INSTITUTO DOMINICANO DE LAS TELECOMUNICACIONES (INDOTEL)

RESOLUCIÓN No. 056-09

QUE ORDENA EL INICIO DEL PROCESO DE CONSULTA PÚBLICA PARA DICTAR EL "REGLAMENTO PARA LA OBTENCIÓN Y PRESERVACIÓN DE DATOS E INFORMACIONES POR PARTE DE LOS PROVEEDORES DE SERVICIOS, EN APLICACIÓN DE LAS DISPOSICIONES DE LA LEY NO. 53-07, SOBRE CRÍMENES Y DELITOS DE ALTA TECNOLOGÍA.".

El **Instituto Dominicano de las Telecomunicaciones (INDOTEL)**, por órgano de su Consejo Directivo y de conformidad con las disposiciones de la Ley General de Telecomunicaciones, No. 153-98, de fecha 27 de mayo de 1998, publicada en la Gaceta Oficial No. 9983, reunido válidamente, previa convocatoria, dicta la presente **RESOLUCIÓN:**

Con motivo del inicio del proceso de consulta pública para dictar el "Reglamento para la obtención y preservación de datos e informaciones por parte de los proveedores de servicios, en aplicación de las disposiciones de la Ley No. 53-07, sobre Crímenes y Delitos de Alta Tecnología".

Antecedentes.-

1. En fecha 23 de abril de 2007, fue promulgada la Ley No. 53-07 sobre Crímenes y Delitos de Alta Tecnología, que tiene por objeto la protección integral de los sistemas que utilicen tecnologías de información y comunicación y su contenido, así como la prevención y sanción de los delitos cometidos contra éstos o cualquiera de sus componentes o los cometidos mediante el uso de dichas tecnologías en perjuicio de personas física o morales, en los términos previstos en esta ley. La integridad de los sistemas de información y sus componentes, la información o los datos, que se almacenan o transmiten a través de éstos, las transacciones y acuerdos comerciales o de cualquiera otra índole que se llevan a cabo por su medio y la confidencialidad de éstos, son todos bienes jurídicos protegidos;

2. Con ocasión de los procesos de investigación seguidos de conformidad con las previsiones de la Ley No. 53-07, los órganos de investigación del Estado y los proveedores de servicios se encuentran en permanente intercambio de información respecto de los casos objeto de investigación, por lo cual se hace necesario que el **INDOTEL** proceda a la puesta en consulta pública, el proyecto de "Reglamento para la obtención y preservación de datos e informaciones por parte de los proveedores de servicios, en aplicación de las disposiciones de la Ley No. 53-07, sobre Crímenes y Delitos de Alta Tecnología", de conformidad con el mandato legal que le ha sido conferido al efecto.

EL CONSEJO DIRECTIVO DEL INSTITUTO DOMINICANO DE LAS TELECOMUNICACIONES (INDOTEL), DESPUÉS DE HABER ESTUDIADO Y DELIBERADO SOBRE EL CASO:

CONSIDERANDO: Que el Instituto Dominicano de las Telecomunicaciones (**INDOTEL**), en su calidad de órgano regulador de las telecomunicaciones en virtud de la Ley 153-98 y de los sujetos regulados por la Ley 126-02 sobre Comercio Electrónico, Documentos y Firmas digitales, así como en su papel de Presidente de la Comisión Nacional para la Sociedad de la Información y el Conocimiento (CNSIC), ha jugado un papel protagónico y de marcado liderazgo no sólo en la elaboración del texto de la Ley

53-07 sobre Crímenes y Delitos de Alta Tecnología, sino también, en su proceso de aprobación y ejecución;

CONSIDERANDO: Que la Ley No. 53-07 sobre Delitos y Crímenes de Alta Tecnología tiene por objeto la protección integral de los sistemas que utilicen tecnologías de información y comunicación y su contenido, así como la prevención y sanción de los delitos cometidos contra éstos o cualquiera de sus componentes o los cometidos mediante el uso de dichas tecnologías en perjuicio de personas física o morales. Y la protección de la integridad de los sistemas de información y sus componentes, la información o los datos, que se almacenan o transmiten a través de éstos, las transacciones y acuerdos comerciales o de cualquiera otra índole que se llevan a cabo por su medio y la confidencialidad de éstos, son todos bienes jurídicos protegidos.

CONSIDERANDO: Que la Ley No. 53-07 dispone en su artículo 56, lo siguiente: "[…] El Instituto Dominicano de las Telecomunicaciones (INDOTEL) creará un reglamento para el procedimiento de obtención y preservación de datos e informaciones por parte de los proveedores de servicios […] Dicha normativa deberá tomar en cuenta la importancia de preservación de la prueba, no obstante la cantidad de proveedores envueltos en la transmisión o comunicación.";

CONSIDERANDO: Que es necesario contar con instrumentos jurídicos adecuados que proporcionen un equilibro, que conlleve la seguridad de una labor eficiente por parte de los Órganos de Investigación del Estado, la protección de la capacidad de los Proveedores de Servicios de proporcionar sus servicios y el establecimiento de salvaguardas relacionadas a la protección de derechos humanos fundamentales tales como libertad de expresión, el respeto a la vida privada, hogar y correspondencia y el derecho a la protección de datos de carácter personal;

CONSIDERANDO: que dentro de los denominados Derechos Individuales y Sociales de los ciudadanos, el numeral 9 del Artículo 8 de la Constitución de la República Dominicana establece que: "La inviolabilidad de la correspondencia y demás documentos privados, los cuales no podrán ser ocupados ni registrados sino mediante procedimientos legales en la substanciación de asuntos que se ventilen en la justicia.

CONSIDERANDO: que el precitado artículo, consagra el principio constitucional sobre la inviolabilidad de las comunicaciones, haciéndose extensible a toda la comunicación de carácter privado, cuyas señales transiten a través de las distintas modalidades de redes telefónicas o mediante el uso del espectro radioeléctrico o por cualquier otro tipo de redes, por lo que es igualmente inviolable el secreto de la comunicación telegráfica, telefónica y cablegráfica. Asimismo, resulta evidente que la misma Constitución, crea una condición de excepción a dicho principio por motivaciones de orden público, cuando establece la posibilidad de que las comunicaciones de tipo privado sean interceptadas mediante procedimientos legales en la substanciación de casos que se ventilen en la justicia;

CONSIDERANDO: Que el artículo 6 de la Ley General de las Telecomunicaciones prohíbe el uso de las telecomunicaciones contrario a las leyes o que tenga por objeto cometer delitos o entorpecer la acción de la justicia;

CONSIDERANDO: Que en virtud del artículo 77 de la Ley 153-98, es deber del **INDOTEL** defender y hacer efectivos los derechos de los clientes, usuarios y prestadores de servicios públicos de telecomunicaciones, mediante la elaboración de reglamentos de alcance general y normas de alcance particular, estableciendo el cumplimiento de las correspondientes obligaciones a las partes y dado el caso, sancionando a quienes no las cumplan, de conformidad con las disposiciones contenidas en la referida Ley;

CONSIDERANDO: Que entre las funciones del Consejo Directivo del **INDOTEL** el artículo 84, literal "b" de la Ley General de Telecomunicaciones señala la de "Dictar reglamentos de alcance general y normas de alcance particular, dentro de las reglas y competencias fijadas por la presente ley, y manteniendo el criterio consultivo de las empresas prestadoras de los diversos servicios públicos regulados y de sus usuarios";

VISTA: La Constitución de la República Dominicana;

VISTA: La Ley General de Telecomunicaciones No.153-98, de fecha 27 de Mayo de 1998;

VISTA: La Ley No. 53-07 sobre Delitos y Crímenes de Alta Tecnología;

VISTO: El Convenio sobre Ciberdelincuencia del Consejo de Europa, del 23 de noviembre del 2001.

VISTO: El Código Procesal Penal de la República Dominicana, aprobado mediante la Ley No.76-02, del 19 de julio del 2002;

EL CONSEJO DIRECTIVO DEL INSTITUTO DOMINICANO DE LAS TELECOMUNICACIONES (INDOTEL), EN EJERCICIO DE SUS FACULTADES LEGALES Y REGLAMENTARIAS

RESUELVE:

PRIMERO: ORDENAR el inicio del proceso de consulta pública para dictar el **"Reglamento para la obtención y preservación de datos e informaciones por parte de los proveedores de servicios, en aplicación de las disposiciones de la Ley No. 53-07, sobre Crímenes y Delitos de Alta Tecnología"**, cuyo texto se encuentra anexo a la presente resolución, formando parte integral de la misma.

SEGUNDO: OTORGAR un plazo de treinta (30) días calendario, contados a partir de la fecha de la publicación de la presente resolución, para que los interesados presenten las observaciones y comentarios que estimen convenientes al **"Reglamento para la obtención y preservación de datos e informaciones por parte de los proveedores de servicios, en aplicación de las disposiciones de la Ley No. 53-07, sobre Crímenes y Delitos de Alta Tecnología"**, de conformidad con el artículo 93 de la Ley General de Telecomunicaciones No. 153-98, del 27 de mayo de 1998, las cuales no serán vinculantes para el órgano regulador.

PARRAFO I: Los comentarios y las observaciones a los que hace referencia el presente artículo deberán ser depositados en formato papel y en formato electrónico, redactados en idioma español, dentro del plazo anteriormente establecido, en las oficinas del Instituto Dominicano de las Telecomunicaciones (**INDOTEL**), ubicadas en el Edificio Osiris, marcado con el número 962 de la Avenida Abraham Lincoln, de esta ciudad de Santo Domingo de Guzmán, Distrito Nacional, en días y horas laborables.

PARRAFO II: Vencido el plazo de treinta (30) días establecido en este ordinal "Segundo", no se recibirán más observaciones y no se concederán prórrogas.

TERCERO: INSTRUIR a la Directora Ejecutiva para que disponga la publicación de esta resolución y su anexo en un periódico de amplia circulación nacional, inmediatamente a

partir de lo cual dichos documentos deberán estar a disposición de los interesados en las oficinas del **INDOTEL**, ubicadas en la primera planta del Edificio Osiris, situado en la avenida Abraham Lincoln No. 962, de esta ciudad de Santo Domingo de Guzmán, Distrito Nacional, así como en la página Web que mantiene esta institución en la red de Internet, en la dirección www.indotel.gob.do.

Así ha sido aprobada, adoptada y firmada la presente resolución, a unanimidad de votos por el Consejo Directivo del **Instituto Dominicano de las Telecomunicaciones (INDOTEL)**, en la ciudad de Santo Domingo de Guzmán, Distrito Nacional, capital de la República Dominicana, hoy día veintinueve (29) del mes de junio del año dos mil nueve (2009).

Firmados:

Dr. José Rafael Vargas
Secretario de Estado,
Presidente del Consejo Directivo

José Alfredo Rizek V.,
En representación del Secretario de Estado
de Economía, Planificación y Desarrollo
Miembro ex oficio del Consejo Directivo

Leonel Melo Guerrero
Miembro del Consejo Directivo

David A. Pérez Taveras
Miembro del Consejo Directivo

Juan Antonio Delgado
Miembro del Consejo Directivo

Joelle Exarhakos Casasnovas
Directora Ejecutiva
Secretaria del Consejo Directivo

"PROYECTO DE REGLAMENTO PARA LA OBTENCIÓN Y PRESERVACIÓN DE DATOS E INFORMACIONES POR PARTE DE LOS PROVEEDORES DE SERVICIOS, EN APLICACIÓN DE LAS DISPOSICIONES DE LA LEY NO. 53-07, SOBRE CRÍMENES Y DELITOS DE ALTA TECNOLOGÍA."

TÍTULO I

DISPOSICIONES GENERALES

Artículo 1.- Definiciones.-

En adición a las definiciones establecidas en la Ley, las expresiones y términos que se emplean en este Reglamento tendrán el significado que se señala a continuación:

1.1. **Abuso Sexual:** Es la práctica sexual con un niño, niña o adolescente por un adulto, o persona cinco (5) años mayor, para su propia gratificación sexual, sin consideración del desarrollo psicosexual del niño, niña o adolescente y que puede ocurrir aún sin contacto físico.

1.2. **Atentado Sexual:** De acuerdo con lo establecido en el Artículo 23 de la Ley 53-07, se considerará que atentar sexualmente será toda acción encaminada a establecer una relación y control emocional sobre un niño, niña, adolescente, incapacitado o enajenado mental cuya finalidad última es la de abusar sexualmente del niño, niña, adolescente, incapacitado o enajenado mental. A fin de la presente definición, se considerará que ha atentado sexualmente, quien a sabiendas de que trata con un niño, niña, adolescente, incapacitado o enajenado mental, por medios electrónicos a distancia y lo sedujere o intentare seducir con fines de connotación sexual y quien a sabiendas de que trata con un niño, niña, adolescente, incapacitado o enajenado mental por medios electrónicos a distancia y lo indujere a la realización de manifestaciones sexuales y, a partir de aquello, lo intente obligar a realizar conductas por vía de amenazas.

1.3 **Centro de Acceso Público:** es cualquier establecimiento cuya actividad principal sea ofrecer el servicio de acceso a Internet, por medio de un pago determinado, o de manera gratuita, así como a otros servicios de red como mensajería instantánea, correo electrónico, video conferencia o Voz sobre IP; además puede hacerse uso de aplicaciones de oficina, editores de imágenes y utilidades de software.

1.4 **Datos de tráfico, conexión, acceso:** Cualesquiera datos informáticos relativos a una comunicación por medio de un sistema informático, generados por un sistema informático como elemento de la cadena de comunicación, que indiquen el origen, destino, ruta, hora, fecha, tamaño y dirección de la comunicación o tipo de servicio subyacente.

1.5 **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.

1.6. **Explotación Sexual Comercial de Niños, Niñas y Adolescentes:** es una violación fundamental de los derechos de la niñez, la cual abarca el abuso sexual por parte de adultos, y remuneración en dinero o en especie para niños, niñas y adolescentes o para una tercera persona o personas, así como el tratamiento como objeto sexual y como mercancía de niños, niñas y adolescentes. Entre las formas principales de explotación sexual comercial de niños,

niñas y adolescentes se encuentran la prostitución, la pornografía, el tráfico con propósitos sexuales y el turismo sexual.

1.7. **Órgano de Investigación:** se entenderá por órgano de investigación de acuerdo a lo establecido en el Código Procesal Penal, al Ministerio Público y los funcionarios y agentes de otras agencias ejecutivas o de gobierno que cumplen tareas auxiliares de investigación con fines judiciales, como la Policía Nacional y su Departamento de Investigación de Crímenes y Delitos de Alta Tecnología (DICAT), entre otros. Asimismo, esta definición será aplicable al **INDOTEL**, en el ejercicio de sus potestades inspectoras y sancionadoras, al amparo del marco legal y regulatorio aplicable a las telecomunicaciones, al comercio electrónico o cuando actúe como auxiliar de la justicia, en aplicación de la Ley No. 53-07.

1.8 **Pornografía Infantil:** Toda representación, por cualquier medio, de niños, niñas y adolescentes, dedicados a actividades sexuales explícitas, reales o simuladas o toda representación de las partes genitales de niños, niñas o adolescentes con fines primordialmente sexuales. Se considera niño o niña, a toda persona desde su nacimiento hasta los doce años, inclusive, y adolescente, a toda persona desde los trece años hasta alcanzar la mayoría de edad.

1.9. **Proveedor de Servicios:** Toda entidad pública o privada, que ofrezca a los usuarios de sus servicios la posibilidad de comunicar a través de un sistema informático o cualquier otra entidad que procese o almacene datos informáticos para dicho servicio de comunicación o para los usuarios del mismo. A titulo enunciativo y no limitativo, se consideran proveedores de servicios los proveedores de acceso, los transmisores de datos, los proveedores de servicios de copia temporal de datos, el servicio de alojamiento de datos, el servicio de enlaces o búsquedas y las Entidades de Certificación.

1.10. **Puntos de Acceso Público:** Es un punto de acceso inalámbrico (denominado en inglés *Hotspot*) cuya finalidad primaria es ofrecer el servicio de acceso a Internet, por medio de un pago determinado, o de manera gratuita, así como a otros servicios de red como mensajería instantánea, correo electrónico, video conferencia o Voz sobre IP. Estos incluyen los puntos de acceso de las universidades que permiten acceso a sus estudiantes, puntos de acceso públicos como los de la Secretaría de Estado de la Juventud, el INDOTEL, y otros de similar naturaleza.

1.11. **Sistema Informático:** Dispositivo o conjunto de dispositivos relacionados, conectados o no, que incluyen computadoras u otros componentes como mecanismos de entrada, salida, transferencia y almacenaje, además de circuitos de comunicación de datos y sistemas operativos, programas y datos, para el procesamiento y transmisión automatizada de datos.

1.12. **Solicitud de Datos:** Procedimiento mediante el cual los Órganos de Investigación, solicitan a los Proveedores de Servicios los Datos de tráfico, conexión, acceso de cualquiera de los usuarios de sus servicios;

1.13. **Urgencia (emergencia):** Situación en la cual se encuentre en peligro la vida de una persona, amenazas o ataques contra el Estado dominicano, la Seguridad Nacional o que involucren la figura del Presidente de la República, Secretarios de Estado o funcionarios electos.

Artículo2.- Alcance.-

2.1 Este Reglamento constituye el marco regulatorio que se aplicará en todo el territorio nacional para el proceso de obtención y preservación de datos e informaciones por parte de los proveedores de servicios, en aplicación de las disposiciones de la Ley No. 53-07, sobre Crímenes y Delitos de Alta Tecnología.

2.3 Este Reglamento deberá interpretarse:

(a) Teniendo en cuenta la necesidad de proteger a las personas contra los crímenes y delitos de alta tecnología;

(b) Considerando la importancia que tiene la preservación de los datos de tráfico, conexión y acceso por parte de los Proveedores de Servicios para la persecución de los crímenes y delitos de alta tecnología;

(c) Considerando la importancia de promover una cultura de cooperación –y no de confrontación- entre el Órgano de Investigación y los Proveedores de Servicios; y

(d) Teniendo en cuenta las normas y recomendaciones internacionales en la materia.

2.4 Las menciones y remisiones a normas contenidas en este Reglamento, se entenderán realizadas a aquellas que se encuentren vigentes en el momento de su aplicación, incluyendo sus posibles modificaciones y normas que las complementen o reemplacen.

Párrafo: En caso de modificación de estas normas, las remisiones previstas en el presente Reglamento serán interpretadas de la forma que mejor se adapte al propósito inicial de tal remisión.

Artículo3.- Obligación de conservar datos.-

De acuerdo a lo dispuesto en el artículo 56 de la Ley No. 53-07, los Proveedores de Servicios tienen la obligación de conservar los datos de tráfico, conexión y acceso especificados en el artículo 4 del presente Reglamento, en la medida en que son generados por los usuarios de sus servicios, a fin de que puedan ser utilizados por los Órganos de Investigación en la solución de Crímenes y Delitos de Alta Tecnología.

Artículo 4.- Datos que deben conservarse.-

1. Los Proveedores de Servicios tienen la obligación de conservar los siguientes datos:

a) Datos necesarios para rastrear e identificar el origen de una comunicación:

1) Con respecto a la telefonía de red fija y a la telefonía móvil:

i) El número de teléfono de llamada; y

ii) El nombre y la dirección del usuario del servicio.

2) Con respecto al acceso a Internet, correo electrónico por Internet y telefonía por Internet:

i) La identificación de usuario asignado;

ii) La identificación de usuario y el número de teléfono asignados a toda comunicación que acceda a la red pública de telefonía; y

iii) El nombre y la dirección del usuario del servicio al que se le ha asignado en el momento de la comunicación una dirección de Protocolo Internet (IP), una identificación de usuario o un número de teléfono.

b) Datos necesarios para identificar el destino de una comunicación:

1) Con respecto a la telefonía de red fija y a la telefonía móvil:

i) El número o números marcados (el número o números de teléfono de destino) y, en aquellos casos en que intervengan otros servicios, como el desvío o la transferencia de llamadas, el número o números hacia los que se transfieren las llamadas; y

ii) Los nombres y las direcciones de los usuarios de los servicios.

2) Con respecto al correo electrónico por Internet y a la telefonía por Internet:

i) La identificación de usuario o el número de teléfono del destinatario o de los destinatarios de una llamada telefónica por Internet; y

ii) Los nombres y direcciones de los usuarios de los servicios y la identificación de usuario del destinatario de la comunicación.

c) Datos necesarios para identificar la fecha, hora y duración de una comunicación:

1) Con respecto a la telefonía de red fija y a la telefonía móvil: la fecha y hora del comienzo y fin de la comunicación;

2) Con respecto al acceso a Internet, correo electrónico por Internet y telefonía por Internet:

i) La fecha y hora de la conexión y desconexión del servicio de acceso a Internet, basadas en un determinado huso horario, así como la dirección del Protocolo Internet, ya sea dinámica o estática, asignada por el Proveedor, así como la identificación de usuario registrado; y

ii) La fecha y hora de la conexión y desconexión del servicio de correo electrónico por Internet o del servicio de telefonía por Internet, basadas en un determinado huso horario.

d) Datos necesarios para identificar el tipo de comunicación:

1) Con respecto a la telefonía de red fija y a la telefonía móvil: el servicio telefónico utilizado; y

2) Con respecto al correo electrónico por Internet y a la telefonía por Internet: el servicio de Internet utilizado.

e) Datos necesarios para identificar el equipo de comunicación de los usuarios o lo que se considera ser el equipo de comunicación:

1) Con respecto a la telefonía de red fija: los números de teléfono de origen y destino;

2) Con respecto a la telefonía móvil:

i) Los números de teléfono de origen y destino;

ii) La identidad internacional del abonado móvil (IMSI) de la parte que efectúa la llamada;

iii) La identidad internacional del equipo móvil (IMEI) de la parte que efectúa la llamada;

iv) La IMSI de la parte que recibe la llamada;

v) La IMEI de la parte que recibe la llamada;

vi) En el caso de los servicios anónimos de pago por adelantado, fecha y hora de la primera activación del servicio y la etiqueta de localización (el identificador de celda desde la que se haya activado el servicio.

3) Con respecto al acceso a Internet, correo electrónico por Internet y telefonía por Internet:

i) El número de teléfono de origen en caso de acceso mediante marcado de números; y

ii) La línea digital de abonado (DSL) u otro punto terminal identificador del autor de la comunicación.

f) Datos necesarios para identificar la localización del equipo de comunicación móvil:

1) La etiqueta de localización (identificador de celda) al comienzo de la comunicación; y

2) Los datos que permiten fijar la localización geográfica de la celda, mediante referencia a la etiqueta de localización, durante el período en el que se conservan los datos de las comunicaciones.

2. De conformidad con el presente Reglamento, no podrá conservarse ningún dato que revele el contenido de la comunicación, salvo aquellos casos que cuenten con la orden de una autoridad judicial competente para tal fin.

Artículo 5.- Acceso a los datos.-

1. Los datos conservados por los Proveedores de Servicios, de conformidad con el presente Reglamento, solamente se proporcionarán a los Órganos de Investigación nacionales competentes, siempre que sean requeridos por estos, y cuando sean necesarios en el marco de una investigación abierta por una violación a los bienes jurídicos protegidos por la Constitución, las leyes, decretos, reglamentos y resoluciones.

2. Para el acceso a dichos datos los Proveedores de Servicios y los Órganos de Investigación, deberán respetar los Derechos Fundamentales de los usuarios, consagrados en la Constitución de la República, en especial los relativos al Derecho a la Intimidad, a la inviolabilidad de las Comunicaciones y a la Protección de Datos de Carácter Personal.

3. Las reglas de la comprobación inmediata y medios auxiliares del Código Procesal Penal serán aplicables para la obtención y preservación de los datos contenidos en un sistema de información o de telecomunicaciones, así como cualquier otra información de utilidad, en la investigación de los crímenes y delitos de alta tecnología.

Artículo 6.- Períodos de conservación.-

Los Proveedores de Servicios garantizarán que los datos mencionados en el artículo 4 se conservarán por un período de tiempo que no será inferior a noventa (90) días laborables, ni superior a dos (2) años a partir de la fecha de su generación y conservación.

TÍTULO II

RÉGIMEN PROCEDIMENTAL PARA LA PRESERVACIÓN DE LOS DATOS

CAPITULO I

OBLIGACIONES Y MEDIDAS DE LOS ÓRGANOS DE INVESTIGACIÓN Y DE LOS PROVEEDORES DE SERVICIOS

Artículo 7.- Obligaciones y medidas de los Órganos de Investigación.-

Los Órganos de Investigación tienen las siguientes obligaciones:

a) Asistir a los Proveedores de Servicios realizando seminarios de entrenamiento técnicos y legales, así como suministrando información sobre las investigaciones basadas en las quejas interpuestas por los Proveedores de Servicios o por la inteligencia recolectada basada en la actividad criminal divulgada por los Proveedores de Servicios;

b) Elaborar los procedimientos escritos para el proceso de las solicitudes de investigación y asegurarse de que dichas solicitudes sean llevadas a cabo conforme a los procedimientos establecidos; las cuales deberán contener, como mínimo, lo siguiente:

    1. Los documentos o informaciones que debe presentar el solicitante ante la unidad de investigación correspondiente, para dar inicio a una investigación;
    2. El procedimiento que debe seguir la unidad de investigación encargada, para solicitar la documentación y/o información al Proveedor de Servicios, indicando las personas en los

órganos de investigación con capacidad de solicitar la información y/o documentación necesaria;

3. El tratamiento que debe dar la unidad encargada a la información y/o documentación obtenida a lo interno de la institución, a los fines de realizar la investigación en cuestión.

c) Proporcionar el entrenamiento necesario a su personal en cómo ejecutar los procedimientos descritos en el literal b) anterior, incluyendo la manera mediante la cual los datos pueden obtenerse de los Proveedores de Servicios y cómo procesar la información recibida;

d) Equipar al personal responsable de la cooperación con los Proveedores de Servicios de los recursos técnicos necesarios, incluyendo el acceso a Internet, dirección de correo electrónico institucional y otros recursos técnicos para permitir que reciban la información de los Proveedores de Servicios en el plazo requerido;

e) Designar al personal debidamente entrenado para interactuar con los Proveedores de Servicios;

f) Definir claramente en sus procedimientos escritos quién o quiénes de su personal puede(n) autorizar qué tipo de medidas y de solicitudes a los Proveedores de Servicios y cómo estas solicitudes pueden ser validadas/autenticadas por los Proveedores de Servicios;

g) Poner a disposición de los Proveedores de Servicios la información acerca de sus procedimientos y, en lo posible, quién de su personal es responsable de la cooperación con los Proveedores de Servicios;

h) Asegurar que las solicitudes enviadas sean específicas, completas y claras, y que proporcionen un nivel suficiente de detalle para permitir que los Proveedores de Servicios identifiquen los datos relevantes. Así mismo deben asegurarse de que las solicitudes sean enviadas al Proveedor de Servicios correspondiente;

i) Proporcionar tantos hechos sobre la investigación como sea posible, sin perjudicar la investigación o ningún derecho fundamental, para permitir a los Proveedores de Servicios identificar los datos relevantes;

j) Proporcionar explicaciones y asistencia a los Proveedores de Servicios con respecto a técnicas no relacionadas con casos de investigación para que entiendan cómo su cooperación dará lugar a investigaciones más eficientes contra el crimen y a una mejor protección para los ciudadanos;

k) Priorizar las solicitudes, especialmente las relacionadas con los volúmenes grandes de datos, para permitir a los Proveedores de Servicios tratar las más importantes primero;

l) Asegurar la confidencialidad de los datos recibidos;

m) Evitar los costes y las interrupciones innecesarias de las operaciones comerciales de los Proveedores de Servicios y de otros tipos de negocios para la remisión de las solicitudes;

n) Restringir el uso de los contactos de emergencia a los casos extremadamente urgentes para asegurarse de que este servicio no sea abusado;

ñ) Asegurar que las órdenes de preservación y otras medidas provisionales sean ejecutadas con la mayor rapidez posible y que el Proveedor de Servicios sea informado a tiempo de que los datos preservados ya no son requeridos;

o) Coordinar su cooperación con los Proveedores de Servicios y compartir buenas prácticas tanto nacional como internacionalmente;

p) Dar seguimiento y revisar el sistema de procesar las solicitudes con fines estadísticos, para identificar las fortalezas y debilidades y publicar tales resultados si lo considera apropiado.

Artículo 8.- Obligaciones y medidas de los Proveedores de Servicios.-

Los Proveedores de Servicios tienen las siguientes obligaciones:

a) Cooperar con los Órganos de Investigación para ayudar a reducir al mínimo el grado en el cual sus servicios son utilizados para la actividad criminal según lo definido por las leyes;

b) Notificar a los Órganos de Investigación de los casos que afecten a cualquier Proveedor de Servicios de los cuales tengan conocimiento. Esto no obliga a los Proveedores de Servicios a buscar activamente hechos o circunstancias que indiquen actividades ilegales;

c) Asistir a los Órganos de Investigación con programas de educación, entrenamiento y cualquier otra ayuda para el buen desarrollo de sus operaciones;

d) Emprender todos los esfuerzos razonables para asistir a los Órganos de Investigación en la ejecución de una solicitud;

e) Elaborar procedimientos escritos para el proceso de las solicitudes, indicando plazos de respuesta dependiendo de la información y/o documentación requerida, y asegurarse que el personal encargado de procesarlas las lleve a cabo conforme a los procedimientos establecidos;

f) Cerciorarse de que el personal responsable de ejecutar los procedimientos mencionados en el literal e) anterior, tenga suficiente entrenamiento para llevar a cabo dicha labor;

g) Designar al personal debidamente entrenado, como punto de contacto para la cooperación con los Órganos de Investigación;

h) Establecer los medios a través de los cuales los Órganos de Investigación pueden contactar su personal designado fuera de horas laborables normales para tratar situaciones de casos de emergencia;

i) Proporcionar al personal responsable de la cooperación con los Órganos de Investigación, los recursos necesarios para permitirles cumplir con las solicitudes formuladas por estos;

j) Organizar su cooperación con los Órganos de Investigación bajo la forma de programas de contactos, y proporcionar una descripción de tales programas a los Órganos de Investigación, incluyendo:

    1. La información necesaria para contactar al personal designado, así como las horas durante las cuales tal personal está disponible;

2. La información requerida para que los Órganos de Investigación puedan remitir solicitudes al personal designado;
3. Otros detalles específicos de conformidad con el personal de contacto designado a (tal fin como en el caso de que un Proveedor de Servicio que opere en varios países, documentos que deben traducirse a una lengua particular etc.);
4. Proporcionar la información sobre el tipo de servicios que ofrecen a los usuarios, incluyendo *web links* a los servicios y a cualquier información adicional, así como a los datos de contacto para mayor información;

k) Proporcionar una lista, a petición de los Órganos de Investigación, de los tipos de datos que se podrían hacer disponibles para cada servicio al recibo de una solicitud, aceptando los Órganos de Investigación que no todos estos datos estarán disponibles para cada investigación;

l) Verificar la autenticidad y procedencia de las solicitudes recibidas de los Órganos de Investigación, en la medida de lo posible para asegurarse que los datos de sus clientes no sean divulgados a personas no autorizadas;

m) Responder a las solicitudes de los Órganos de Investigación por escrito y asegurándose que dichos documentos estén disponibles en el plazo establecido en los procedimientos;

n) Estandarizar el formato para enviar la respuesta a las solicitudes de los Órganos de Investigación;

ñ) Procesar las solicitudes a tiempo, conforme a los procedimientos establecidos;

o) Asegurar que la información transmitida a los Órganos de Investigación sea completa, exacta y esté debidamente protegida;

p) Asegurar la confidencialidad de las solicitudes recibidas;

q) Proporcionar explicaciones al Órgano de Investigación que envía la solicitud si la misma es rechazada o la información solicitada no puede ser proporcionada;

r) Dar seguimiento y revisar el sistema para procesar las solicitudes con fines estadísticos, para identificar las fortalezas y debilidades de dicho procedimiento y publicar tales resultados si lo consideran apropiado.

CAPITULO II

SOLICITUDES, DOMICILIOS, PROCEDIMIENTOS Y PLAZOS

Artículo 9.- Solicitudes.-

1. Todas las Solicitudes de los Órganos de Investigación a los Proveedores de Servicio, a las que se refiere el presente Reglamento, serán formuladas por escrito, utilizando por lo menos uno de los siguientes métodos:

    a) Documentos digitales o mensajes de datos firmados digitalmente, transmitidos mediante protocolos de comunicación electrónica tales como correo electrónico, transferencia de archivos, entre otros;

b) Correspondencia con acuse de recibo;

c) Acto de Alguacil; o

d) Cualquier otro medio físico o electrónico que pueda dejar constancia de la certitud de su recepción, la identidad del autor y de la integridad y confidencialidad del contenido de la misma.

2. Para los efectos de este Reglamento, toda Solicitud que se haga de conformidad con las letras b) y c) deberá ser entregada, para el caso de una persona física o natural, a su persona o en su residencia o domicilio constituido, y para el caso de una persona jurídica, entregadas a la persona de su representante legal o un(a) funcionario(a) acreditado(a) del notificado, o en su domicilio constituido, en ambos casos, dejando constancia del día, hora y lugar en que se practicó la notificación, así como el nombre de la persona que la recibió y su relación con el requerido.

Artículo 10.-Punto de Contacto de los Órganos de Investigación.-

1. A fin del presente Reglamento, el Departamento de Investigación de Crímenes y Delitos de Alta Tecnología (DICAT) de la Policía Nacional, fungirá como el punto de contacto entre los Proveedores de Servicios y los Órganos de Investigación.

2. El DICAT recibirá las comunicaciones cursadas por medio de escritos en formato papel en la Avenida Leopoldo Navarro, esquina Avenida México, Palacio de la Policía Nacional, Santo Domingo de Guzmán, Distrito Nacional, Republica Dominicana u otra dirección que previamente publique el DICAT en un diario de circulación nacional.

3. El DICAT recibirá las comunicaciones cursadas por medios electrónicos en la dirección de correo electrónico dicat@policianacional.gob.do y en los formularios que a tal efecto se habiliten en la página Web http://www.policianacional.gob.do/dicat .

Artículo 11.- Registro de Domicilio.-

1. Los Proveedores de Servicios deberán registrar una dirección de correo electrónico ante el DICAT en la cual se considerarán válidas las comunicaciones y solicitudes.

2. Los cambios de direcciones de correo electrónico registrado deberán ser informados al DICAT, en un plazo no menor de treinta (30) días calendarios previos al cambio de dicha dirección.

Artículo 12.- Procedimiento para la remisión de Solicitudes por parte de los Órganos de Investigación.-

1. Todas las Solicitudes a los Proveedores de Servicios de datos de tráfico, conexión y acceso de los usuarios de sus servicios se realizará mediante comunicación de acuerdo a lo establecido en el artículo 9 de este Reglamento, de parte del órgano encargado de investigar el ilícito de que trate, a través del Ministerio Público correspondiente, el cual a su vez la remitirá al Proveedor de Servicios en cuestión.

2. Para los casos relacionados a crímenes contra la humanidad; crímenes y delitos contra la Nación, el Estado y la paz pública; amenazas o ataques contra el Estado dominicano, la Seguridad Nacional o que involucren la figura del Presidente de la República, Secretarios de

Estado o funcionarios electos, de acuerdo a lo que dispone la Ley No. 53-07, el órgano encargado de investigar dichos ilícitos será la División de Investigación de Delitos Informáticos (DIDI) del Departamento Nacional de Investigaciones (DNI), en coordinacion con el Departamento de Investigación de Crímenes y Delitos de Alta Tecnología (DICAT) de la Policía Nacional.

3. Para todas los demás crímenes y delitos no establecidos en el numeral 2 precedente, el órgano encargado de investigar dichos ilícitos será el Departamento de Investigación de Crímenes y Delitos de Alta Tecnología (DICAT) de la Policía Nacional.

4. Para las Solicitudes de datos de tráfico, conexión y acceso de los usuarios de sus servicios a Proveedores de Servicios extranjeros, se realizará mediante comunicación de acuerdo a lo establecido en el artículo 9 de este Reglamento, de parte del órgano encargado de investigar el ilícito de que trate, a través del Ministerio Público correspondiente, el cual a su vez la remitirá al Órgano de Investigación correspondiente en el país donde esté ubicado el Proveedor de Servicio, el cual a su vez la remitirá al Proveedor de Servicios en cuestión o, en su defecto, a las redes de cooperación internacional en materia de delitos informáticos.

Artículo 13.- Requisitos de las Solicitudes a los Proveedores de Servicios.-

1. Todas las Solicitudes a los Proveedores de Servicios deberán ser realizadas por escrito. En casos de extrema urgencia serán aceptables solicitudes orales, las cuales deberán ser seguidas por su correspondiente solicitud por escrito.

2. En cuanto a la forma, las Solicitudes deberán cumplir como mínimo con los siguientes requerimientos:

   a) Toda la comunicación debe incluir el nombre de contacto, el número de teléfono y la dirección de correo electrónico del agente del Órgano de Investigación que busca los datos de modo que el Proveedor de Servicios pueda entrar en contacto con el solicitante si se presentase cualquier asunto;

   b) Los Proveedores de Servicios no serán contactados por un agente de los Órganos de Investigación a través de un correo electrónico personal del agente, sino a través de una cuenta de correo electrónico institucional;

   c) Todas las comunicaciones deben estar en papel con membrete del departamento, y toda la correspondencia debe incluir el número de la central telefónica y la dirección del Portal Web de la agencia del Órgano de Investigación, de modo que los Proveedores de Servicios puedan tomar medidas para verificar la autenticidad de solicitudes si lo juzgan apropiado; De todas formas, las solicitudes también podrán ser enviadas en formato electrónico si están firmadas digitalmente. En adición a esto se podrán utilizar otros medios de autenticación electrónica previamente acordados entre las partes.

3. En cuanto a su contenido, las Solicitudes como un mínimo deben contener la siguiente información:

   a) El número de registro;

   b) Referencia al fundamento jurídico;

c) Los datos específicos solicitados; y

d) La información para verificar el origen de la solicitud.

Artículo 14.- Procedimiento para la remisión de las respuestas a las Solicitudes de los Órganos de Investigación.-

1. Todo Proveedor de Servicios que sea destinatario de una Solicitud de acuerdo con lo previsto en el literal a) del Artículo 9 del presente Reglamento, deberá acusar recibo de la recepción de dicha solicitud.

2. Dicho acuse de recibo se remitirá mediante documentos digitales o mensajes de datos firmados digitalmente a la misma dirección de correo electrónico utilizada por el Órgano de Investigación para remitir la Solicitud, en el plazo máximo de veinticuatro (24) horas desde su recepción.

3. El acuse de recibo deberá incluir el siguiente contenido mínimo:

   a) Mención expresa a la naturaleza de "Acuse de Recibo";

   b) El número de registro de la Solicitud; y

   c) Fecha y hora en la que el documento digital o mensaje de dato fue recibido por el Proveedor de Servicios.

4. Todo Proveedor de Servicios que sea destinatario de una Solicitud por parte de los Órganos de Investigación deberá verificar la autenticidad de dicha solicitud para asegurarse que los datos de sus clientes no serán divulgados a personas no autorizadas.

5. Todo Proveedor de Servicios que sea destinatario de una Solicitud deberá responder a dicha Solicitud en lo plazos establecidos en el artículo 15 del presente Reglamento.

Artículo 15.- Plazo para la entrega de los datos.-

1. Los Proveedores de Servicios deberán responder las Solicitudes de los Órganos de Investigación en un plazo máximo de cinco (5) días calendario.

2. Para los casos de emergencia o urgencia de acuerdo a lo establecido en el artículo 1 del presente Reglamento, el plazo de respuesta a las Solicitudes por parte de los Proveedores de Servicios será de veinticuatro (24) horas.

TÍTULO III

DE LA REGULACIÓN DE LOS CENTROS DE ACCESO PÚBLICO, PUNTOS DE ACCESO PÚBLICO Y SOBRE EL BLOQUEO DE CONTENIDO DE PÁGINAS EN INTERNET CON CONTENIDO DE EXPLOTACIÓN SEXUAL COMERCIAL DE NIÑOS, NIÑAS Y ADOLESCENTES

Artículo 16.- Obligaciones de los propietarios de los Centros de Acceso Público.-

1. Los propietarios de los Centros de Acceso Público tendrán las siguientes obligaciones:

a) Mantener un registro de los usuarios, no inferior a noventa (90) días laborables, con el nombre, Cédula de Identidad y Electoral u otro documento de identidad como el pasaporte, en el caso de extranjeros, o en su defecto fecha de nacimiento y nacionalidad del usuario, fecha, hora y duración del servicio e individualización del equipo utilizado;

b) Prohibir el acceso a páginas de Internet, chats, portales o cualquier programa de contenido de Explotación Sexual Comercial de niños, niñas y adolescentes;

c) Implementar mecanismos de seguridad como programas y aplicaciones que impidan el acceso a páginas y similares con contenido de Explotación Sexual Comercial de niños, niñas y adolescentes;

d) Supervisar a los niños, niñas y adolescentes mientras se encuentren en los Centros de Acceso Público; y

e) En caso de los Centros de Acceso Público que poseen "Salas privadas", las cuales no pueden ser supervisadas por los propietarios de los Centros de Acceso Público, prohibir el acceso a niños, niñas y adolescentes a dichas salas.

2. Los propietarios de los Centros de Acceso Público tendrán un plazo de noventa (90) días calendario, a partir de la entrada en vigencia del presente Reglamento, para adecuar e implementarlas medidas y mecanismos de seguridad necesarios para el cumplimiento de las obligaciones establecidas en este Reglamento.

Artículo 17.- Obligaciones de los propietarios de los Puntos de Acceso Público.-

1. Los propietarios de los Puntos de Acceso Público tendrán las siguientes obligaciones:

a) Crear un registro inicial, en el cual los usuarios de sus servicios deban registrar sus datos, tales como nombre, Cédula de identidad y Electoral o en su defecto fecha de nacimiento y nacionalidad;

b) No permitir el acceso de usuarios "anónimos". Aun el servicio sea gratuito los usuarios deberán registrarse creando cuentas de usuario en las que se deberá almacenar la dirección MAC (MAC Address) de la tarjeta inalámbrica del equipo del usuario;

c) Mantener un registro de los usuarios de sus servicios, no inferior a noventa (90) días laborables, de páginas de Internet que fueron visitadas, así como cuánto tiempo duraron en ellas. Este registro debe incluir la dirección MAC, la dirección IP pública asignada por el enrutador inalámbrico al momento de la conexión, la fecha y la hora de las mismas;

d) Prohibir el acceso a páginas Web, chats, portales o cualquier programa de contenido de Explotación Sexual Comercial de niños, niñas y adolescentes;

e) Implementar mecanismos de seguridad como programas y aplicaciones que impidan el acceso a páginas y similares con contenido de Explotación Sexual Comercial de niños, niñas y adolescentes.

2. Los propietarios de los Puntos de Acceso Público tendrán un plazo de noventa (90) días calendario, a partir de la entrada en vigencia del presente Reglamento, para adecuar e

implementar las medidas y mecanismos de seguridad necesarios para el cumplimiento de las obligaciones establecidas en este Reglamento.

Artículo 18.- Obligación de los Proveedores de Servicio de bloquear páginas en el Internet con contenido de Explotación Sexual Comercial de Niños, Niñas y Adolescentes.-

Los Proveedores de Servicio tendrán la obligación de proceder a realizar el bloqueo de páginas en Internet con contenido de Explotación Sexual Comercial de Niños, Niñas y Adolescentes, en la medida en que sean detectadas por los Proveedores, usuarios o por los organismos de investigación y prevención en la materia.

Artículo 19.- Criterios para la evaluación y clasificación del contenido de páginas en Internet para ser considerado de Explotación Sexual Comercial de Niños, Niñas y Adolescentes.-

1. Los Proveedores de Servicios para poder clasificar un material de Explotación Sexual Comercial de Niños, Niñas y Adolescentes tendrán en cuenta los siguientes criterios:

    a) Las definiciones y conceptos establecidos en el artículo 1 del presente Reglamento, en particular las referentes a Abuso Sexual, Explotación Sexual Comercial de Niños, Niñas y Adolescentes y Pornografía Infantil, así como las definiciones de Agresión Sexual y Violación según lo establecido por la Ley 24-97, que modifica el Código Penal Dominicano, y sanciona la violencia contra la mujer, doméstica e intrafamiliar;

    b) Presentación de las partes genitales de un niño, niña o adolescente con fines sexuales, o en un contexto de página pornográfica o como parte de una escena sexual (conjunto de acciones de índole sexual);

    c) Escenas sexuales con animales o figuras fantasiosas o imágenes o figuras virtuales, digitalizadas o creadas;

    d) Escenas sexuales que involucren violencia, tortura, sometimiento, o similares;

    e) Niños, niñas, adolescentes o adultos con apariencia de niños o niñas, que aparecen en contextos utilizados por adultos y prohibidos para niños por la ley. Ej.: bares, prostíbulos y que se encuentren en el contexto de una página pornográfica o como parte de una escena sexual;

    f) Que el contexto de la página o escena incluya o sugiera expresa o sutilmente, reserva, secreto o confidencialidad o invitación a ser parte o miembro activo de esa comunidad;

    g) Niños, niñas y adolescentes utilizando artículos o juguetes sexuales en un contexto de página pornográfica o como parte de una escena sexual o en cualquier otro contexto;

    h) Representaciones simbólicas referidas a objetos de uso de niños, niñas o adolescente tales como juguetes, ropa, accesorios y comestibles;

    i) Que el contexto de la página o escena incluya oferta de servicio o posibilidad de compraventa de material, contraprestación, pago por ver, o solicitudes de carácter sexual;

j) Cualquier página que promueva al país como paraíso de la Explotación Sexual Comercial de Niños, Niñas y Adolescentes;

2. Para aplicar los criterios descritos anteriormente, los Proveedores de Servicios deberán tener en cuenta:

a) Si no resulta claramente aplicable uno o más criterios de los mencionados anteriormente, la página debe ser descartada.

b) En caso de duda se sugiere revisar con mayor detenimiento el contenido de la página antes de cualquier decisión. Si no es posible confirmar, la sugerencia es descartar.

c) La aplicación de un solo criterio puede ser suficiente para proceder a hacer inaccesible dicho contenido.

d) En ocasiones es necesaria la aplicación de dos o más criterios para clasificar el material.

e) Es posible que apliquen dos o más criterios, pero ello no es imprescindible.

TÍTULO IV

DISPOSICIONES FINALES

Artículo 20.- Sanciones.-

Serán susceptibles de ser sancionados con las penas establecidas por el artículo 60 de la Ley 53-07 sobre Crímenes y Delitos de Alta Tecnología los Proveedores de Servicio, los propietarios de los Puntos de Acceso Público y de los Centros de Acceso Público que no cumplan con las obligaciones de conservación de los datos establecidos por los artículos 3, 16, 17 y la obligación de páginas en Internet con contenido de Explotación Sexual Comercial de Niños, Niñas y Adolescentes, según lo establece el artículo 18 y 19 del presente Reglamento.

Artículo 21.- Reglamentación sobre los Criterios de Seguridad de los Centros y Puntos de Acceso Público.-

Para el cumplimiento de las obligaciones establecidas en los artículos 16 y 17 sobre las obligaciones de los propietarios de los Centros y Puntos de Acceso Públicos, el Instituto Dominicano de las Telecomunicaciones (INDOTEL) tendrá la potestad de definir reglamentariamente, mediante Resolución, los criterios técnicos de seguridad que deban cumplir estos centros y puntos de acceso para garantizar el cumplimiento de dichas obligaciones.

Artículo 22.- Entrada en Vigencia.-

El presente Reglamento entrará en vigencia desde la fecha de su publicación en la Gaceta Oficial o en un periódico de circulación nacional.