INSTITUTO DOMINICANO DE LAS TELECOMUNICACIONES (INDOTEL)

RESOLUCIÓN No. 086-11

QUE APRUEBA 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, en ejercicio de las facultades conferidas por la Ley General de Telecomunicaciones, No. 153-98, por la Ley de Comercio Electrónico, Documentos y Firmas Digitales, No. 126-02 y por el Decreto No. 335-03, que aprueba el Reglamento de Aplicación de esta última, ha dictado la presente **RESOLUCIÓN**:

Con motivo 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 29 de junio de 2009, el Consejo Directivo del **INDOTEL** dictó su Resolución No. 056-09, mediante la cual ordenó 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", con el objeto de dar cumplimiento a lo dispuesto en el artículo 56 de la Ley No. 53-07, sobre la facultad del **INDOTEL** para crear un reglamento para el procedimiento de obtención y preservación de datos e informaciones por parte de los proveedores de servicios y cuyo dispositivo reza textualmente:

> ***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.*

2. La indicada Resolución No. 056-09, fue publicada en fecha 17 de septiembre de 2009 en el periódico "Listin Diario", y dispuso un plazo de treinta (30) días calendario, contados a partir de la publicación de la misma, para que los interesados presentaran las observaciones, comentarios o sugerencias que estimaran pertinentes sobre dicha norma.

3. Del 15 al 30 de octubre de 2009, las empresas **ONEMAX, S. A.**, (en adelante "**ONEMAX**"), **TRYLOGY DOMINICANA, S. A.** (en adelante "**VIVA**"), **COMPAÑÍA DOMINICANA DE TELEFÓNOS, S. A.,** (en adelante **"CLARO"**)**, ORANGE DOMINICANA, S. A**. (en adelante "**ORANGE**") y **TRICOM, S. A.** (en adelante **"TRICOM"**), depositaron por ante este órgano regulador sus comentarios a la citada resolución.

4. En fecha 23 de abril de 2010, el Consejo Directivo de **INDOTEL** celebró la Audiencia Pública en cuestión, ejerciendo su derecho de participación en la misma los representantes acreditados de las empresas **ONEMAX, VIVA, CLARO, ORANGE** y **TRICOM**;

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 No. 53-07 contra Crímenes y Delitos de Alta Tecnología, sino también, en su proceso de aprobación y ejecución;

CONSIDERANDO: Que la Ley No. 53-07 contra Crímenes y Delitos 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, así como 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, que *[…] 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 Civiles y Políticos de los ciudadanos, en particular en lo que respecta al Derecho a la Intimidad, el numeral 3 del Artículo 44 de la Constitución de la República Dominicana establece que:

> *3) Se reconoce la inviolabilidad de la correspondencia, documentos o mensajes privados en formatos físico, digital, electrónico o de todo otro tipo. Sólo podrán ser ocupados, interceptados o registrados, por orden de una autoridad judicial competente, mediante procedimientos legales en la sustanciación de asuntos que se ventilen en la justicia y preservando el secreto de lo privado, que no guarde relación con el correspondiente proceso. Es inviolable el secreto de la comunicación telegráfica, telefónica, cablegráfica, electrónica, telemática o la establecida en otro medio, salvo las autorizaciones otorgadas por juez o autoridad competente, de conformidad con la ley;*

CONSIDERANDO: Que el precitado numeral 3, consagra el principio constitucional sobre la inviolabilidad de las comunicaciones, haciéndose extensible a cualquier toda 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, cablegráfica, electrónica o telemática. 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 el artículo 52 la Ley No. 53-07 dispone que *las reglas de la comprobación inmediata y medios auxiliares del Código Procesal Penal, Ley No. 76-02, se aplicarán para la obtención y preservación de los datos contenidos en un sistema de información o sus componentes, datos de tráfico, conexión, acceso o cualquier otra información de utilidad, en la investigación de los delitos penalizados en la presente ley…;*

CONSIDERANDO: Que el artículo 192 del Código Procesal Penal, Ley No. 76-02, en lo que respecta a la Interceptación de las Telecomunicaciones, establece que *se requiere autorización judicial para la interceptación, captación y grabación de las comunicaciones, mensajes, datos, imágenes o sonidos transmitidos a través de redes públicas o privadas de telecomunicaciones por el imputado o cualquier persona que pueda facilitar razonablemente información relevante para la determinación de un hecho punible, cualquiera sea el medio técnico utilizado conocerlas…;*

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*;

CONSIDERANDO: Que conforme lo dispuesto por el artículo 93 de la Ley General de Telecomunicaciones, No. 153-98, antes de dictar resoluciones de carácter general, el órgano regulador deberá consultar a los interesados, debiendo quedar constancia escrita de la consulta y sus respuestas;

CONSIDERANDO: Que el Consejo Directivo del **INDOTEL** tiene el deber de ponderar los comentarios que ha recibido con ocasión de la puesta en consulta pública del **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**, contenida en la Resolución No.056-09 de este organismo colegiado;

CONSIDERANDO: Que durante el período de consulta pública habilitado por este Consejo Directivo, a fin de recibir los comentarios de los posibles interesados en la redacción final de la modificación del indicado reglamento, fueron recibidos comentarios por parte de las concesionarias **ONEMAX, VIVA, CLARO, ORANGE** y **TRICOM**, los cuales serán analizados en el cuerpo de la presente Resolución;

CONSIDERANDO: Que en tal virtud, el Consejo Directivo del **INDOTEL**, en cumplimiento del mandato contenido en el artículo 93.1 antes citado, se abocará al análisis de los comentarios y observaciones recibidos por parte de **ONEMAX, VIVA, CLARO, ORANGE** y **TRICOM**, sobre la propuesta de reglamento de que se trata, cuyas opiniones no serán vinculantes para este órgano regulador, conforme lo establece el artículo 93.2 de la Ley General de Telecomunicaciones, No.153-98;

CONSIDERANDO: Que, no obstante todos los comentarios presentados por las empresas que participaron del proceso de consulta pública han sido conocidas y evaluadas por este órgano regulador, por razones de economía procesal y simplificación en la presentación de la norma, las mismas serán colocadas de manera íntegra en un archivo, el cual se encontrará publicado como un anexo a la presente Resolución y 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, en la página Web que mantiene el **INDOTEL** en la red de Internet y disponible para consulta en las oficinas del órgano regulador, dando así cumplimiento al mandato del artículo 93.1 de la Ley;

CONSIDERANDO: Que los comentarios presentados en ocasión del proceso de consulta pública en torno a la propuesta 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**, se centraron en siete (7) puntos, a saber: Los datos que deben conservarse por los Proveedores de Servicio (artículo 4), los períodos de conservación de los datos (artículo 6), los requisitos de las solicitudes a los Proveedores de Servicios (artículo 13), las obligaciones de los propietarios de los Centros de Acceso Público (artículo 16), las obligaciones de los propietarios de los Puntos de Acceso Público (artículo 17), la obligación de los Proveedores de Servicio de bloquear páginas en Internet con contenido de material de abuso infantil (artículo 18) y el plazo para la entrada en vigencia del reglamento (artículo 22);

CONSIDERANDO: Que las concesionarias que han realizado comentarios respecto del reglamento en proceso de consulta pública han emitido sus criterios en cuanto a los datos que deben conservarse por los Proveedores de Servicio;

CONSIDERANDO: Que el objetivo principal de este Reglamento es facilitar la investigación de los Crímenes y Delitos de Alta Tecnología, independientemente de la relación que el usuario tenga con la prestadora. Por lo tanto, lo que se persigue es identificar/rastrear quién es la persona que hace uso de dicho servicio en un tiempo específico;

CONSIDERANDO: Que en ese sentido, la obligación de almacenar los datos de tráfico, conexión y acceso por parte de los Proveedores de Servicio sólo se extiende a los datos de sus clientes y bajo ninguna circunstancia puede entenderse que se extiende a almacenar los datos de otros proveedores. Así, cada Proveedor tiene la obligación de almacenar los datos que permitan rastrear e identificar el origen, destino, fecha, hora, duración tipo, equipo y localización de una comunicación;

CONSIDERANDO: Que en cuanto a los datos necesarios para identificar el tipo de comunicación los datos que se solicitan a los Proveedores de Servicios se refiere a aquellos datos que identifican una comunicación en particular, en los casos de la telefonía de red fija y a la telefonía móvil: el servicio telefónico utilizado se refiere a la telefonía fija, móvil, prepago o postpago; en los casos que se refieren al correo electrónico por Internet y a la telefonía por Internet, no se está requiriendo el tipo de tecnología utilizado (ADSL, Dial-Up), sino a qué servicio por internet utiliza el usuario en particular;

CONSIDERANDO: Que en lo que respecta a los datos necesarios para identificar el equipo de comunicación de los usuarios o lo que se considera ser el equipo de comunicación, en particular, la IMSI de la parte que recibe la llamada; la IMEI de la parte que recibe la llamada; y los servicios anónimos, este Consejo Directivo ha considerado prudente eliminar dichos datos del listado de los que deben ser conservados, en virtud de que en la actualidad la prestadora con la cual el usuario posee un servicio contratado, no dispone de la información relacionada con la IMSI y la IMEI de la parte que recibe una comunicación y por ende le resulta imposible almacenar dichos datos;

CONSIDERANDO: Que dentro de las obligaciones que se han establecido en el presente reglamento no se les ha solicitado a los Proveedores de Servicios guardar los datos de llamadas generadas mediante el uso de servicios Web públicos tipo Skype, MSN, Google talk y similares; en caso de que los Órganos de Investigación deseen obtener dicho datos de tráfico, conexión y acceso de dichos servicios deberán hacerlo en atención al Proveedor de Servicio que ofrece el mencionado servicio;

CONSIDERANDO: Que en cuanto a la prohibición de conservar datos referentes al contenido de una comunicación a menos que medie una orden de una autoridad judicial competente para tal fin, es preciso aclarar que dicha disposición lo que viene es a establecer que todo proveedor de servicios, conforme dispone la Ley No. 53-07 y el presente reglamento, tiene la obligación de guardar los datos de tráfico, conexión y acceso de sus usuarios, sin embargo, les está prohibido guardar la información referente al contenido de la comunicación que se llevó a cabo;

CONSIDERANDO: Que en tal sentido, en lo que respecta al Servicio de Mensajería de Texto Corta (SMS), este Consejo Directivo entiende pertinente esclarecer que almacenar el contenido de los mismos sin la debida orden de una autoridad judicial competente, constituye una violación al artículo 5 de la Ley General de Telecomunicaciones, No. 153-98, en cuanto a la inviolabilidad y secreto de las telecomunicaciones; Por lo tanto, los Proveedores de Servicio deberán asegurarse de almacenar los datos los datos de tráfico, conexión y acceso de sus usuarios correspondientes omitiendo el contenido de dicha comunicación;

CONSIDERANDO: Que entre los comentarios planteados sobre la Resolución No. 056-09 en lo referente a los períodos de conservación de los datos de tráfico conexión y acceso de los usuarios de sus servicios, considerando que conforme lo establecido por el artículo 56 de la Ley No. 53-07, se establece un plazo mínimo de noventa (90) días en el cual los Proveedores de Servicios deben almacenar los datos mencionados precedentemente y que el **INDOTEL** mediante el presente Reglamento establece un período máximo de dos años para la guarda de esta información, lo que genera un impacto en capacidad, y por ende, económico en las operaciones y presupuesto de las empresas;

CONSIDERANDO: Que como bien se ha afirmado el artículo 56 de la Ley No. 53-07 pone en manos de este órgano regulador la elaboración de un Reglamento que establezca los procedimientos de obtención y preservación de los datos de tráfico conexión y acceso de los usuarios. Que asimismo, el mencionado artículo 56 establece un plazo durante el cual los Proveedores de Servicios deben almacenar dichos datos estableciendo un plazo mínimo de noventa (90) días;

CONSIDERANDO: Que se hace preciso aclarar que la redacción propuesta para el artículo 6 del Reglamento deja en completa libertad al Proveedor de Servicios de elegir el tiempo de conservación de los datos de tráfico conexión y acceso, siempre que sea entre el plazo de noventa (90) días a dos (2) años. Por lo tanto, todo Proveedor de Servicios que desee conservar dichos datos por un período superior a los noventa (90) días lo podrá hacer siempre y cuando ese período no exceda de los dos (2) años;

CONSIDERANDO: Que en lo que se refiere a la distinción entre días calendarios y laborales para la conservación de los datos de tráfico conexión y acceso, este Consejo Directivo entiende pertinente acoger la propuesta realizada por las concesionarias respecto de no cambiar los noventa (90) días calendario por noventa (90) días laborables, en razón de las diferentes variables que debe tomarse en consideración para realizar cambios en las aplicaciones y en las

plataformas de los Proveedores de Servicio, sin contar la inversión significativa que representa adquirir la capacidad de almacenamiento adicional requerida para dichos fines;

CONSIDERANDO: Que entre las observaciones a la Resolución No. 056-09, se presentó el que versa sobre la oralidad de las Solicitudes a los Proveedores de Servicios en caso de urgencia, considerando las concesionarias las solicitudes deben ser siempre por escrito, no deben ser aceptables las solicitudes orales puesto que no hay ninguna garantía para el Proveedor de Servicios de la regularidad de tal solicitud, ni de que eventualmente estas serán seguidas por la solicitud escrita. Asimismo son del criterio que se debe de poner un plazo dentro del cual la solicitud por escrito debe ser entregada a los Proveedores de Servicios, puesto que en caso de que el mismo quede abierto, podría tardar demasiado y poner en riesgo los derechos del usuario sobre el cual se requieren los datos;

CONSIDERANDO: Que según el artículo 1 de la propuesta 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** se considera como un caso de urgencia toda situación en la cual se encuentre en peligro la vida de una persona, amenazas o a cuando se traten de ataques contra el Estado Dominicano, la Seguridad Nacional o que involucren la figura del Presidente de la República, Ministros, Secretarios de Estado o funcionarios electos;

CONSIDERANDO: Que este Consejo Directivo no solamente comprende la preocupación de los concesionarios en que se entreguen datos de tráfico, conexión y acceso de sus usuarios a personas que no estén autorizadas a recibirlos, así como entiende la obligación que tienen de salvaguardar dichos datos de acuerdo con preceptos constitucionales y legales;

CONSIDERANDO: Que conforme señalan en sus comentarios se debe establecer un plazo dentro del cual la solicitud por escrito debe ser entregada a los Proveedores de Servicios en el cual se formalice la solicitud, en la manera en que ordena el Reglamento puesto en consulta pública; Es por esta razón que este Consejo Directivo considera optimo otorgar a los Órganos de Investigación un plazo de cuatro (4) horas para remitir la correspondiente solicitud por escrito so pena de que la misma sea desechada por los Proveedores de Servicios; En tal sentido se añadirá al Reglamento que sea aprobado en esta resolución, una aclaración al respecto;

CONSIDERANDO: Que en cuanto a las obligaciones de los propietarios de los Centros de Acceso Público, se expusieron comentarios al Reglamento colocado en consulta pública que se pronunciaban en sentido de que el plazo otorgado para que estos Centros de ajusten a las disposiciones del Reglamento es extremadamente corto, tomando en consideración que dichos centros no disponen de un alto número de personal que se pueda dedicar entendiendo la situación a este tipo de labores, así como que sería necesario que se definan los Criterios de Seguridad de los Centros y Puntos de Acceso Público, según dispone el artículo 21 del mismo Reglamento;

CONSIDERANDO: Que una de las razones fundamentales para elaborar el presente Reglamento ha sido la problemática que representa para los Órganos de Investigación realizar pesquicias en los Centros de Acceso Público, los cuales en su mayoría no cuentan con los dispositivos de seguridad necesarios para salvaguardar los datos requeridos de sus usuarios en caso de que se violen disposiciones legales;

CONSIDERANDO: Que el combate a la ciberdelincuencia es una responsabilidad compartida, que exige una acción coordinada por parte de las autoridades gubernamentales, el sector privado y los ciudadanos. Por lo tanto, esta acción coordinada debe prever desde el desarrollo de un marco jurídico adecuado, que los Órganos de Investigación del Estado cuenten con las herramientas e instrumentos necesarios para investigar estos crímenes y delitos hasta la educación de los usuarios para evitar que se conviertan en víctimas del flagelo de la ciberdelincuencia;

CONSIDERANDO: Que por lo tanto, les corresponderá a los propietarios de los Centros de Acceso Público tomar mayor responsabilidad sobre el tema de la ciberdelincuencia, en la misma forma en que ya lo han hecho los Proveedores de Servicio de manera que adecuen sus Centros a las disposiciones de este Reglamento;

CONSIDERANDO: Que tanto este órgano regulador como el Departamento de Investigación de Crímenes y Delitos de Alta Tecnología de la Policía Nacional (DICAT), se han abocado a asumir los compromisos establecidos en el presente reglamento, definiendo los criterios técnicos de seguridad y las reglas que deban cumplir estos centros, así como de la labor de concientizar a los propietarios y al personal que labora en dichos centros para garantizar el cumplimiento de dichas obligaciones;

CONSIDERANDO: Que, otro de los comentarios recibidos en relación al proyecto de Reglamento que nos ocupa, se refiere a las obligaciones de los propietarios de los Puntos de Acceso Público, señalándose que se ha hecho muy difícil implementar medidas de seguridad que garanticen la autenticidad de los datos personales de los ciudadanos que se conectan a través del Punto de Acceso Público, al igual que la preocupación por el mal uso que pudiese hacer el propietario del Punto de Acceso Público de las informaciones personales suministradas por los usuarios;

CONSIDERANDO: Que, actualmente los Puntos de Acceso Público son una forma de prestación del servicio de acceso a Internet casi obligatorio, en los establecimientos que sirven en distintos lugares donde se reúnen personas para recreación, estudio, u otra actividad en lugares abiertos; que, esto ha contribuido a que en el país existan en innumerables plazas, universidades, aeropuertos, restaurantes, y otros miles de tipos de establecimientos a nivel mundial;

CONSIDERANDO: Que, los Puntos de Acceso Público se han convertido en un servicio adicional que se ofrece al cliente que visita uno de los establecimientos mencionados precedentemente, pero al mismo tiempo son utilizados cada vez más como herramientas publicitarias para llegar a un alto número de usuarios, tanto en manera de folleto, como utilizando las direcciones de correos de las personas que acceden a los mismos para hacer publicidad por correo electrónico; que, para estos fines, los Puntos de Acceso Público necesitan valerse de herramientas auxiliares como los portales cautivos, los cuales obligan al usuario a realizar una autenticación al iniciar cada sesión;

CONSIDERANDO: Que, las informaciones requeridas a los usuarios para autenticarse y acceder a un Punto de Acceso Público, son seleccionadas por los propietarios del servicio, de manera que puedan lograr un balance entre obtener la mayor información del usuario, sin que esto implique una molestia para el mismo, y siempre que éste ofrezca su consentimiento expreso para que dichos datos sean recolectados y se le informe claramente el propósito y tratamiento que se dará a los mismos;

CONSIDERANDO: Que, este órgano regulador entiende que la implementación de las herramientas que permitan la autenticación de los usuarios de Puntos de Acceso Público, para poder cumplir con el Reglamento, no involucran un alto costo de implementación o administración, siempre que los propietarios de los Puntos de Acceso Público sean responsables de mantenerlas disponibles y actualizadas; que, asimismo toda empresa que ofrece un servicio de Internet a sus clientes vía un Punto de Acceso Público debe tener la capacidad de incluir el costo que pueda implicar el mantenimiento de estas herramientas, dentro de las responsabilidades que ya tiene dando mantenimiento a su red y/o servicio de internet, ya sea con su personal interno o contratando los servicios de las prestadoras o empresas de integración de redes del país;

CONSIDERANDO: Que, según se señala en el artículo 21 del Reglamento, el **INDOTEL** publicará, un documento técnico que contenga los requerimientos mínimos con los que debe contar un Punto de Acceso Público para brindar servicio a sus clientes; que, el mismo deberá señalar los mecanismos necesarios para garantizar la información necesaria para que los órganos de investigación puedan llevar a cabo sus funciones cabalmente y al mismo tiempo aseguren la protección de la privacidad de los usuarios de los Puntos de Acceso Público;

CONSIDERANDO: Que según se señala en el artículo 21 del Reglamento el **INDOTEL** publicará, una vez esté aprobado el presente Reglamento, un documento técnico que contenga los requerimientos mínimos con los que debe contar un Punto de Acceso Público para brindar servicio a sus clientes. El cual deberá señalar los mecanismos necesarios para garantizar la información necesaria para que los órganos de investigación puedan llevar a cabo sus funciones cabalmente y al mismo tiempo aseguren la protección de la privacidad de los individuos que hagan uso de dichos servicios;

CONSIDERANDO: Que entre los comentarios presentados por las empresas respecto del artículo 18 del Reglamento en su versión puesta en consulta pública, se encuentran los relativos a la obligación de los Proveedores de Servicio de bloquear páginas en Internet con contenido de material de abuso infantil;

CONSIDERANDO: Que como bien se ha indicado en los comentarios a la propuesta de Reglamento el bloqueo de una página de Internet con contenido de material de abuso infantil, sólo es posible si dicha página es alojada en los servidores del Proveedor de Servicio a quien se hace la solicitud de bloqueo, es decir, una página creada en el servidor de un Proveedor de Servicio no puede ser bloqueada por otro Proveedor de Servicio, so pena de que la acción anterior implicaría el bloqueo de la dirección IP de dicho servidor, lo que afectaría los demás usuarios que están alojados en esta dirección haciendo uso de dicho servidor de una forma transparente y legal;

CONSIDERANDO: Que conforme el artículo 49 de la Constitución de la República, en la cual se reconoce el derecho a la libertad de expresión de los individuos, en el cual se establece que *toda persona tiene derecho a expresar libremente sus pensamientos, ideas y opiniones, por cualquier medio, sin que pueda establecerse censura previa*;

CONSIDERANDO: Que un aspecto que debe considerarse sobre la libertad de expresión son los límites que debe tener el ejercicio de la misma. El ejercicio de los derechos fundamentales no es ilimitado. La concurrencia de un derecho con otros igualmente reconocidos como fundamentales, exige la armonización en la coexistencia de estos derechos. En este sentido, un derecho fundamental debe ceder ante otro cuando afecte más al individuo o a la comunidad. "*Cuando concurren dos derechos fundamentales a de compaginarse su ejercicio teniendo en*

cuenta una cualidad atribuida por igual a todos los derechos subjetivos: su elasticidad. Dos derechos concurrentes son susceptibles de comprimirse recíprocamente, sin llegar a anularse (…) [la comprensión de un derecho fundamental en unos casos puede ser mayor para un derecho o mayor para otro derecho], *determinar estos casos, en función de las naturalezas conjugadas de los derechos concurrentes, constituye la proyección del principio de excepcionalidad*"[1]. A este efecto, en el ámbito *ius* informativo existen ciertas excepciones: los derechos personales y el interés general de la sociedad;

CONSIDERANDO: Que el concepto de Sociedad de la Información alude *a un nuevo tipo de sociedad, una nueva era en el proceso evolutivo del hombre, donde la información constituye el elemento determinante en el desarrollo y desenvolvimiento social y humano. (…) En este reciente y dinámico contexto (…) localizamos como caracteres esenciales la bidireccionalidad de la información y la generalizada expansión de las tecnologías que permiten su tratamiento. De este modo, nos enfrentamos a un mundo donde todo interactúa y se retroalimenta, en el que la información cada vez emana de un número mayor de fuentes y se dirige a un público más amplio y diverso*[2];

CONSIDERANDO: Que el medio paradigmático de la Sociedad de la Información es el Internet[3], que evidencia el carácter global de la Sociedad de la Información. En el medio del Internet existe la comunicación masiva de todo tipo de mensajes con un carácter multidireccional y sin control;

CONSIDERANDO: Que uno de los aspectos que tiene que regularse en la Sociedad de la Información es el contenido que circula, especialmente en Internet por su difusión mundial. En este sentido, "*Las discusiones sobre contenido usualmente se enfocan en tres grupos. El primer grupo es el contenido que cuenta con consenso global para su control. Se incluye aquí la pornografía infantil y algunos temas como la justificación del genocidio y el incitamiento u organización de actos terroristas (…). El segundo grupo es el contenido que podría ser de carácter delicado para países, regiones o grupos étnicos en particular debido a sus valores religiosos y culturales específicos. (…) El tercer grupo se refiere al contenido que podría generar susceptibilidad política e ideológica. En esencia, esto se refiere a la censura en Internet*"[4];

CONSIDERANDO: Que el control de contenido en Internet supone restricción a la libertad de expresión y al derecho a la información[5]. La proliferación de páginas web, blogs, listas de correos y foros de discusión hace aún más diverso el contenido en Internet. Pero ese contenido puede ser lesivo para otros derechos fundamentales (como el derecho a la intimidad, al honor y a la propia imagen, a la dignidad humana, entre otros) y para el interés general de la sociedad

---

[1] Desantes Guanter, José María. La Información como Derecho, Editora Nacional, Madrid, España, 1974, p. 66.

[2] López Zamora, Paula. *Nuevas perspectivas del derecho a la información en la Sociedad de la Información*, Revista de Derecho y Tecnología, Centro de Investigaciones Jurídicas y Políticas, Universidad Católica del Táchira, No. 6-7, enero-diciembre 2005, Táchira, Venezuela, p. 12. Desantes Guanter, José María; Soria, Carlos. *Los Límites de la Información*…, cit., p. 15.

[3] Hay otros medios que hacen posible la Sociedad de la Información como las comunicaciones móviles, pero indudablemente es el Internet el que ha conformado el elemento principal de sustento y desarrollo de este nuevo contexto social.

[4] Kurbalija, Jovan; Gelbstein, Eduardo. *Gobernanza de Internet: asuntos, actores y brechas*, Traducción de Ana María Piza, DiploFoundation y la Sociedad para el Conocimiento Mundial, Malta, 2005, pp. 135-136.

[5] Idem, p. 139.

(apología del terrorismo, racismo, xenofobismo, entre otros), por lo que es comprensible que se establezcan restricciones para el acceso a ciertos contenidos en Internet;

CONSIDERANDO: Que nuestra Constitución, no ajena a esta línea de pensamiento, estableció como límites a la libertad de expresión el respeto al derecho al honor, a la intimidad, así como a la dignidad y la moral de las personas, en especial la protección de la juventud y de la infancia, de conformidad con la ley y el orden público;

CONSIDERANDO: Que no ha sido la intención detrás de esta propuesta de reglamento el bloquear páginas de internet que no estén alojadas en los servidores del Proveedor de Servicio al que se le notifica el contenido de material de abuso infantil o que puedan afectar el derecho a la libertad de expresión o el derecho a la información de los individuos. En consecuencia el Reglamento será modificado en este sentido, para brindar mayor claridad sobre este punto;

CONSIDERANDO: Que varias de las concesionarias que han realizado comentarios respecto del reglamento en proceso de consulta pública han externado su opinión respecto del plazo para la entrada en vigencia del reglamento, oscilando dichas opiniones en que el mismo debe entrar en vigencia en un período desde 6 a 12 meses;

CONSIDERANDO: Que el Consejo Directivo, luego de haber evaluado la observación planteada, entiende pertinente lo sugerido, por lo que modificará el Reglamento que será aprobado con esta resolución extendiendo un plazo adecuado para la entrada en vigencia del mismo;

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, de fecha 23 de abril de 2007;

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;

VISTA: La Resolución No. 056-09, dictada por el Consejo Directivo del **INDOTEL** en fecha 29 de junio de 2009, que ordenó 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**;

VISTOS: Los escritos depositados por las concesionarias **ONEMAX, VIVA, CLARO, ORANGE** y **TRICOM** con motivo de su participación en el proceso de Consulta Pública dispuesto por la Resolución del Consejo Directivo No. 056-09;

OIDOS: Los representante autorizados de la **ONEMAX, VIVA, CLARO, ORANGE** y **TRICOM** durante la audiencia pública celebrada en fecha 26 de octubre de 2005;

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

RESUELVE:

PRIMERO: ACOGER parcialmente, los comentarios presentados por las prestadoras de servicios públicos de telecomunicaciones **ONEMAX, VIVA, CLARO, ORANGE** y **TRICOM**, con ocasión del proceso de Consulta Pública iniciado mediante la Resolución No. 056-09 de este Consejo Directivo, para aprobar 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**; **DISPONIENDO** la integración de todos los cambios señalados en el cuerpo de la presente resolución en la versión definitiva del **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** que se apruebe mediante este documento.

SEGUNDO: APROBAR 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 íntegro se transcribe a continuación:

"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 No. 53-07 contra Crímenes y Delitos de Alta Tecnología, las expresiones y términos que se emplean en este Reglamento tendrán el significado que se señala a continuación:

1.1 **Centro de Acceso Público:** es cualquier establecimiento que ofrezca servicios 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; y donde además puede hacerse uso de aplicaciones de oficina, editores de imágenes y utilidades de software.

1.2 **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.

1.3 **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.

1.4 **Material de Abuso Infantil:** Significa todo material que represente o describa: (a) agresiones sexuales en contra de una persona que es, parece ser o se presume que sea un niño, niña o adolescente; (b) una persona que es, parece ser o se presume que sea un niño, niña o adolescente, realizando o que parezca que realiza una pose o actividad sexual solo o en presencia de otra persona; o (c) tortura o actos de barbarie en contra de una persona que es, parece ser o se presume que sea un niño, niña o adolescente;

1.5 **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, tales como la Policía Nacional y su Departamento de Investigación de Crímenes y Delitos de Alta Tecnología (DICAT), entre otros.

1.6. **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 título 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.

1.7. **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.

1.8 **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.

1.9. **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;

1.10. **Urgencia:** 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, Ministros, Secretarios de Estado o funcionarios electos.

Artículo 2.- Alcance e interpretación

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, así como establecer el régimen de obligaciones de los Proveedores de Servicios y de los propietarios de los Puntos y Centros de Acceso Público para el bloqueo de material de abuso infantil en sus respectivas redes y sistemas.

2.2 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.

Artículo 3.- 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, cuando el número de destino sea dentro de la misma red.

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

            i) La identificación de usuario y/o facilidad asignada;

            ii) La identificación de usuario y/o facilidad 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 y/o facilidad 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, cuando el número de destino sea dentro de la misma red.

        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 (IP), ya sea dinámica o estática, asignada por el Proveedor de Servicios, así como la identificación del 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;

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 éstos, 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 sean conservados por un período de tiempo que no será inferior a noventa (90) días, 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 para 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, 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 costos e 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 y las reglamentaciones correspondientes, mediante el cumplimiento de las obligaciones puestas a su cargo en el presente Reglamento;

b) Notificar a los Órganos de Investigación de los casos que afecten a cualquier Proveedor de Servicios de los cuales tengan conocimiento;

c) Asistir a los Órganos de Investigación, de conformidad con la disponibilidad de los Proveedores de Servicios, 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) 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;

l) 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;

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

n) 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 para identificar las fortalezas y debilidades de dicho procedimiento.

s) Cumplir con las obligaciones establecidas en el Título III del presente reglamento, referente al bloqueo de contenido de páginas en internet con contenido de material de abuso infantil

CAPITULO II

SOLICITUDES, DOMICILIOS, PROCEDIMIENTOS Y PLAZOS

Artículo 9.- Solicitudes

1. Todas las Solicitudes de Datos 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 de Datos 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, entregada 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, República 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 calendario previos al cambio de dicha dirección.

Artículo 12.- Procedimiento para la remisión de Solicitudes de Datos 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 y del Punto de Contacto de los Órganos de Investigación, 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, Ministros, 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 coordinación con el Departamento de Investigación de Crímenes y Delitos de Alta Tecnología (DICAT) de la Policía Nacional.

3. Para todos 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 y del Punto de Contacto de los Órganos de Investigación, 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 de Datos 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 en un plazo máximo de 4 horas so

pena de ser desechada por los Proveedores de Servicios.

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

   a) Toda 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 la necesidad en base a los supuestos definidos en el presente Reglamento;

   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.

3. En cuanto a su contenido, las Solicitudes de Datos 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 Datos de los Órganos de Investigación

1. Todo Proveedor de Servicios que sea destinatario de una Solicitud de Datos 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 o indicada por el Órgano de Investigación para remitir la Solicitud de Datos, 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 de Datos; 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 de Datos 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 de Datos deberá responder a dicha solicitud en los 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 Datos de los Órganos de Investigación en un plazo máximo de cinco (5) días laborales.

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 de Datos 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 MATERIAL DE ABUSO INFANTIL

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, 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 material de abuso infantil;

c) Implementar mecanismos de seguridad como programas y aplicaciones que impidan el acceso a páginas y similares con contenido de material de abuso infantil;

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 un (1) año 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 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 cuando 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, de páginas de Internet que fueron visitadas, así como cuánto tiempo permanecieron en ellas. Este registro debe incluir la dirección MAC, la dirección de Protocolo de Internet (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 material de abuso infantil;

e) Implementar mecanismos de seguridad como programas y aplicaciones que impidan el acceso a páginas y similares con contenido de material de abuso infantil.

2. Los propietarios de los Puntos de Acceso Público tendrán un plazo de un (1) año, 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 Internet con contenido de material de abuso infantil

Los Proveedores de Servicio tendrán la obligación de proceder a realizar el bloqueo de páginas en Internet con contenido de material de abuso infantil siempre que se encuentre creada en sus redes y en la medida en que sean debidamente notificados por parte del Ministerio Público.

Artículo 19.- Criterios para la evaluación y clasificación del contenido de páginas en Internet para ser considerado de material de abuso infantil

1. Al momento de que el Ministerio Público tenga conocimiento de la existencia de una página en Internet con contenido de material de abuso infantil deberá hacer uso de los siguientes criterios para poder determinar si procede emitir una solicitud de bloqueo a los Proveedores de Servicio:

    a) Las definiciones y conceptos establecidos en el artículo 1 del presente Reglamento, en particular la referente a Material de Abuso 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 destino para el acceso a Material de Abuso Infantil o de agresión y/o abuso en contra de niños, niñas y adolescentes;

2. Para aplicar los criterios descritos anteriormente, el Ministerio Público deberá 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 sólo 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, las obligaciones establecidas y medidas establecidas por el artículo 8 y la obligación de bloquear páginas en Internet con contenido de Material de Abuso Infantil, 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 a los seis (6) meses desde la fecha de su publicación en un periódico de circulación nacional.

TERCERO: Instruir a la Directora Ejecutiva del **INDOTEL** para que en cumplimiento de los dispuesto por el artículo 21 del **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** convoque al Departamento de Investigación de Crímenes y Delitos de Alta Tecnología de la Policía Nacional (DICAT), para elaborar el correspondiente instructivo sobre los criterios técnicos de seguridad que deban cumplir los Centros y Puntos de Acceso Públicos.

CUARTO: DISPONER que la presente Resolución sea publicada en un periódico de amplia circulación nacional, en el Boletín Oficial del **INDOTEL** y en la página que el **INDOTEL** mantiene en la Internet.

Así ha sido aprobada y firmada la presente Resolución por unanimidad de votos del 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 primero (1ro) del mes de septiembre del año dos mil once (2011).

Firmados:

David A. Pérez Taveras
Secretario de Estado,
Presidente del Consejo Directivo

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

Leonel Melo Guerrero
Miembro del Consejo Directivo

Domingo Tavárez
Miembro del Consejo Directivo

Juan Antonio Delgado
Miembro del Consejo Directivo

Joelle Exarhakos Casasnovas
Directora Ejecutiva
Secretaria del Consejo Directivo