

**TEXTO APROBADO POR LA COMISION PRIMERA DE LA H. CAMARA DE REPRESENTANTES EN PRIMER DEBATE DEL PROYECTO DE LEY N° 100/09 CAMARA “POR MEDIO DE LA CUAL SE REFORMA EL TÍTULO VII BIS DEL CÓDIGO PENAL O LEY 599 DE 2000 Y SE MODIFICAN ALGUNAS DISPOSICIONES DEL CÓDIGO DE PROCEDIMIENTO PENAL O LEY 906 DE 2004, EN MATERIA DE PROTECCIÓN DE LA INFORMACIÓN Y DE LOS DATOS”.**

El Congreso de Colombia,

DECRETA

**Artículo 1º. Definiciones.** Para los efectos de las conductas contempladas tanto en el Título VII Bis del Código Penal, intitulado como “De la protección de la información y de los datos”, como de las disposiciones correspondientes de la Ley 906 de 2004, y con el fin de adoptar una adecuada hermenéutica de los textos en ellos empleados, se adoptan las siguientes definiciones:

**Bot Net.** Redes de sistemas de computación conectadas y controladas de forma remota por una computadora que actúa como “command”, diseñadas para ejecutar tareas sin el conocimiento ni el consentimiento del dueño del sistema.

**Booteo.** Proceso que inicia el sistema operativo cuando el usuario enciende una computadora; se encarga de la inicialización del sistema y de los diversos dispositivos.

**Comunicación no privada.** Cualquier mensaje o intercambio de datos que trascienda la esfera íntima de las personas.

**Comunicación privada.** Cualquier mensaje de datos entre individuos que se identifican convenientemente generado, enviado, recibido, almacenado o comunicado a través de sistemas informáticos, predicable de asuntos estrictamente personales.

**Datos informáticos.** Cualquier representación de hechos, informaciones o conceptos de una forma que permita su tratamiento digital.

**Dato personal.** Cualquier información numérica, alfabética, gráfica, fotográfica, acústica o de cualquier otro tipo concerniente a personas físicas o jurídicas identificadas o identificables. Para los efectos de la presente Ley, también se tendrán en cuenta las definiciones previstas en el artículo 3º, literales e, f, g y h de la Ley Estatutaria N° 1266 de 31 de diciembre 2008, en materia de *Habeas Data*.

**Dato Personal Sensible.** Son aquellos informes de carácter personal concernientes a la salud, sexo, filiación política, raza, de comportamiento u origen étnico, que hacen parte del haber íntimo de la persona y pueden ser recabados únicamente con el consentimiento expreso e informado de su titular.

**Gestión de Seguridad de la Información.** Conjunto de buenas prácticas expresado o no en un sistema de servicio de seguridad tendente a proteger y gestionar los activos de información de una entidad pública o privada.

**Gusano.** Programa o código de programación transmitido como un adjunto de mail que se replica copiándose o iniciando su copia en otro programa, sector de booteo de una computadora, o documento, pero que no requiere de un portador para poder replicarse.

**Hacking.** Procedimiento mediante el que se violan los códigos personales y/o el acceso a datos o sistemas informáticos sin autorización y/o conocimiento del titular.

**Link.** Es sinónimo de “acoplamiento”, en el sentido práctico de Internet este término está referido a un enlace o hipervínculo.

**Malware.** Expresión derivada del inglés “malicious” software, también llamado “badware”. Es un software que tiene como objetivo infiltrarse en una computadora o dañarla sin el consentimiento de su propietario y/o usuario. Existen diferentes tipos de malware, como son los virus informáticos, los gusanos, los troyanos, los programas de spyware/adware e incluso los bots, “Crash programs” y “Cancer routines”, así como cualquier otra técnica igual o similar que se desarrolle en el futuro.

**Phishing.** Máscara, usualmente implementada por SPAM, mediante la que se busca apoderarse de manera ilegítima de la identidad o de los datos de una persona otorgados por un sistema de información.

**Prestador de servicio.** Es toda entidad pública o privada que ofrezca a los usuarios de sus servicios, la posibilidad de comunicarlos a través de un sistema informático, red de comunicaciones, y/o red o servicio de telecomunicaciones; también, se entiende por tal cualquier entidad que almacene o trate datos informáticos para un servicio de comunicación o para sus usuarios.

**Pop up.** Denota un elemento emergente de un sitio web que se utiliza generalmente dentro de la terminología de Internet.

**Sistema de autenticación.** Cualquier procedimiento que se emplee para identificar, de manera unívoca, a un usuario de un sistema informático.

**Sistema de autorización.** Cualquier procedimiento que se emplee para verificar que un usuario identificado está autorizado para realizar determinadas acciones.

**Sistema electrónico.** Es un conjunto de circuitos que interactúan entre sí para obtener un resultado.

**Sistema informático.** Es todo dispositivo aislado o conjunto de equipos y/o sistemas de información interconectados o relacionados entre sí, siempre que uno o varios de ellos permitan el tratamiento automatizado de datos.

**Sistema telemático.** Es el formado por equipos informáticos interconectados por una red de comunicaciones o telecomunicaciones que, a su vez, está constituida por circuitos, equipos de transmisión y equipos de conmutación.

**Software (soporte o equipamiento lógico).** Es la suma total de los programas de cómputo, procedimientos, reglas, documentación, manuales y datos asociados que forman parte de las

operaciones de un sistema de cómputo. Al efecto, se tendrán en cuenta los conceptos incorporados en el Decreto N° 1360 de 23 de junio 1989 y en las normas de propiedad intelectual vigentes aplicables a los programas de ordenador.

**Spam.** Correo electrónico comercial no deseado, enviado a la dirección electrónica de una persona sin contar con su consentimiento y/o autorización.

**Spyware.** Programa que se instala sin el conocimiento del usuario para recolectar y enviar información de manera no legítima.

**Troyanos.** Programa malicioso o dañino disfrazado de software inofensivo, que puede llegar a tomar el control de la computadora, con miras a provocar el daño para el que fue creado.

**Virus.** Programa o código de programación transmitido como un adjunto de mail o dispositivo que permite su réplica, copiándose o iniciando su copia o reproducción en otro programa de ordenador o equipo de cómputo.

**Web site o Portal Web.** Sitio virtual en Internet que comprende una colección de páginas Web, datos, imágenes, videos y activos de información digitales, hospedados en uno o en varios servidores.

**Parágrafo.** El Presidente de la República, mediante el ejercicio de la potestad reglamentaria y en la medida en que las necesidades y los desarrollos tecnológicos así lo exijan, revisará y actualizará en forma periódica el glosario de que da cuenta éste artículo.

**Artículo 2º.** El Artículo 269A del Código Penal, incorporado mediante ley 1273 de 2009, quedará así:

*Art. 269A. Acceso abusivo a un sistema informático.* El que, sin autorización del titular, del tenedor legítimo o de autoridad competente, y con la finalidad de obtener datos informáticos o con otra finalidad ilícita, acceda a un sistema informático protegido con una medida de seguridad, o se mantenga dentro del mismo en contra de la voluntad de quien tenga el derecho a excluirlo, incurrirá en pena de prisión de cuarenta y ocho (48) a noventa y seis (96) meses y en multa de cien (100) a mil (1000) salarios mínimos legales mensuales vigentes, siempre y cuando la conducta no configure otro delito”.

**Artículo 3º.** El Artículo 269B del Código Penal, incorporado mediante ley 1273 de 2009, quedará así:

*ARTÍCULO 269B. Obstaculización ilegítima de sistema informático o red de telecomunicación.* El que, sin estar autorizado para ello, impida u obstaculice el funcionamiento o el acceso normal a un sistema informático, a los datos informáticos allí contenidos, o a una red de telecomunicaciones, incurrirá en pena de prisión de cuarenta y

ocho (48) a noventa y seis (96) meses y en multa de 100 a 1000 salarios mínimos legales mensuales vigentes, siempre que la conducta no constituya delito sancionado con una pena mayor.

**Artículo 4º.** El Artículo 269C del Código Penal, incorporado mediante ley 1273 de 2009, quedará así:

Artículo 269C. *Interceptación, control o sustracción de datos informáticos.* El que, sin la existencia de orden judicial previa, intercepte, controle o sustraiga datos informáticos en su origen, destino, transmisión o en un sistema informático o telemático, o las emisiones electromagnéticas provenientes de un sistema informático o telemático que las transporte, incurrirá en pena de prisión de cuarenta y ocho (48) a noventa y seis (96) meses y en multa de cien (100) a mil (1000) salarios mínimos legales mensuales vigentes.

**Artículo 5º.** El Artículo 269D del Código Penal, incorporado mediante ley 1273 de 2009, quedará así:

ARTÍCULO 269D: *Daño informático.* El que dañe, destruya o altere datos informáticos o un sistema de tratamiento de información o sus partes o componentes lógicos, incurrirá en pena de prisión de cuarenta y ocho (48) a noventa y seis (96) meses y en multa de cien (100) a mil (1000) salarios mínimos legales mensuales vigentes.

**Artículo 6º.** El Artículo 269E del Código Penal, incorporado mediante ley 1273 de 2009, quedará así:

Artículo 269E: *Uso de software malicioso.* El que produzca, trafique, adquiera, distribuya, venda, use o envíe software malicioso o intrusivo, incurrirá en pena de prisión de cuarenta y ocho (48) a noventa y seis (96) meses y en multa de cien (100) a mil (1000) salarios mínimos legales mensuales vigentes, siempre que la conducta no constituya delito sancionado con pena mayor.

**Artículo 7º.** El Artículo 269F del Código Penal, incorporado mediante ley 1273 de 2009, quedará así:

ARTÍCULO 269F. *Violación de datos personales.* El que, sin estar autorizado para ello, obtenga, compile, sustraiga, ofrezca, venda, intercambie, envíe, compre, intercepte,

divulgue, modifique o emplee códigos personales, datos personales contenidos en ficheros, archivos, bases de datos o medios semejantes, incurrirá en pena de prisión de cuarenta y ocho (48) a noventa y seis (96) meses y en multa de 100 a 1000 salarios mínimos legales mensuales vigentes.

**Artículo 8º.** El Artículo 269G del Código Penal, incorporado mediante ley 1273 de 2009, quedará así:

**ARTÍCULO 269G:** *Suplantación de sitios Web para la captura de Datos Personales.* El que, con la finalidad de obtener datos personales y/o protegidos, mediante páginas electrónicas, enlaces o ventanas emergentes, consiga que un usuario informático acceda por error a una dirección IP distinta a la IP de un Portal o Web Real, incurrirá en pena de prisión de cuarenta y ocho (48) a noventa y seis (96) meses y en multa de cien (100) a mil (1000) salarios mínimos legales mensuales vigentes.

El que diseñe, desarrolle, trafique, venda, ejecute, programe o envíe páginas electrónicas, enlaces o ventanas emergentes para la realización de cualquiera de las conductas punibles descritas en este Título, incurrirá en pena de prisión de veintiocho (28) a cuarenta y seis (46) meses y en multa de cien (100) a mil (1000) salarios mínimos legales mensuales vigentes, siempre que la conducta no constituya otro delito sancionado con pena mayor.

**Artículo 9º.** El Artículo 269H del Código Penal, incorporado mediante ley 1273 de 2009, quedará así:

**ARTÍCULO 269 H:** *Circunstancias de agravación punitiva:* Las penas imponibles de acuerdo con los artículos descritos en este Título, se aumentarán de la mitad a las tres cuartas partes si la conducta se cometiere:

1. Sobre redes o sistemas informáticos o de comunicaciones estatales u oficiales o del sector financiero, nacionales o extranjeros.
2. Por servidor público en ejercicio de sus funciones.
3. Si el sujeto activo de la conducta se vale de la confianza depositada por el poseedor de la información o por quien tuviere un vínculo contractual con este.
4. Cuando se revele o dé a conocer el contenido de la información en perjuicio de otro.
5. Con la obtención de provecho para sí o para un tercero.
6. Con fines terroristas o con la generación de riesgo para la seguridad o la defensa nacionales.
7. Mediante la utilización como instrumento de un tercero que obra de buena fe.

8. Si las conductas se realizan por el responsable de la administración, manejo o control de dicha información.

9. Sobre datos informáticos o información informatizada bajo reserva industrial o comercial, o sobre datos o información informatizada de carácter político y/o militar, relacionados con la seguridad del Estado.

10. Mediante el uso no legítimo de datos personales de carácter sensible.

11. Si con la comisión de la conducta se causaren daños graves al sujeto pasivo de la acción.

**Artículo 10°.** El artículo 192 de la Ley 599 de 2000, quedará así:

Artículo 192: *Interceptación de comunicaciones.* El que, sin la existencia de orden judicial previa o sin autorización del titular, del tenedor legítimo, o de autoridad competente, sustraiga, oculte, extravíe, destruya, intercepte, controle o impida una comunicación privada dirigida a otra persona, o se entere indebidamente de su contenido, incurrirá en pena de prisión de cuarenta y ocho (48) a noventa y seis (96) meses y en multa de cien (100) a mil (1000) salarios mínimos legales mensuales vigentes, siempre que la conducta no constituya delito sancionado con pena mayor”.

**Artículo 11°.** El artículo 294 de la Ley 599 de 2000, quedará así:

Artículo 294: *Documento.* Para los efectos previstos en la ley penal, se entiende por documento toda expresión de persona conocida o conocible recogida por escrito o por cualquier medio mecánico o técnicamente impreso, electrónico o informático, o mediante cualquier otro soporte material que exprese o incorpore datos o hechos que tengan capacidad probatoria”.

**Artículo 12°.** El artículo 14 de la Ley 906 de 2004, quedará así:

Artículo 14. *Intimidación.* Toda persona tiene derecho al respeto de su intimidad. Nadie podrá ser molestado en su vida privada.

No podrán hacerse registros, allanamientos ni incautaciones en domicilio, residencia, o lugar de trabajo, sino en virtud de orden escrita del Fiscal General de la Nación o de su delegado, con arreglo de las formalidades y motivos previamente definidos en este código. Se entienden excluidas las situaciones de flagrancia y demás contempladas por la ley.

Cuando se trate de la búsqueda selectiva de datos personales organizados con fines legales, recogidos en bases de datos por instituciones públicas o privadas o entidades debidamente

autorizadas para ello, que no sean de libre acceso, o cuando fuere necesario interceptar comunicaciones, se requerirá el consentimiento expreso del titular del derecho a la intimidad y/o de la información, o una orden judicial previa emitida por el respectivo juez de control de garantías.

De la misma manera, se deberá proceder cuando resulte necesaria la recuperación de información dejada al navegar por Internet u otros medios tecnológicos que produzcan efectos equivalentes, o el acceso a esta, o cuando ella se encuentre en medio físico, almacenada en equipos, o haya sido tratada en sistemas de información y/o transmitida a través de redes de comunicaciones.

En estos casos, dentro de las treinta y seis (36) horas siguientes a la realización de los procedimientos, se deberá adelantar una audiencia ante el juez de control de garantías, con el fin de determinar la legalidad formal y material de la actuación”.

**Artículo 13°.** El artículo 69 de la Ley 906 de 2004, quedará así:

Artículo 69. *Requisitos de la denuncia, de la querrela o de la petición.* La denuncia, querrela o petición se hará verbalmente, o por escrito, o por cualquier medio técnico que permita la identificación del autor, dejando constancia del día y hora de su presentación y contendrá una relación detallada de los hechos que conozca el denunciante. Este deberá manifestar, si le consta, que los mismos hechos ya han sido puestos en conocimiento de otro funcionario. Quien la reciba advertirá al denunciante que la falsa denuncia implica responsabilidad penal. En caso de que la denuncia se acompañe de elementos materiales y/o de evidencia física, se observarán las disposiciones señaladas para la cadena de custodia.

En todo caso se inadmitirán las denuncias sin fundamento.

La denuncia podrá ampliarse a instancia del denunciante, o del funcionario competente, sobre aspectos de importancia para la investigación.

Los escritos anónimos que no suministren evidencias o datos concretos que permitan encauzar la investigación se archivarán por el fiscal correspondiente”.

**Artículo 14°.** El artículo 154 de la Ley 906 de 2004, quedará así:

Artículo 154. *Modalidades.* Se tramitarán en audiencia preliminar:

1. El acto de poner a disposición del juez de control de garantías los elementos recogidos en registros, allanamientos e interceptaciones de comunicaciones. También la solicitud de

búsqueda selectiva de datos personales en bases de datos y la recuperación de información dejada al navegar por internet u otros medios tecnológicos, que produzcan efectos equivalentes, todas ordenadas por la fiscalía, y la búsqueda o recolección de datos o información sistematizada ordenada por un juez de control de garantías para su control de legalidad dentro de las treinta y seis (36) horas siguientes.

2. La práctica de una prueba anticipada.
3. La que ordena la adopción de medidas necesarias para la protección de víctimas y testigos.
4. La que resuelve sobre la petición de medida de aseguramiento.
5. La que resuelve sobre la petición de medidas cautelares reales.
6. La formulación de la imputación.
7. El control de legalidad sobre la aplicación del principio de oportunidad.
8. Las que resuelvan asuntos similares a los anteriores.

**Artículo 15°.** El artículo 204 de la Ley 906 de 2004, quedará así:

Artículo 204. *Órgano técnico-científico.* El Instituto Nacional de Medicina Legal y Ciencias Forenses, de conformidad con la ley y lo establecido en el Estatuto Orgánico de la Fiscalía General de la Nación, prestará auxilio y apoyo técnico-científico en las investigaciones desarrolladas por la Fiscalía General de la Nación y por los organismos con funciones de policía judicial. Igualmente lo hará con el imputado, su defensor, y la víctima cuando estos lo soliciten.

La Fiscalía General de la Nación, el imputado o su defensor se apoyarán, cuando fuere necesario, en laboratorios privados nacionales o extranjeros o en los de universidades públicas o privadas, nacionales o extranjeras.

También, prestarán apoyo técnico-científico los laboratorios forenses de los organismos de policía judicial”.

**Artículo 16°.** El artículo 236 de la Ley 906 de 2004, quedará así:

Artículo 236. *Recuperación de información dejada al navegar por internet u otros medios tecnológicos que produzcan efectos equivalentes.* Cuando el fiscal tenga motivos razonablemente fundados, de acuerdo con los medios cognoscitivos previstos en este Código, para inferir que el indiciado o el imputado ha estado transmitiendo información útil para la investigación que se adelanta, durante su navegación por Internet u otros medios tecnológicos que produzcan efectos equivalentes, solicitará al Juez de Control de Garantías que permita la aprehensión de los computadores y servidores que éste pueda haber utilizado, disquetes y demás medios de almacenamiento físico, para que expertos en informática forense descubran, recojan, analicen y custodien la información que recuperen.

En estos casos serán aplicables analógicamente, según la naturaleza de este acto, los criterios establecidos para los registros y allanamientos.

La aprehensión de que trata este artículo se limitará exclusivamente al tiempo necesario para la captura de la información en él contenida. Inmediatamente se concluya esa tarea se devolverán los equipos incautados”.

**Artículo 17°.** El artículo 237 de la Ley 906 de 2004, quedará así:

Artículo 237. *Audiencia de control de legalidad posterior.* Dentro de las veinticuatro (24) horas siguientes al diligenciamiento de las órdenes de registro y allanamiento, retención de correspondencia, interceptación de comunicaciones o recuperación de información dejada al navegar por Internet u otros medios similares, el fiscal y/o la víctima, comparecerán ante el Juez de Control de Garantías, para que realice la audiencia de revisión de legalidad sobre lo actuado incluida la orden.

Durante el trámite de la audiencia sólo podrán asistir, además del fiscal y la víctima, los funcionarios de la policía judicial y los testigos o peritos que prestaron declaraciones juradas con el fin de obtener la orden respectiva, o que intervinieron en la diligencia o que recolectaron y examinaron los elementos materiales o evidencia física.

El juez podrá, si lo estima conveniente, interrogar directamente a los comparecientes y, después de escuchar los argumentos del fiscal o la víctima, decidirá de plano sobre la validez del procedimiento.

PARÁGRAFO. Si el cumplimiento de la orden ocurrió luego de formulada la imputación, se deberá citar a la audiencia de control de legalidad al imputado y a su defensor para que, si lo desean, puedan realizar el contradictorio. En este último evento, se aplicarán analógicamente, de acuerdo con la naturaleza del acto, las reglas previstas para la audiencia preliminar”.

**Artículo 18°.** El artículo 255 de la Ley 906 de 2004, quedará así:

Artículo 255. *Responsabilidad.* La aplicación de la cadena de custodia es responsabilidad de los servidores públicos que entren en contacto con los elementos materiales probatorios y evidencia física.

Los particulares y/o las víctimas, que por razón de su trabajo o por el cumplimiento de las funciones y/o obligaciones propias de su cargo, en especial el personal de los servicios de salud que entren en contacto con elementos materiales probatorios y evidencia física, son responsables por su recolección, preservación y entrega a la autoridad correspondiente.

**Artículo 19°.** El artículo 257 de la Ley 906 de 2004, quedará así:

Artículo 257. *Inicio de la cadena de custodia.* El servidor público que, en actuación de indagación o investigación policial, o recolección y examen, hubiere embalado y rotulado los datos, el elemento material probatorio y evidencia física, lo custodiará.

**Artículo 20°.** El artículo 275 de la Ley 906 de 2004, quedará así:

Artículo 275. *Elementos materiales probatorios y evidencia física.* Para efectos de este código se entiende por elementos materiales probatorios y evidencia física, los siguientes:

- a) Huellas, rastros, manchas, residuos, vestigios y similares, dejados por la ejecución de la actividad delictiva;
- b) Armas, instrumentos, objetos y cualquier otro medio utilizado para la ejecución de la actividad delictiva;
- c) Dinero, bienes y otros efectos provenientes de la ejecución de la actividad delictiva;
- d) Los elementos materiales descubiertos, recogidos y asegurados en desarrollo de diligencia investigativa de registro y allanamiento, inspección corporal y registro personal;
- e) Los documentos de toda índole hallados en diligencia investigativa de inspección o que han sido entregados voluntariamente por quien los tenía en su poder o que han sido abandonados allí;

- f) Los elementos materiales obtenidos mediante grabación, filmación, fotografía, video o cualquier otro medio avanzado, utilizados como cámaras de vigilancia, en recinto cerrado o en espacio público;
- g) El mensaje de datos, como el intercambio electrónico de datos, Internet, correo electrónico, telegrama, télex, telefax o similar, regulados por la Ley 527 de 1999 o las normas que la sustituyan, adicionen o reformen;
- h) Los demás elementos materiales similares a los anteriores y datos informáticos o información sistematizada, descubiertos, recogidos y custodiados por el Fiscal General o por el fiscal directamente o por conducto de servidores de policía judicial o de peritos del Instituto Nacional de Medicina Legal y Ciencias Forenses, o de laboratorios aceptados oficialmente, o de los particulares y/o víctimas, que por razón de sus trabajo o por el cumplimiento de sus funciones y/o obligaciones los hayan recolectado.

**Artículo 21°.** El Artículo 267 de la Ley 906 de 2004 quedará así:

Artículo 267. *Facultades de quien no es imputado y de la víctima:* Quien sea informado o advierta que se adelanta investigación en su contra, podrá asesorarse de abogado. Aquél o éste, podrán buscar, identificar empíricamente, recoger y embalar los elementos materiales probatorios y evidencia física, y hacerlos examinar por peritos particulares a su costa, o solicitar a la Policía Judicial que lo haga. Tales elementos, el informe sobre ellos y las entrevistas que hayan realizado con el fin de descubrir información útil, los pondrá a disposición de la fiscalía o autoridades competentes. Estas mismas facultades las tendrá la víctima.

Igualmente, podrán solicitar al Juez de Control de Garantías que lo ejerza sobre las actuaciones que consideren hayan afectado o afecten sus derechos fundamentales. O con el fin de obtener la legalidad formal y material de los elementos materiales y evidencia física que, por razón de su trabajo o por el cumplimiento de sus funciones y/o obligaciones, hayan podido recolectar para poner a disposición de la fiscalía o autoridades competentes.

**Artículo 22°.** El Artículo 268 de la Ley 906 de 2004 quedará así:

Artículo 268. *Facultades del imputado y de la víctima.* El imputado o su defensor, la víctima, durante la investigación, podrán buscar, identificar empíricamente, recoger y embalar los elementos materiales probatorios, elementos lógicos y evidencia física. Con la solicitud para que sean examinados y la constancia de que se es imputado o defensor de éste, los trasladarán al respectivo laboratorio del Instituto Nacional de Medicina Legal y Ciencias Forenses, donde los entregarán bajo recibido”.

**Artículo 23°.** El Artículo 269 de la Ley 906 de 2004 quedará así:

Artículo 269. *Contenido de la solicitud.* La solicitud deberá contener en forma separada, con claridad y precisión, las preguntas que en relación con el elemento material o lógico probatorio y evidencia física entregada, se requiere que responda el perito o peritos, previa la investigación y análisis que corresponda.

**Artículo 24°.** El Artículo 270 de la Ley 906 de 2004 quedará así:

Artículo 270. *Actuación del perito.* Recibida la solicitud y los elementos mencionados en los artículos anteriores, el perito los examinará. Si encontrare que el contenedor, tiene señales de haber sido o intentado ser abierto, o que la solicitud no reúne las mencionadas condiciones lo devolverá al solicitante. Lo mismo hará en caso de que encontrare alterado el elemento por examinar. Si todo lo hallare aceptable, procederá al examen y análisis que corresponda y a la elaboración del informe pericial.

El informe pericial se entregará bajo recibo al solicitante y se conservará un ejemplar de aquel y de este por parte del perito.

**Artículo 25°.** El Artículo 271 de la Ley 906 de 2004 quedará así:

Artículo 271. *Facultad de entrevistar.* El imputado o su defensor, y la víctima, podrán entrevistar a personas con el fin de encontrar información útil para la defensa o la investigación. En esta entrevista se emplearán las técnicas aconsejadas por la criminalística.

La entrevista se podrá recoger y conservar por escrito, en grabación magnetofónica, en video o en cualquier otro medio técnico idóneo.

**Artículo 26°.** El Artículo 272 de la Ley 906 de 2004 quedará así:

Artículo 272. *Obtención de declaración jurada.* El imputado o su defensor, la víctima, podrán solicitar a un alcalde municipal, inspector de policía o notario público, que le reciba declaración jurada a la persona, cuya exposición pueda resultar de especial utilidad para la investigación. Esta podrá recogerse por escrito, grabación magnetofónica, en video o en cualquier otro medio técnico idóneo.

**Artículo 27°.** El Artículo 273 de la Ley 906 de 2004 quedará así:

Artículo 273. *Criterios de valoración.* La valoración de los elementos materiales probatorios y evidencia física se hará teniendo en cuenta su legalidad, autenticidad, sometimiento a cadena de custodia y el grado actual de aceptación científica, técnica o artística de los principios en que se funda el informe.

**Artículo 28°.** El Artículo 274 de la Ley 906 de 2004 quedará así:

Artículo 274. *Solicitud de prueba anticipada.* El imputado o su defensor, la víctima, o su apoderado, podrán solicitar al juez de control de garantías, la práctica anticipada de cualquier medio de prueba, en casos de extrema necesidad y urgencia, para evitar la pérdida o alteración del medio probatorio. Se efectuará una audiencia, previa citación al fiscal correspondiente para garantizar el contradictorio.

Se aplicarán las mismas reglas previstas para la práctica de la prueba anticipada y cadena de custodia.

**Artículo 29°.** El artículo 424 de la Ley 906 de 2004, quedará así:

Artículo 424: *Prueba documental.* Para los efectos previstos en este Código se entienden por documentos, los siguientes:

1. Textos manuscritos, mecanografiados, impresos, informáticos o electrónicos.
2. Grabaciones magnetofónicas.
3. Discos de todas las especies que contengan grabaciones.
4. Grabaciones fonópticas o videos.
5. Películas cinematográficas.
6. Grabaciones computacionales.
7. Mensajes de datos.
8. El télex, telefax y similares.
9. Fotografías.
10. Radiografías.
11. Ecografías.
12. Tomografías.
13. Electroencefalogramas.
14. Electrocardiogramas.
15. Datos expresados en cualquier soporte conocido o por conocer.
16. Cualquier otro objeto similar o análogo a los anteriores.

**Artículo 30°.** De todos los delitos previstos en el Título VII Bis del Código Penal conocerán, de forma privativa, los Jueces Penales del Circuito al tenor de lo señalado en el artículo 36 de la Ley 906 de 2004.

**Artículo 31°.** La presente Ley rige desde la fecha de su promulgación y deroga todas las disposiciones que le sean contrarias, en especial el texto del artículo 195 del C. P. que había sido introducido por el artículo 25 de la Ley 1288 de cinco marzo 2009.

En los anteriores términos fue aprobado el presente proyecto de ley, con modificaciones, según consta en las actas Nos. 24 y 25 del 20 y 21 de abril de 2010, respectivamente; así mismo este proyecto fue anunciado para discusión y votación entre otras fechas el día 14 de abril de 2010, según consta en el acta No. 23 de esa misma fecha.

**EMILIANO RIVERA BRAVO**  
**Secretario Comisión Primera Constitucional**