

Este ToolKit puede funcionar conjuntamente con el Autopsy Forensic Browser, consistente en una interfaz gráfica que le facilitará notablemente su labor a la par que le permitirá generar vistosos salidas gráficas para sus informes.

Para analizar sus datos empleando este ToolKit dedique el tiempo necesario a su configuración inicial, que luego agradecerá, pues dispondrá de una poderosa herramienta forense para organizar y estudiar sus evidencias. Debido a la gran cantidad de opciones se necesitaría un documento solamente dedicado a esta herramienta, así que a modo de resumen, algunas de las funciones básicas con las que podrá contar son las siguientes opciones de análisis:

Opción	Descripción
Análisis de archivos	Muestra la imagen como archivos y directorios, permitiendo ver incluso aquellos que estarían ocultos por el sistema operativo.
Búsqueda por palabra clave	Permite buscar dentro de la imagen palabras clave, pueden ser archivos o cualquier otra referencia que se le pase como argumento.
Tipo de archivo	Permite tanto la búsqueda como la ordenación de archivos según su tipo.
Detalles de la imagen	Muestra en detalle la imagen a examinar, permitiendo saber dónde se encuentran físicamente los datos dentro de ella.
Matadatos	Permite ver elementos del sistema de archivos que no se muestran habitualmente, como las referencias a directorios o los archivos eliminados.
Unidad de datos	Ofrece la posibilidad de entrar en el máximo detalle de cualquier archivo, permitiendo examinar el contenido real del mismo, ya sea en ASCII o en hexadecimal.

Como se indicó al inicio de este apartado, las herramientas expuestas anteriormente necesitan de la ejecución sobre un sistema operativo ya instalado. En ocasiones le será de gran utilidad disponer de un entorno tipo *Live*, que le permita realizar un examen forense de imágenes sin tener que dedicar un equipo específico para ello y sin necesidad cargar otro sistema operativo. Estas soluciones suelen encontrarse en CDs o DVDs preparados para tal fin, veamos alguno de ellos.

HELIX CD

Se trata de un Live CD de respuesta ante incidentes, basado en una distribución Linux denominada *Knoppix* (que a su vez está basada en Debian). Posee la mayoría de las herramientas necesarias para realizar un análisis forense tanto de equipos como de imágenes de discos. Puede descargarlo gratuitamente de:

http://www.e-fense.com/helix/.

Este CD ofrece dos modos de funcionamiento, tras ejecutarlo nos permitirá elegir entre arrancar un entorno MS Windows o uno tipo Linux. En el primero de ellos disponemos de un entorno con un conjunto de herramientas, casi 90 Mb, que nos permitirá principalmente interactuar con sistemas "vivos", pudiendo recuperar la información volátil del sistema. En el arranque Linux, disponemos de un Sistema Operativo completo, con un núcleo modificado para conseguir una excelente detección de hardware, no realiza el montaje de particiones swap, ni ninguna otra operación sobre el disco duro del equipo sobre el que se arranque. Es ideal para el análisis de equipos "muertos", sin que se modifiquen las evidencias pues montará los discos que encuentre en el sistema en modo sólo lectura. Además de los comandos de análisis propios de los entornos UNIX/Linux, se han incorporado una lista realmente interesante de herramientas y ToolKits, alguno de ellos comentados anteriormente como el Sleuth Kit y Autopsy.

F.I.R.E. Linux

Se trata de otro CD de arranque que ofrece un entorno para respuestas a incidentes y análisis forense, compuesto por una distribución Linux a la que se le han añadido una serie de utilidades de seguridad, junto con un interfaz gráfico que hace realmente fácil su uso. Al igual que el kit anterior, por su forma de montar los discos no realiza ninguna modificación sobre los equipos en los que se ejecute, por lo que puede ser utilizado con seguridad. Este live CD está creado y mantenido por William Salusky y puede descargarse gratuitamente desde la dirección http://biatchux.dmzs.com. En esta interesantísima distribución podrá disponer de una serie de funcionalidades que le aportará muchas ventajas en su análisis, entre las que cabe destacar:

- ✓ Recolección de datos de un sistema informático comprometido y hacer un análisis forense.
- ✓ Chequear la existencia de virus o malware en general desde un entorno fiable.
- ✓ Posibilidad de realización de test de penetración y vulnerabilidad.
- ✓ Recuperación datos de particiones dañadas.

Las herramientas que posee F.I.R.E son conocidas y muy recomendables, aunque sin entrar en detalles sobre cada una de ellas, podrá encontrar las siguientes:

- ✓ `Nessus, nmap, whisker, hping2, hunt, fragrouter.`
- ✓ `Ethereal, Snort, tcpdump, ettercap, dsniff, airsnort.`
- ✓ `Chkrootkit, F-Prot.`
- ✓ TCT, Autopsy.
- ✓ `Testdisk, fdisk, gpart.`
- ✓ SSH (cliente y servidor), VNC (cliente y servido)
- ✓ Mozilla, ircII, mc, Perl, biew, fenris, pgp.

5

Conclusiones

Con este trabajo se ha pretendido realizar una primera incursión en el apasionante y novedoso mundo del Análisis Forense Digital, exponiendo aquellas características y particularidades propias de esta disciplina de la seguridad informática. Se ha enfocado el tema desde el punto de vista de una herramienta indispensable que toda organización debe contemplar dentro de su política de seguridad y enmarcada dentro del proceso de respuesta a incidentes en los sistemas informáticos.

Se ha intentado destacar la necesidad imperiosa de aplicar metodologías y procedimientos específicos con el fin de asegurar la garantía de calidad de las evidencias durante todo el proceso forense, haciendo hincapié en la recopilación y custodia de las evidencias digitales. Se han expuesto también las diferencias a la hora de llevar a cabo un análisis forense en dos de los sistemas operativos más extendidos, MS Windows y UNIX/Linux, y cómo podemos disponer de herramientas software específicas que nos pueden ayudar en el análisis, sin entrar en las de tipo hardware por motivos de espacio y tiempo.

Desde el punto de vista de la situación actual de la disciplina, se destaca una falta de unicidad de criterios tanto a la hora de definir estándares para las herramientas a emplear, como para el proceso de certificación y acreditación de los profesionales del sector. Aunque si se ha encontrado una importante comunidad de desarrollo, tanto por parte de organizaciones como por parte de grupos de software de libre distribución, que están continuamente aportando nuevas herramientas y procedimientos.

Destacar en este campo el Concurso de Reto Forense que se viene celebrando desde el año 2004, en el que los participantes deben analizar un sistema informático comprometido. Éste reto está patrocinado por las dos principales entidades académicas de seguridad informática de España y México, la UNAM a través de la DGSCA y el UNAM-CERT y la organización pública Red.es a través del Grupo de Seguridad de RedIRIS, con el apoyo de organizaciones y organismos de seguridad informática iberoamericanos y mundiales.

También cabe mencionar los proyectos como el "Spanish Honeynet Project", http://www.honeynet.org.es/ organización de investigación no lucrativa compuesta por profesionales de seguridad informática dedicada a temas de seguridad centrados en tecnologías de redes trampa. Su objetivo principal es estudiar, comprender y avisar sobre los motivos y tácticas de la comunidad *hacker*, además comparten los conocimientos sobre las distintas herramientas y prácticas utilizadas por los atacantes en Internet.

6
Bibliografía y referencias

Libros

“Seguridad en las Comunicaciones y en la Información”, G. Díaz Orueta y otros. Ed. UNED
“Software Libre. Herramientas de Seguridad”. Tony Howlet. Ed. Anaya Multimedia.
“Hackers 2”. J. Scambray, S. McClure y G. Kurtz. ED. Osborne-McGraw-Hill.
“Extreme Exploits”. V. Oppleman, Brett Watson. Ed. Anaya Multimedia.

Referencias

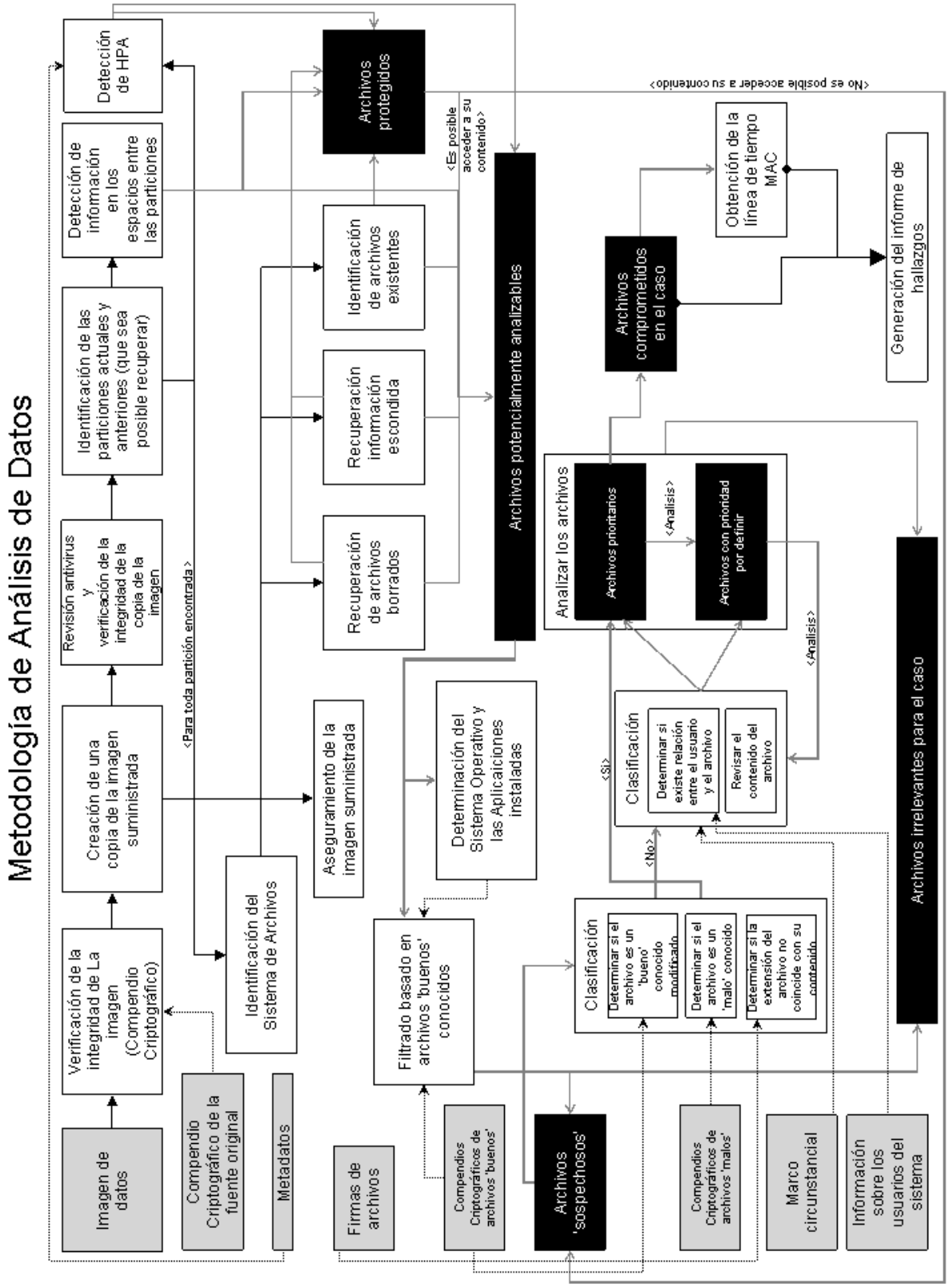
SP-800-61 ”Computer Security Incident Handling Guide”. T. Grance. NIST-USA. 2002
"GIAC Security Essentials, Practical Assignment" Version 1.4b. Tan Koon Yaw. SANS Institute 2003.
"Forensic Examination of Digital Evidence: A Guide for Law Enforcement". John Ashcroft. U.S. Dep. of Justice, Apr. 2004
"Helix 1.7 for Beginners". BJ Gleason and Drew Fahey. Manual Version Mar. 2006
"First Responder’s Manual". U.S. Dep. of Energy Computer Forensic Laboratory. 1999.
“Análisis Forense Digital GNU/Linux”. David Ditrich y Ervin Sarkisov. 2002
RFC-3227. “Guidelines for Evidence Collection and Archiving”. Feb. 2002.
Análisis técnicos del Reto Forense ediciones 1 y 2 (comunidad RedIris). 2004 y 2005.
CoBIT 4.0 “Control Objective for Information and Related Technology”. IT Governance Institute 2005.
“Una Propuesta Metodológica y su Aplicación en The Sleuth Kit y EnCase Descargar en disco”. Octubre de 2005. Jonathan Córdoba; Ricardo Laverde; Diego Ortiz; Diana Puentes.

7
URLs

www.auditoresdesistemas.com
www.criptored.upm.es
www.dfrws.org
www.e-fense.com
www.enfsi.org
www.forensics-es.org
www.foundstone.com
www.google.es
www.ioce.org
www.isaca.org
www.opensourceforensics.org
www.red.es
www.securityfocus.com
www.wikipedia.org

Apéndices

A.1.- Esquema del proceso de respuesta a incidentes.



Fuente: "Una Propuesta Metodológica y su Aplicación en The Sleuth Kit y EnCase Descargar en disco". Octubre de 2005. Jonathan Córdoba; Ricardo Laverde; Diego Ortiz; Diana Puentes.

A.2.- Ejemplo de e-mail de notificación sobre incidentes a un ISP.

TO: abuse_email@example-isp.com
Ref: Intrusion notification

Please be advised that on the [date of compromise] an intrusion took place into and against our systems.

Upon a thorough analysis of the systems involved, evidence appeared that the intrusion in questiontook place from two IP addresses pertaining to a rank monitored by your company.

IP addresses and time and hour mentioned in our report are the following:

Time	Ip Address
01:18:47	xxx.xxx.xxx.xxx
09:29:17	xxx.xxx.xxx.xxx

These times and hours correspond to GMT+1. Correspondence with regard to your time GMT+2 is as follows:

Time	Ip Address
02:18:47	xxx.xxx.xxx.xxx
10:29:17	xxx.xxx.xxx.xxx

We beg you please take the adequate and proper administrative and/or legal steps in order to avoid, in the future, as far as you possibly can, these type and kind of unfair & elegal actions.

Should you require / need any additional clarification / information, please do not hesitate to contact us through any o the below quoted means:

Phone:
E-mail:

We most earnestly thank you for your attention and coorperation towards a balanced and profitable business running.

A.3.- Glosario de términos.

Exploit

Exploit (del inglés to exploit, explotar, aprovechar) es el nombre con el que se identifica un programa informático malicioso, o parte del programa, que trata de forzar alguna deficiencia o vulnerabilidad de otro programa. El fin puede ser la destrucción o inhabilitación del sistema atacado, aunque normalmente se trata de violar las medidas de seguridad para poder acceder al mismo de forma no autorizada y emplearlo en beneficio propio o como origen de otros ataques a terceros. Los exploits se pueden caracterizar según las categorías de vulnerabilidades utilizadas para su ataque.

Honeypot

Se denomina Honeypot al software o conjunto de computadores cuya intención es atraer a crackers o spammers, simulando ser sistemas vulnerables o débiles a los ataques. Es una herramienta de seguridad informática utilizada para recoger información sobre los atacantes y sus técnicas. Los Honeypots pueden distraer a los atacantes de las máquinas más importantes del sistema, y advertir rápidamente al administrador del sistema de un ataque, además de permitir un examen en profundidad del atacante, durante y después del ataque al honeypot.

Algunos honeypots son programas que se limitan a simular sistemas operativos no existentes en la realidad y se les conoce como honeypots de baja interacción y son usados fundamentalmente como medida de seguridad. Otros sin embargo trabajan sobre sistemas operativos reales y son capaces de reunir mucha más información; sus fines suelen ser de investigación y se los conoce como honeypots de alta interacción.

También se llama honeypot a un website o sala de chat, que se ha creado para descubrir a otro tipo de usuarios con intenciones criminales, (e.j., pedofilia).

Inodo

En informática, un inodo o (i-node en inglés) es una estructura de datos propia de los sistemas de archivos tradicionalmente empleados en los sistemas operativos tipo UNIX como es el caso de Linux.

Un inodo contiene las características (permisos, fechas, ubicación, pero NO el nombre) de un archivo regular, directorio, o cualquier otro objeto que pueda contener el sistema de ficheros.

El término "inodo" refiere generalmente a inodos en discos (dispositivos en modo bloque) que almacenan archivos regulares, directorios, y enlaces simbólicos. El concepto es particularmente importante para la recuperación de los sistemas de archivos dañados.

Cada inodo queda identificado por un número entero, único dentro del sistema de ficheros, y los directorios recogen una lista de parejas formadas por un número de inodo y nombre identificativo que permite acceder al archivo en cuestión: cada archivo tiene un único inodo, pero puede tener más de un nombre en distintos o incluso en el mismo directorio para facilitar su localización.

Rootkit

Un rootkit es un conjunto de herramientas usadas frecuentemente por los intrusos o crackers que consiguen acceder ilícitamente a un sistema informático. Estas herramientas sirven para esconder los procesos y archivos que permiten al intruso mantener el acceso al sistema, a menudo con fines maliciosos. Hay rootkits para una amplia variedad de sistemas operativos, como Linux, Solaris o Microsoft Windows.

Fuente: www.wikipedia.org