INSTITUTO DOMINICANO DE LAS TELECOMUNICACIONES (INDOTEL)

RESOLUCIÓN No. 055-06

QUE APRUEBA LA NORMA COMPLEMENTARIA DE LA LEY 126-02 SOBRE PROTECCIÓN DE DATOS DE CARÁCTER PERSONAL POR LOS SUJETOS REGULADOS.

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 dispuesto por este Consejo Directivo mediante su Resolución No. 077-05, de fecha 23 de junio de 2005, para dictar las Normas Complementarias de la Ley 126-02 sobre Comercio Electrónico, Documentos y Firmas Digitales.

Antecedentes.-

1. La Ley No. 126-02 sobre Comercio Electrónico, Documentos y Firmas Digitales, promulgada el 4 de septiembre de 2002, así como su Reglamento de Aplicación aprobado por el Decreto No. 335-03, de 8 de abril de 2003 y las Normas Complementarias aprobadas en desarrollo de éstos, constituyen el marco legal por el que se regulan las actividades de prestación de servicios de los Sujetos Regulados respecto del Comercio Electrónico, Documentos y Firmas Digitales;

2. El Consejo Directivo del **INDOTEL** aprobó, mediante su Resolución No. 42-03, de fecha 17 de marzo de 2003, juntamente con el Reglamento de Aplicación de la Ley de Comercio Electrónico, Documentos y Firmas Digitales, la propuesta de **Agenda Regulatoria**, que entró en vigencia una vez que el Poder Ejecutivo promulgó el precitado Reglamento de Aplicación de la Ley No. 126-02, en la que fueron contempladas las "Normas Complementarias" de la Ley de Comercio Electrónico;

3. Dentro de la citada **Agenda Regulatoria** fue prevista la **"Norma sobre Protección de Datos de Carácter Personal por los Sujetos Regulados"**, con el objeto de respetar la obligación impuesta en el artículo 40, inciso c) de la Ley No. 126-02, el cual dispone que las entidades de certificación están obligadas a garantizar la protección, confidencialidad y debido uso de la información suministrada por el suscriptor; teniendo en consideración que la República Dominicana aún no cuenta con normas de alcance general referidas a la protección de datos personales, y que el Reglamento de Aplicación de dicha Ley, en su artículo 21, inciso "c", faculta al **INDOTEL** a dictar las normas relativas a la protección de los datos personales de los suscriptores, a ser aplicadas por las entidades de certificación y las unidades de registro;

4. En fecha 23 de junio de 2005, el Consejo Directivo del **INDOTEL** adoptó la Resolución No. 077-05, que ordenó el inicio del proceso de Consulta Pública para dictar las Normas Complementarias de la Ley 126-02, sobre Comercio Electrónico, Documentos y Firmas Digitales, cuyo dispositivo reza textualmente:

> "**PRIMERO: ORDENAR** el inicio del proceso de consulta pública para la aprobación de las "Normas Complementarias" de la Ley No. 126-02, sobre Comercio Electrónico,

Documentos y Firmas Digitales, de fecha 4 de septiembre de 2002, cuyos textos se encuentran anexo a la presente resolución, formando parte integral de la misma, que se describen a continuación:

a) Norma sobre Protección de los Derechos de los Consumidores y Usuarios;
b) Norma sobre Protección de Datos de Carácter Personal por los Sujetos Regulados;
c) Norma sobre Publicidad y Difusión de Información de los Consumidores y Usuarios por los Sujetos Regulados;
d) Norma de Aplicación de la Ley No. 126-02 a los Procedimientos Aduaneros;
e) Norma sobre Medios de Pagos Electrónicos;
f) Norma de Aplicación de la Ley No. 126-02 a Derechos Reales sobre Bienes Inmuebles; y,
g) Norma sobre la Determinación de la Hora Oficial en Medios Electrónicos e Internet.

SEGUNDO: ORDENAR al **Director Ejecutivo Interino** la publicación en un periódico de amplia circulación nacional de esta resolución y de los proyectos de **"Normas Complementarias"** de la Ley No. 126-02, sobre Comercio Electrónico, Documentos y Firmas Digitales de fecha 4 de septiembre de 2002, sometidas a consulta pública, que conforman su anexo, previamente citados en el ordinal "Primero" que antecede. Dispone, de igual modo, que a partir de la referida publicación antes descrita todos los documentos que conforman las "Normas Complementarias" de la Ley No. 126-02, sobre Comercio Electrónico, Documentos y Firmas Digitales propuestas estarán a disposición de los interesados en las oficinas del **INDOTEL**, ubicadas en la primera planta del Edificio Osiris, situado en la Ave. Abraham Lincoln No. 962 de esta ciudad de Santo Domingo de Guzmán, Distrito Nacional, Capital de la República Dominicana, así como en la página web que mantiene esta institución en la red de Internet, en la dirección www.indotel.gov.do.

TERCERO: FIJAR un plazo de treinta (30) días calendario, contados a partir de la fecha de la publicación de la presente Resolución, en un periódico de amplia circulación nacional, para que los interesados presenten las observaciones y comentarios que estimen convenientes a los proyectos de las Normas Complementarias de la Ley No. 126-02, sobre Comercio Electrónico, Documentos y Firmas Digitales, que conforma el anexo de esta Resolución.

PARRAFO I: Los comentarios y las observaciones a los que hace referencia el presente artículo deberán ser depositados en formato físico y en formato electrónico, redactados en idioma español, dentro del plazo anteriormente establecido, en un (1) original y cinco (5) copias, dirigidos al **Instituto Dominicano de las Telecomunicaciones (INDOTEL),** Edificio Osiris, Avenida Abraham Lincoln número 962, Santo Domingo de Guzmán, Distrito Nacional, Capital de la República Dominicana, de lunes a viernes, en horario de 8:30 A.M. a 5:00 P.M.

PARRAFO II: Vencido el plazo de treinta (30) días establecido en el presente ordinal no se recibirán más observaciones ni se concederán prórrogas a los interesados para depositar otros escritos."

5. La Resolución No. 077-05, cuyo dispositivo ha sido copiado precedentemente, fue publicada en fecha 20 de julio de 2005 en el periódico "Hoy" 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;

6. En fecha 2 de septiembre de 2005, la empresa **VERIZON DOMINICANA, C. POR A.**, depositó por ante este órgano regulador sus comentarios a la citada Resolución;

7. En fecha 26 de octubre de 2005, el Consejo Directivo de **INDOTEL** celebró la Audiencia Pública de la Resolución No. 077-05, en el domicilio de la institución, ejerciendo su derecho

de participación en la misma los representantes acreditados de la empresa **VERIZON DOMINICANA, C. POR A.**

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

CONSIDERANDO: Que de acuerdo al artículo 2.2 del Reglamento de Aplicación de la Ley No. 126-02, se consideran como Sujetos Regulados por la Ley No. 126-02, su Reglamento de Aplicación y las Normas Complementarias que dicte el Instituto Dominicano de Telecomunicaciones (**INDOTEL**) "*las entidades de certificación, los proveedores de servicios de firma electrónica y las unidades de registro, así como los proveedores de servicios o infraestructura de soporte operacionalmente vinculados con estas en la medida de su relación contractual*";

CONSIDERANDO: Que en virtud de los artículos 56 de la Ley No. 126-02 y 39 y 43 del Reglamento de Aplicación de la Ley No. 126-02, el **INDOTEL** será el órgano rector y regulador de las actividades realizadas por los Sujetos Regulados en lo que respecta a Comercio Electrónico, Documentos y Firmas Digitales;

CONSIDERANDO: Que el artículo 40, c) de la Ley No. 126-02 establece la obligación de las Entidades de Certificación de "*Garantizar la protección, confidencialidad y debido uso de la información suministrada por el Suscriptor*";

CONSIDERANDO: Que el artículo 9.6, literal e) del Reglamento de Aplicación de la Ley No. 126-02, al tratar sobre el contenido de las disposiciones que deberán contener las Prácticas de Certificación de las Entidades de Certificación, incluye, entre otros, la "*Política de Protección de Datos Personales, acorde con la normativa complementaria a ser dictada por **INDOTEL**"*;

CONSIDERANDO: Que el artículo 21, literal c) del Reglamento de Aplicación de la Ley No. 126-02, prevé que las Entidades de Certificación están obligadas al cumplimiento, entre otras, de las Normas Complementarias que dicte el **INDOTEL** en relación con la "*protección de los datos personales de los Suscriptores de los Certificados*";

CONSIDERANDO: Que el artículo 27.3, literal d) del indicado Reglamento de Aplicación de la Ley No. 126-02, establece que a las Unidades de Registro se les aplicarán las mismas obligaciones que a las Entidades de Certificación en materia de "*Protección de datos personales*";

CONSIDERANDO: Que el artículo 43, literal p) del mismo Reglamento antes señalado indica que el **INDOTEL** tendrá la función de "*velar por el correcto manejo y mantenimiento de la confidencialidad, por parte de los sujetos regulados, de las informaciones de los suscriptores*";

CONSIDERANDO: Que los Datos de Carácter Personal comprenden aquella información concerniente a una persona física, la cual puede ser identificada o es identificable en vista de dicha información;

CONSIDERANDO: Que las relaciones entre los Sujetos Regulados y los Consumidores y Usuarios de los servicios que éstos prestan, precisan en muchos casos del tratamiento de información concerniente a dichos Consumidores y Usuarios y que dicha información puede incluir Datos de Carácter Personal;

CONSIDERANDO: Que en la actualidad, la República Dominicana no cuenta con una norma que establezca de forma general un régimen regulador del tratamiento de los Datos de Carácter Personal;

CONSIDERANDO: Que el conocimiento y tratamiento, sin un marco legal que lo regule, de los Datos de Carácter Personal de los Consumidores y Usuarios de los servicios prestados por los Sujetos Regulados, podría lesionar derechos fundamentales de tales Consumidores y Usuarios, en particular, su derecho a la intimidad;

CONSIDERANDO: Que son numerosos los países del panorama internacional que cuentan con normas reguladoras del tratamiento de Datos de Carácter Personal;

CONSIDERANDO: Que, por su propia naturaleza, las transacciones efectuadas a través del Comercio Electrónico y mediante Documentos y Firmas Digitales, tienen un elevado potencial de favorecer el intercambio de bienes y servicios a nivel internacional;

CONSIDERANDO: Que la inexistencia de un marco normativo en la República Dominicana que regule el tratamiento de Datos de Carácter Personal por los Sujetos Regulados, podría ir en detrimento de la capacidad de este país para poder realizar transacciones electrónicas con países que si cuentan con tal normativa;

CONSIDERANDO: Que, en virtud de todo lo anteriormente indicado, se hace necesario que el **INDOTEL** instrumente una norma tendente a regular el tratamiento de los Datos de Carácter Personal de los Consumidores y Usuarios tratados por los Sujetos Regulados, debiéndose articular dicha norma atendiendo a la especialidad del sector del Comercio Electrónico, Documentos y Firmas Digitales, así como a las tendencias normativas sobre esta materia a nivel internacional;

CONSIDERANDO: Que la protección de Datos de Carácter Personal requiere que se garanticen una serie de principios y facultades que se refieren a la calidad, licitud, legitimidad y seguridad de los Datos de Carácter Personal objeto de tratamiento;

CONSIDERANDO: Que la calidad de los Datos de Carácter Personal implica que los mismos sean correctos, exactos, actualizados, necesarios, pertinentes y que sean conservados únicamente en tanto en cuanto se mantenga la finalidad del tratamiento para el cual fueron recabados;

CONSIDERANDO: Que la licitud del tratamiento consiste en que los Datos de Carácter Personal no sean recogidos por medios fraudulentos, desleales o ilícitos y que tal tratamiento no tenga como resultado una lesión en los derechos de los Consumidores y Usuarios, siendo necesario que dicha recogida sea conforme a lo establecido en las disposiciones jurídicas aplicables y que el tratamiento sea justo;

CONSIDERANDO: Que la legitimidad que precisa el tratamiento de los Datos de Carácter Personal requiere, salvo en supuestos excepcionales especialmente previstos en las normas jurídicas de aplicación, el otorgamiento del consentimiento de los Consumidores y Usuarios (como titulares de los Datos de Carácter Personal), para que se efectúe dicho tratamiento, el cual deberá tener una finalidad determinada, específica y explícita. Este consentimiento deberá ser libre, informado, previo, inequívoco y para ciertos casos, como para ciertos Datos de Carácter Personal especialmente sensibles y que precisan protección específica, expreso y por escrito;

CONSIDERANDO: Que para los Sujetos Regulados obtener el consentimiento de los Consumidores y Usuarios y así legitimar el tratamiento de sus Datos de Carácter Personal, es necesario que dichos Sujetos Regulados proporcionen a los titulares de los Datos de

Carácter Personal información detallada acerca de la identidad del Sujeto Regulado y características del tratamiento previsto;

CONSIDERANDO: Que la seguridad que debe primar en el tratamiento de los Datos de Carácter Personal se refiere a la obligación de los Sujetos Regulados de adoptar las medidas técnicas y organizativas necesarias para garantizar la seguridad de los Datos de Carácter Personal que traten, atendiendo a los riesgos que podrían padecer dichos Datos respecto a su pérdida total, parcial, modificación o acceso no autorizado;

CONSIDERANDO: Que en aras de garantizar la seguridad de los Datos de Carácter Personal de los Consumidores y Usuarios, es necesario la implementación de medidas de seguridad acordes al tipo de Datos de Carácter Personal que se traten y que dichas medidas deben ser más seguras cuanto mayor sea la sensibilidad de los Datos de Carácter Personal a tratar;

CONSIDERANDO: Que en aras de preservar la intimidad de los Consumidores y Usuarios se hace necesario el establecimiento de la obligación de secreto o confidencialidad de los Sujetos Regulados respecto a los Datos de Carácter Personal que estos traten, procurándose que dichos Datos no sean comunicados o revelados a terceras personas, a menos que una norma jurídica establezca lo contrario para casos excepcionales;

CONSIDERANDO: Que la revelación o Comunicación de Datos de Carácter Personal por un Sujeto Regulado a un tercero, supone una alteración de las condiciones de seguridad y secreto que se prevén para el tratamiento de Datos de Carácter Personal y, en consecuencia, puede lesionar los derechos de los Consumidores y Usuarios y que, por ello y salvo en supuestos excepcionales expresamente previstos en la normativa aplicable, tales Comunicaciones de Datos de Carácter Personal deben ser previamente consentidas por los Consumidores y Usuarios titulares de esos Datos de Carácter Personal, habiendo sido previamente informados éstos de la finalidad y destinatario de tal Comunicación;

CONSIDERANDO: Que entre los supuestos en los que, a pesar de existir un acceso por un tercero a Datos de Carácter Personal, no resulta aplicable el régimen general de las Comunicaciones de Datos de Carácter Personal, se encuentra el régimen de acceso por terceros (o Encargados del Tratamiento) a los Datos de Carácter Personal, al objeto de prestar un servicio al Sujeto Regulado responsable de dichos Datos y realizar un tratamiento de datos por cuenta de tal Sujeto Regulado. En tal contexto, mientras el Encargado del Tratamiento no realice tratamientos por su cuenta sino únicamente por cuenta del Sujeto Regulado responsable, no serán de aplicación los requisitos previstos para las Comunicaciones de Datos de Carácter Personal; que no obstante, la actividad del Encargado del Tratamiento deberá estar regulada en un contrato que determine y limite claramente los tratamientos a realizar por éste, debiendo ser efectuados tales tratamientos siempre por cuenta del Sujeto Regulado responsable;

CONSIDERANDO: Que las transferencias internacionales o movimientos de Datos de Carácter Personal fuera de la República Dominicana suponen que el tratamiento de los Datos de Carácter Personal se ubique en un territorio al cual no alcanzan las medidas protectoras de este país, en lo que respecta al tratamiento de dichos Datos, lo que podría atentar contra los derechos de los Consumidores y Usuarios titulares de los mismos, por lo que tales transferencias internacionales precisarán del previo consentimiento de esos Consumidores y Usuarios, salvo en los supuestos específicamente previstos en la normativa aplicable;

CONSIDERANDO: Que entre los supuestos de transferencia internacional que se exceptúan del requisito de consentimiento previo del Consumidor o Usuario titular de los Datos de Carácter Personal, reviste especial relevancia aquel en el que la transferencia

internacional tenga un destinatario que posea un nivel de protección adecuado, lo que se producirá cuando dicho destinatario: (i) esté situado en un Estado que posea y aplique normas jurídicas cuyo contenido sea suficiente para garantizar la protección de los Datos de Carácter Personal que se vayan a tratar, o (ii) se comprometa contractualmente frente al Sujeto Regulado que realice la transferencia internacional y al **INDOTEL**, a tratar los Datos de Carácter Personal conforme a lo dispuesto en la normativa de la República Dominicana aplicable, y reconozca contractualmente al **INDOTEL** facultad para penalizar el incumplimiento de esta obligación en un importe igual al aplicable como sanción bajo dicha normativa;

CONSIDERANDO: Que los Consumidores y Usuarios cuyos Datos de Carácter Personal se tratan por los Sujetos Regulados, deben tener derecho a acceder a los Datos de Carácter Personal tratados y obtener información sobre las circunstancias en las que se desarrolla el tratamiento, a rectificarlos cuando sean incorrectos o inexactos y a cancelarlos, impidiendo el tratamiento por el Sujeto Regulado;

CONSIDERANDO: Que el **INDOTEL** cuenta con un poder de inspección y sanción frente a los Sujetos Regulados, pudiendo, en consecuencia, sancionarlos cuando estos lesionen los derechos de los Consumidores y Usuarios respecto al tratamiento de sus Datos de Carácter Personal;

CONSIDERANDO: Que entre los comentarios presentados por la empresa **VERIZON DOMINICANA, C. POR A.** respecto de la Norma Complementaria de la Ley No. 126-02 sobre Protección de Datos de Carácter Personal por los Sujetos Regulados, en su versión puesta en consulta pública, se encuentra el siguiente:

> *"**Responsabilidad del Estado.** Un tema que no ha sido incluido expresamente en las normas y que debería de ser objeto de un procedimiento y normativa separada, es el de los supuestos en que el Estado, justificado en fines públicos, como el de la investigación de los delitos, persiga información personal de presuntos infractores, a fin de realizar pesquisas electrónicas mediante comparación de grandes cantidades de datos o mediante la reunificación de datos que han sido entregados a distintas organizaciones públicas y privadas con otros fines distintos a los de la investigación criminal.*
>
> *En éste como en otros supuestos, debe exigirse la existencia de una normativa específica, que además de ser clara establezca como límite el principio de proporcionalidad a fin de que en cada caso en que esté en peligro el derecho a la autodeterminación informativa, aún cuando el Estado alegue estos intereses públicos, se demuestre que esa comparación de datos o el procesamiento en concreto sea el único medio idóneo y racional para alcanzar los fines propuestos, de manera que no burle la expectativa del consumidor o usuario de que el Estado tendrá también límites en su actividad investigativa."*

CONSIDERANDO: Que si bien es cierto que es responsabilidad del Estado contar con una normativa que regule lo relativo al tratamiento de Datos de Carácter Personal por parte del Estado, no es menos cierto que el tema aludido en el comentario de **VERIZON DOMINICANA, C. POR A.** excede del alcance de la Norma Complementaria que nos ocupa, que se limita al tratamiento de Datos de Carácter Personal por los Sujetos Regulados;

CONSIDERANDO: Que **VERIZON DOMINICANA, C. POR A.** expuso también en sus comentarios, lo siguiente:

> *"**Transferencias internacionales de datos.** La norma debe establecer también cierta restricción a la transmisión de los datos personales desde países o con destino a países cuya legislación no ofrezca garantías análogas a las previstas en esta disposición, exceptuando las transferencias internacionales de créditos, las transferencias de información para los efectos de prestar colaboración a las autoridades judiciales y policiales internacionales, la transferencia por autorización del usuario o consumidor, así como cualquier otra transferencia que resulte de la aplicación de tratados o convenios internacionales en que el estado de República Dominicana sea parte."*

CONSIDERANDO: Que en el Derecho comparado internacional, la regulación de las transferencias internacionales de datos se apoya en la idea de evitar movimientos de Datos de Carácter Personal con destino a países que no otorguen un nivel de protección equiparable al que se otorga en el Derecho local aplicable; que luego de la aprobación de la Norma Complementaria, la Republica Dominicana contará con un marco regulador del tratamiento de Datos de Carácter Personal, al menos, en lo que respecta a los Sujetos Regulados; que en tal virtud, este Consejo Directivo estima apropiado incluir ciertas restricciones para el movimiento de Datos de Carácter Personal fuera de la República Dominicana, si bien dichas restricciones deberán, por razones evidentes de competencia, ceñirse exclusivamente a los Datos de Carácter Personal tratados por Sujetos Regulados; que, en consecuencia, *la Norma Complementaria que será aprobada de manera definitiva mediante esta resolución será modificada respecto de la versión puesta en consulta pública, de acuerdo con lo arriba expuesto*;

CONSIDERANDO: Que **VERIZON DOMINICANA, C. POR A.** planteó también, en sus comentarios a la Resolución No. 077-05, lo siguiente:

> *"**Recogida de datos.** Consideramos que la calificación de "inequívoco" en los artículos 4 y 6, debe ser eliminada pues la misma es interpretativa, además de que entendemos es suficiente con que se requiera una comunicación "expresa" y "precisa"."*

CONSIDERANDO: Que los artículos referidos en el comentario de **VERIZON DOMINICANA, C. POR A.,** establecen las informaciones que deberán suministrar a los Interesados los Sujetos Regulados cuando les soliciten Datos de Carácter Personal (Art. 4) así como la necesidad de consentimiento previo de aquellos, para el tratamiento de dichos Datos por parte de los sujetos Regulados (Art. 6); que cuando una empresa decide recabar datos de carácter personal debe, para poder utilizarlos, obtener el consentimiento de la persona que los cede; que ese consentimiento no se basa en el simple otorgamiento de la información, sino en que los Interesados sean conscientes de que sus datos serán tratados y las finalidades a las que van a ser destinados. Por ello, es importante que se suministre al Interesado información que no ofrezca dudas ni posible equivocación, y asimismo, que la persona que de sus datos personales consienta su tratamiento de manera que no admita duda o equivocación; que el término "inequívoco" es común en este tipo de normas, en los países que cuentan con normativa de protección de Datos de Carácter Personal; que, en virtud de todo lo antes indicado, es importante a juicio de este Consejo Directivo que el término "inequívoco" se mantenga en los artículos 4 y 6 de la Norma que será aprobada mediante la presente resolución;

CONSIDERANDO: Que **VERIZON DOMINICANA, C. POR A.** expuso en sus comentarios, lo siguiente:

*"**Recogida de datos de terceros.** El supuesto del artículo 5 parece no tener sentido. ¿En qué caso se obtiene información de Interesados que no haya sido suministrada por ellos o con su autorización? En caso de que el Sujeto Regulado reciba esa información de manos de terceros, ¿su obligación es frente al Interesado o frente a esos terceros? Consideramos que el Sujeto Regulado no debe tener mayor obligación que la puesta a su cargo en el caso de remisión de información no solicitada."*

CONSIDERANDO: Que el supuesto previsto en el artículo 5 de la Norma Complementaria, se refiere precisamente a aquellos supuestos en los que el Sujeto Regulado obtiene información de fuentes terceras (distintas del Interesado) como, por ejemplo, al proporcionarlos un tercero u obtenerlos de una fuente accesible al publico; que en estos supuestos, independientemente de que los Interesados no le hayan proporcionado la información al Sujeto Regulado - o, incluso, con más intensidad precisamente por ello - los Interesados tienen derecho a ser informados de la existencia de un tratamiento de datos realizado por tal Sujeto Regulado, todo ello en los términos previstos actualmente en la Norma Complementaria; que sólo de esta forma podría garantizarse plenamente el derecho a la autodeterminación informativa de los Interesados (Ej. Derecho de cancelación, rectificación, etc.); por lo cual el artículo comentado será mantenido en el texto de la Norma que será aprobada en el dispositivo de esta resolución;

CONSIDERANDO: Que entre los comentarios de **VERIZON DOMINICANA, C. POR A.** se encuentra también el siguiente:

*"**Consentimiento.** La calificación que hace el párrafo 7.1 (a) es a nuestro juicio subjetiva e interpretable por lo que debe eliminarse. Nos preguntamos, ¿cómo puede el Sujeto Regulado determinar la manera en que el Interesado otorgó su consentimiento para saber luego si el mismo es válido o no? En caso de que la información sea obtenida por el Sujeto Regulado utilizando uno de esos medios, entonces aplicaría una sanción contra éste o sus empleados, no así cuando el Interesado ha accedido a otorgar información por coacción de un tercero. De ahí que sugerimos que se elimine la mención "para ser válido" contenida en la parte capital del párrafo 7.1."*

CONSIDERANDO: Que el artículo 7.1, (a) recoge simplemente vicios del consentimiento que, en nuestro Derecho Común y en Derecho comparado, lo convierten en inválido de pleno derecho; que el Código Civil de la República Dominicana recoge supuestos semejantes en su artículo 1109, cuando establece que: "No hay consentimiento válido, si ha sido dado por error, arrancado por violencia o sorprendido por dolo."; que en consecuencia, la Norma Complementaria que se apruebe en el dispositivo de esta resolución no será modificada en este aspecto;

CONSIDERANDO: Que otro de los comentarios de **VERIZON DOMINICANA, C. POR A.** sobre la Norma que nos ocupa es el que a continuación se transcribe:

*"**Consentimiento para el tratamiento.** La lectura combinada del párrafo 8.1 con el párrafo 8.3 de la norma, resulta que el único caso en que el Interesado puede oponerse al uso de la información, es cuando la misma se precisa para el cumplimiento o mantenimiento del contrato[1]. En ese sentido, consideramos que esta facultad discrecional del Interesado, coloca al Sujeto Regulado en una situación de desventaja, sobre todo si la*

[1] *"La norma no especifica, si es para el mantenimiento o cumplimiento del "tratamiento" o del contrato. Asumimos que es para lo segundo."*

ejecución del contrato debe hacerse por vía judicial. Requerir una orden de la autoridad implicaría tratar de levantar la oposición del Interesado o requerir del tribunal que fuere apoderado, ordenar revelar la información correspondiente al Interesado, para que la misma sea admitida en justicia."

CONSIDERANDO: Que la preocupación manifestada por **VERIZON** en este punto parece referirse más a la cancelación de los Datos de Carácter Personal que al consentimiento; que, no obstante, es entendible la inquietud manifestada por esa empresa, por lo que la Norma Complementaria que será aprobada en esta resolución será modificada respecto de la versión puesta en consulta pública, al objeto de evitar que la cancelación o la "retirada del consentimiento" pueda ser utilizado como vehículo para impedir que prospere una acción que le corresponda legítimamente ejercer a un Sujeto Regulado;

CONSIDERANDO: Que **VERIZON DOMINICANA, C. POR A.** expuso en sus comentarios, lo siguiente:

*"**Consentimiento sobre información sensible.** El párrafo 10.2, hace referencia a "información sensible", sin embargo no se distingue si esta "información sensible" es lo mismo que los "datos especialmente protegidos", definidos en el artículo 9."*

CONSIDERANDO: Que el comentario tiene un fundamento claro, conciso y de peso y en consecuencia, la Norma será modificada en ese aspecto;

CONSIDERANDO: Que **VERIZON DOMINICANA, C. POR A.** presentó también el siguiente comentario a la Resolución No. 077-05:

*"**Medidas de seguridad.** Es necesario especificar en el artículo 11, que dichas medidas deben concordar con los estándares vigentes en la industria, que definan mejores prácticas en seguridad de información."*

CONSIDERANDO: Que el Consejo Directivo, luego de haber evaluado la observación planteada por **VERIZON**, entiende pertinente lo sugerido, por lo que se añadirá a la Norma que sea aprobada en esta resolución, un Párrafo al respecto;

CONSIDERANDO: Que la empresa **VERIZON DOMINICANA, C. POR A.** expuso en sus comentarios, lo siguiente:

*"**Auditoria y medidas de seguridad.** El artículo 22 establece que se auditará el cumplimiento con las medidas de seguridad previstas en los procedimientos e instrucciones vigentes en materia de seguridad de datos. Sin embargo, no queda claro a qué procedimientos e instrucciones en materia de seguridad de datos se refiere este acápite. Parecería que se refiere a estándares tales como ISO 17799 y CobIT, pero es recomendable que se aclare para facilitar su interpretación y cumplimiento. Por otra parte, es imprescindible que se establezcan los criterios, lineamientos y límites de tales auditorias, a fin de otorgar seguridad a los Sujetos Regulados.*

Medidas de nivel medio. Las medidas de seguridad del nivel medio deben incluir el control sobre registro de acceso, según se especifica en el art. 29 sobre las medidas de seguridad de nivel alto. Esto, debido a que a nuestro juicio, la sensibilidad de la información relativa a detalles financieros amerita estas medidas."

CONSIDERANDO: Que los "procedimientos e instrucciones en materia de seguridad" aluden a aquellas medidas concretas implementadas por el Sujeto Regulado al objeto de cumplir con las medidas de seguridad previstas en la Norma Complementaria; por ejemplo, si la Norma requiere un control de acceso, distintos "procedimientos en materia de seguridad" serían un sistema de código para entrar en una puerta, un sistema de control biométrico, una llave, etc.; que, no obstante, se modificará la Norma para aclarar el acápite referido por **VERIZON DOMINICANA, C. POR A.** en la primera parte de su comentario;

CONSIDERANDO: Que, en lo tocante a las medidas de seguridad del nivel medio, la experiencia internacional de otras jurisdicciones con tradición en lo que respecta a la aplicación de medidas de seguridad para Datos de Carácter Personal, demuestra que el registro de acceso es una medida que puede tener un coste muy caro a medio plazo, razón por la cual se reserva para el nivel alto; que por este motivo, es preferible mantener el criterio previsto en la Norma Complementaria puesta en consulta pública; que, en consecuencia, entendemos que no debe modificarse la Norma Complementaria en este aspecto;

CONSIDERANDO: Que otro de los comentarios de **VERIZON DOMINICANA, C. POR A.** sobre la Norma que nos ocupa es el que se copia a seguidas:

> *"**Registro de accesos.** En el artículo 29, sugerimos incluir como obligación, guardar el nodo o la identificación (dirección IP, nombre netBIOS, etc.) de la terminal utilizada para realizar el acceso o intento de acceso, pues esto facilita la auditoria o investigaciones de accesos a datos que se determinen no autorizados.*
>
> *En este mismo artículo, se debe además requerir que el mecanismo utilizado para registrar los accesos pueda ser protegido contra desactivación, eliminación o modificación indebida, con el objetivo de preservar la integridad del mismo.*
>
> *Entendemos además, que las medidas de seguridad para datos de carácter personal descritos en el Título IV de esta norma no cubren aspectos relativos a la seguridad de las plataformas y redes sobre los que funcionan las aplicaciones que manejan este tipo de datos. Ejemplo de estos son la protección de las plataformas contra software maliciosos, como virus, gusanos, troyanos, spyware, etc., que pueden poner en riesgo la confidencialidad, integridad y disponibilidad de los datos; así como la aplicación oportuna de las actualizaciones y/o parches de seguridad a los sistemas operativos y plataformas, y otras medidas de seguridad para prevenir vías alternas de acceso a los datos de carácter personal. Es preciso poner a cargo de los Sujetos Regulados, la obligación de contar con seguridad en sus plataformas y redes y hacer mantenimientos razonables periódicos de las mismas."*

CONSIDERANDO: Que el Consejo Directivo, luego de haber evaluado las observaciones planteadas en los dos primeros párrafos del comentario, acoge lo sugerido en cuanto a las medidas de nivel alto, las cuales serán modificadas en la Norma que se apruebe en el dispositivo de esta resolución, al objeto de incorporar los comentarios de **VERIZON DOMINICANA, C. POR A.**;

CONSIDERANDO: Que en cuanto a lo planteado por **VERIZON** *sobre la seguridad de las plataformas y redes sobre las que funcionan las aplicaciones que manejan ese tipo de datos*, las Normas Complementarias de la Ley 126-02 sobre Procedimientos de Seguridad

(basada en el estándar ISO 17799) y sobre Criterios de Auditoría, establecen parámetros mínimos que deben ser observados por los Sujetos Regulados, tanto previamente al inicio del servicio, como en lo sucesivo, para lo cual el **INDOTEL** está facultado a realizar auditorías periódicas y por solicitud motivada, no requiriendo de modificación alguna la Norma elaborada en este sentido;

CONSIDERANDO: Que **VERIZON DOMINICANA, C. POR A.** presentó también el siguiente comentario a la Resolución No. 077-05:

> *"**Secreto.** Entendemos que la calificación que hace el artículo 35 de "secreto profesional" es inapropiada y redundante, toda vez que ya el texto y la finalidad de la norma, es precisamente poner a cargo del Sujeto Regulado, ciertas obligaciones de confidencialidad y uso de la información que adquiere de parte de los consumidores o usuarios.*
>
> *En adición, el "secreto profesional" está regulado en nuestro país, por los artículos 377 y 378 del Código Penal, por lo que calificar como tal a la actividad de los Sujetos Regulados, sería abrir la puerta a sanciones penales que la Ley 126 no contempla. Sugerimos que esta disposición sea eliminada."*

CONSIDERANDO: Que el concepto de "secreto profesional" no es redundante sino complementario respecto de las demás disposiciones de la Norma; que no obstante, y al objeto de evitar posibles confusiones respecto a su alcance, se sustituirá el término "secreto profesional" por "secreto";

CONSIDERANDO: Que otro de los comentarios de **VERIZON DOMINICANA, C. POR A.** a la Resolución No. 077-05, es el que se presenta a seguidas:

> *"**Responsabilidad Sujetos Regulados.** Sugerimos incluir en el artículo 37 o en cualquier otro lugar de la norma, alguna indicación de que el Sujeto Regulado se encuentra exento de responsabilidad, en caso de cumplir con los requerimientos del suscriptor o usuario, en caso de revelación de información."*

CONSIDERANDO: Que en principio, el tratamiento de Datos por el Sujeto Regulado de acuerdo con las indicaciones y consentimiento del Interesado (siempre cumpliendo lo previsto en la Norma) debería producir que dicho tratamiento fuera legítimo y no diera lugar a existencia de infracción ni, por lo tanto, sanción. Sin embargo, esto no implica que el Sujeto Regulado esté exonerado de responsabilidad dado que dicha responsabilidad puede surgir por otros motivos (por ejemplo, incumplimiento contractual, infracción de otras normas jurídicas distintas a la Norma Complementaria ahora comentada, entre otros), por lo que la propuesta de **VERIZON** no generará cambios en la Norma que será aprobada en el dispositivo de esta resolución;

CONSIDERANDO: Que la empresa **VERIZON** expuso en sus comentarios lo siguiente:

> *"**Graduación de sanciones.** Al igual que en las demás normas, entendemos que los daños y perjuicios deben ser evaluados por un tribunal, no por el INDOTEL a priori, por lo que no debe ser un elemento de consideración al momento de imponer sanciones en perjuicio de los Sujetos Regulados."*

CONSIDERANDO: Que este Consejo Directivo ha estimado oportuno el comentario avanzado por **VERIZON DOMINICANA, C. POR A.**, toda vez que la magnitud de los daños

y el eventual perjuicio sufrido, aún cuando son simples criterios de valoración, son ajenos a la esfera de acción de este órgano regulador y, como tal, independientes de cualquier acción de carácter administrativo; que, en tal virtud, procede realizar la modificación correspondiente en el texto de la Norma a ser aprobado;

VISTA: La Ley General de Telecomunicaciones No. 153-98 del 27 de mayo de 1998;

VISTA: La Ley de Comercio Electrónico, Documentos y Firmas Digitales, No. 126- 02, de fecha 4 del mes de septiembre de 2002;

VISTO: El Reglamento de Aplicación de la Ley No. 126-02, aprobado por el Decreto del Poder Ejecutivo número 335, de fecha 8 del mes de abril de 2003;

VISTA: La Resolución No. 42-03, dictada por el Consejo Directivo del **INDOTEL** en fecha 17 del mes de marzo de 2003, mediante la cual se aprueba el Reglamento de Aplicación a la Ley No. 126-02, sobre Comercio Electrónico, Documentos y Firma Digital y la Agenda Regulatoria en materia de Comercio Electrónico de la República Dominicana;

VISTA: La Resolución del Consejo Directivo del **INDOTEL** No. 077-05, de fecha 23 de junio de 2005, que ordenó el inicio del proceso de Consulta Pública para dictar las "Normas Complementarias" de la Ley No. 126-02, sobre Comercio Electrónico, Documentos y Firmas Digitales;

VISTO: El escrito depositado por **VERIZON DOMINICANA, C. POR A.**, con motivo de su participación en el proceso de Consulta Pública dispuesto por la Resolución del Consejo Directivo No. 077-05;

OIDOS: Los representante autorizados de **VERIZON DOMINICANA, C. POR A** ante el Consejo Directivo del **INDOTEL** 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 la empresa **VERIZON DOMINICANA, C. POR A.,** con ocasión del proceso de consulta pública iniciado mediante la Resolución No. 077-05, de este Consejo Directivo, para dictar la Norma Complementaria de la Ley No. 126-02 sobre Comercio Electrónico, Documentos y Firmas Digitales sobre **Protección de Datos de Carácter Personal por los Sujetos Regulados**, conforme a lo que ha sido indicado en el texto de esta resolución; **DISPONIENDO** la integración de todos los cambios señalados en el cuerpo de la presente resolución en la versión definitiva de la Norma Complementaria de la Ley No. 126-02 sobre Comercio Electrónico, Documentos y Firmas Digitales sobre **Protección de Datos de Carácter Personal por los Sujetos Regulados** que se aprueba mediante este documento.

SEGUNDO: APROBAR la Norma Complementaria de la Ley No. 126-02 sobre Comercio Electrónico, Documentos y Firmas Digitales sobre **Protección de Datos de Carácter Personal por los Sujetos Regulados**, cuyo texto íntegro se transcribe a continuación:

NORMA COMPLEMENTARIA
SOBRE PROTECCIÓN DE DATOS DE CARÁCTER PERSONAL POR LOS SUJETOS REGULADOS

TÍTULO I
DISPOSICIONES GENERALES

ART. 1.- OBJETO Y ÁMBITO DE APLICACIÓN

1.1 La presente Norma se dicta en desarrollo de lo dispuesto en la letra (c) del artículo 40 de la Ley No 126-02 el cual establece la obligación de las Entidades de Certificación de garantizar la protección, confidencialidad y debido uso de la información suministrada por el Suscriptor así como de lo regulado en la letra (c) del artículo 21 del Reglamento de Aplicación que regula la posibilidad de que el INDOTEL regule lo relativo a la protección de los Datos de Carácter Personal de los Suscriptores de Certificados.

1.2 Esta Norma establece el marco regulador aplicable al Tratamiento de Datos de Carácter Personal de los Consumidores y Usuarios por parte de los Sujetos Regulados.

1.3 Lo dispuesto en la presente Norma será aplicable a los Tratamientos de Datos de Carácter Personal de los Interesados que realicen los Sujetos Regulados, siendo irrelevante a estos efectos si tal Tratamiento se lleva a cabo en Archivos digitales o en papel, salvo cuando esta Norma establezca diferencias para uno u otro tipo de Archivos.

ART. 2.- DEFINICIONES

A los efectos de esta Norma, los siguientes términos cuando sean utilizados con letras mayúsculas según se indica, tendrán el significado que se establece a continuación:

(a) "Acceso Autorizado": autorizaciones concedidas a un usuario, esto es un sujeto o proceso autorizado para acceder a Datos o Recursos, para la utilización de los diversos Recursos;

(b) "Autenticación": procedimiento de comprobación de la identidad de un usuario;

(c) "Cesión" o "Comunicación": toda revelación de Datos de Carácter Personal realizada a una persona distinta del Interesado;

(d) "Certificado Digital": es el Documento Digital emitido y firmado digitalmente por una Entidad de Certificación, que identifica unívocamente a un Suscriptor durante el período de vigencia del Certificado, y que se constituye en prueba de que dicho Suscriptor es la fuente o el originador del contenido de un Documento Digital o Mensaje de Datos que incorpore su Certificado asociado;

(e) "Consumidor": es la persona natural o jurídica que contrata o solicita los servicios que presta un Sujeto Regulado atendiendo a las funciones que le corresponden como tal, comprendiendo, entre otros, a los

Suscriptores;

(f) "Contraseña": información confidencial, frecuentemente constituida por una cadena de caracteres, que puede ser usada en la Autenticación de un usuario;

(g) "Control de Acceso": mecanismo que, en función de la Identificación ya Autenticada, permite Acceder a Datos o Recursos;

(h) "Copia del Respaldo": copia de los datos de un Archivo en un Soporte que posibilite su recuperación;

(i) "Datos de Carácter Personal": cualquier información concerniente a personas naturales identificadas o identificables. Los datos relativos a personas jurídicas no serán considerados Datos de Carácter Personal, sin perjuicio de aquellos datos relativos a personas naturales que se encuentren vinculadas a dichas personas jurídicas que si podrán ser considerados como Datos de Carácter Personal, comprendiendo, entre otros, los datos de sus representantes, apoderados o trabajadores;

(j) "Documento Digital": es la información codificada en forma digital sobre un soporte lógico o físico, en la cual se usan métodos electrónicos o similares que se constituyen en representación de actos, hechos o datos jurídicamente relevantes;

(k) "Encargado del Tratamiento": la persona natural o jurídica, autoridad pública, servicio o cualquier otro organismo que, solo o conjuntamente con otros, trate Datos de Carácter Personal por cuenta del Sujeto Regulado;

(l) "Entidad de Certificación": es aquella institución o persona jurídica autorizada conforme a la Ley No. 126-02, el Reglamento de Aplicación y las Normas Complementarias dictadas por el INDOTEL al respecto, que está facultada para emitir Certificados en relación con las Firmas Digitales de las personas, ofrecer o facilitar los servicios de registro y estampado cronológico de la transmisión y recepción de Mensajes de Datos, así como cumplir otras funciones relativas a las comunicaciones basadas en las Firmas Digitales, Firma Electrónicas u otros procedimientos de seguridad;

(m) "Archivo": todo conjunto organizado de Datos de Carácter Personal, cualquiera que fuere la forma o modalidad de su creación, almacenamiento, organización y acceso;

(n) "Firma Digital": se entenderá como un valor numérico que se adhiere a un Mensaje de Datos o Documento Digital y que, utilizando un procedimiento matemático conocido, vinculado a la clave del Iniciador y al texto del Mensaje o Documento, permite determinar que este valor se ha obtenido exclusivamente con la clave del Iniciador y el texto del Mensaje o Documento, y que el Mensaje o Documento inicial no ha sido modificado después de efectuada la transmisión;

(ñ) "Identificación": procedimiento de reconocimiento de la identidad de un usuario;

(o) "Incidencia": cualquier anomalía que afecte o pudiera afectar a la seguridad de los datos;

(p) "INDOTEL": Instituto Dominicano de las Telecomunicaciones, órgano regulador de las telecomunicaciones y del comercio electrónico, documentos y Firmas Digitales, de conformidad con las Leyes No.153-98 General de Telecomunicaciones y la Ley No. 126-02, respectivamente;

(q) "Interesado": persona natural que, actuando como Consumidor o Usuario, es titular de los Datos de Carácter Personal que sean objeto del Tratamiento por el Sujeto Regulado;

(r) "Ley No. 126-02": Ley de Comercio Electrónico, Documentos y Firmas Digitales, número 126-02;

(s) "Mensaje de Datos": es la información generada, enviada, recibida, almacenada o comunicada por medios electrónicos o similares como pudieran ser, entre otros, el intercambio electrónico de datos, denominado EDI por sus siglas en inglés, o el correo electrónico;

(t) "Norma": la presente Norma sobre Protección de Datos de Carácter Personal por los Sujetos Regulados, incluidas las modificaciones que en un futuro se puedan producir en la misma;

(u) "Normas Complementarias": normas dictadas por el INDOTEL en desarrollo de la Ley No. 126-02 y el Reglamento de Aplicación, para regular áreas específicas de esta materia;

(v) "Procedimiento de Disociación": todo Tratamiento de Datos de Carácter Personal de modo que la información que se obtenga no pueda asociarse a persona identificada o identificable;

(w) “Proveedor de Servicios de Firma Electrónica”: es toda persona moral, nacional o extranjera, pública o privada, que preste servicios de certificación, y cuyos Certificados de Firma no sirven para soportan firmas con valor legal de Firma Digital, sin perjuicio de los demás servicios que puedan realizar;

(x) "Recurso": cualquier parte componente de un Sistema de Información;

(y) "Reglamento de Aplicación": Reglamento de Aplicación de la Ley No. 126-02, aprobado mediante el Decreto No. 335-03;

(z) "Responsable de Seguridad": persona o personas a las que el Sujeto Regulado ha asignado formalmente la función de coordinar y controlar las medidas de seguridad aplicables de acuerdo con lo dispuesto en esta Norma;

(aa) "Responsable del Archivo o Tratamiento": Sujeto Regulado que decida sobre la finalidad, contenido y uso del Tratamiento. Salvo que en la presente Norma se indique lo contrario, se entenderá que todas las menciones a los Sujetos Regulados se refieren a aquellos que actúan como Responsables del Archivo o Tratamiento;

(bb) "Salario Mínimo": será el salario mínimo nacional más bajo percibido por los trabajadores del sector privado no sectorizado de empresas industriales, comerciales y de servicios, fijado por el Comité Nacional de Salarios de la Secretaría de Estado de Trabajo de la República Dominicana;

(cc) "Sistema de Información": conjunto de ficheros, programas, soportes y equipos empleados para el almacenamiento y Tratamiento de Datos de Carácter Personal;

(dd) “Sujeto Regulado”: las Entidades de Certificación, los Proveedores de Servicios de Firma Electrónica y las Unidades de Registro, así como los Proveedores de Servicios o Infraestructura de Soporte operacionalmente vinculados con estas en la medida de su relación contractual;

(ee) "Suscriptor": es la persona que contrata con una Entidad de Certificación la expedición de un Certificado Digital, para que sea nombrada o identificada en él. Esta persona tiene la obligación de mantener bajo su estricto y exclusivo control el procedimiento para generar su Firma Digital;

(ff) "Transferencias Internacionales de Datos de Carácter Personal": todo movimiento de Datos de Carácter Personal sin importar el soporte en que se encuentren los mismos ni el tipo de tratamiento que reciban, fuera del territorio de la República Dominicana , bien sea en el contexto de una Comunicación de Datos; con destino a un Encargado del Tratamiento; o en cualquier otro contexto y con cualquier otro destino, incluyendo, sin limitación, el movimiento a o desde sucursales o establecimientos permanentes;

(gg) "Tratamiento": en relación con los Datos de Carácter Personal, toda operación o procedimiento técnico de carácter automatizado o no, que permita, de forma total o parcial, su recogida, grabación, conservación, elaboración, modificación, bloqueo, cancelación, eliminación, publicación, difusión, distribución, revelación o transmisión;

(hh) "Usuario": es la persona que, sin ser Consumidor, puede, sin embargo, recibir servicios prestados por un Sujeto Regulado atendiendo a las funciones que le corresponden como tal, comprendiendo, entre otros, la validación de la integridad y autenticidad de un Documento Digital o de un Mensaje de Datos con base en un Certificado Digital del Suscriptor originador del Mensaje.

ART. 3.- INTERPRETACIÓN

3.1 La presente Norma deberá interpretarse:

(a) Considerando la importancia que para la protección de la intimidad y honor de los Interesados tiene el establecimiento de un marco regulador cierto para el Tratamiento de sus Datos de Carácter Personal por parte de los Sujetos Regulados;

(b) Observando lo dispuesto en la normativa dominicana reguladora del Comercio Electrónico, Documentos y Firmas Digitales y, en especial, la Ley No. 126-02, el Reglamento de Aplicación, las

Normas Complementarias y otras disposiciones que puedan dictarse en desarrollo de esta materia.

3.2 Las menciones y remisiones a normas legales contenidas en esta Norma, 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 legales, las remisiones previstas en la presente Norma serán interpretadas de la forma que mejor se adapte al propósito inicial de tal remisión.

TÍTULO II
INFORMACIÓN EN LA RECOGIDA DE LOS DATOS DE CARÁCTER PERSONAL

CAPÍTULO I

RECOGIDA DE DATOS DIRECTAMENTE DE LOS PROPIOS INTERESADOS

ART. 4.- INFORMACIÓN A SUMINISTRAR EN LA RECOGIDA DE DATOS DIRECTAMENTE DE LOS PROPIOS INTERESADOS

4.1 Los Sujetos Regulados que, en sus relaciones con los Interesados, les soliciten Datos de Carácter Personal, deberán informarles de forma previa a su recogida y de modo expreso, preciso e inequívoco de, al menos, los siguientes extremos:

(a) De que los Datos de Carácter Personal serán almacenados en un Archivo de Datos de Carácter Personal al objeto de ser Tratados;

(b) De las características de dicho Tratamiento;

(c) De la finalidad de la recogida de los Datos de Carácter Personal;

(d) Del carácter obligatorio o facultativo de su respuesta a las preguntas que les sean formuladas;

(e) De las consecuencias de la obtención de los Datos de Carácter Personal o de la negativa a suministrarlos;

(f) De la posibilidad de ejercitar los derechos de acceso, rectificación y cancelación de acuerdo con lo dispuesto en el Título IX de esta Norma; y

(g) De la identidad y dirección del Sujeto Regulado o, en su caso, dirección en la cual el Sujeto Regulado haya fijado domicilio en la República Dominicana de acuerdo con lo dispuesto en la normativa aplicable.

Párrafo: No será necesaria la información a que se refiere la letra (d) del apartado 4.1, si el contenido de ella se deduce claramente de la naturaleza de los Datos de Carácter Personal que se solicitan o de las circunstancias en que se recaban.

4.2 Cuando se utilicen cuestionarios, formularios u otros escritos para la recogida, figurarán en los mismos, en forma claramente legible, las advertencias a que se refiere el apartado 4.1 precedente.

Párrafo: A los efectos de lo previsto en el apartado 4.2 será irrelevante el soporte en el que tales cuestionarios, formularios o escritos, siendo lo allí dispuesto aplicable tanto en el caso de Documentos Digitales como documentos en papel.

4.3 Lo previsto en este artículo se entenderá sin perjuicio de aquellas otras obligaciones de información que pudieran ser aplicables a los Sujetos Regulados de acuerdo con lo dispuesto en otras normas legales de aplicación, entre otras, la Ley No. 126-02, el Reglamento de Aplicación y las Normas Complementarias.

CAPÍTULO II

RECOGIDA DE DATOS DE FUENTES DISTINTAS DE LOS PROPIOS INTERESADOS

ART. 5.- INFORMACIÓN A SUMINISTRAR EN LA RECOGIDA DE DATOS DE FUENTES DISTINTAS A LOS PROPIOS INTERESADOS

5.1 En aquellos casos en los que los Sujetos Regulados recojan Datos de Carácter Personal relativos a los Interesados de fuentes distintas a éstos, según se regula en el artículo 4 de esta Norma, los Sujetos Regulados deberán informar a estos Interesados, de forma expresa, precisa e inequívoca, dentro de los tres meses siguientes al momento del registro de los Datos de Carácter Personal, de los siguientes extremos:

(a) Aquellos previstos en las letras (a), (b), (c), (f) y (g) del apartado 4.1 de esta Norma; y

(b) La procedencia de los Datos de Carácter Personal indicando, de existir, la identidad y dirección de la entidad de la que los Datos de Carácter Personal procedan.

5.2 No será de aplicación lo dispuesto en el apartado 5.1 anterior en los siguientes supuestos, que tendrán carácter taxativo:

(a) Cuando el suministro de la información a los Interesados resulte imposible o exija esfuerzos desproporcionados a criterio del INDOTEL, en consideración, entre otros, al número de Interesados, a la antigüedad de los Datos de Carácter Personal y al coste de suministrar tal información; o

(b) Cuando los Interesados hayan sido ya informados previamente de todos los extremos previstos en el apartado 5.1.

TÍTULO III
CONSENTIMIENTO PARA EL TRATAMIENTO DE DATOS DE CARÁCTER PERSONAL

CAPÍTULO I

CONSENTIMIENTO PARA EL TRATAMIENTO DE DATOS DE CARÁCTER PERSONAL NO ESPECIALMENTE PROTEGIDOS

ART. 6.- OBLIGACIÓN DE OBTENER EL CONSENTIMIENTO

El Tratamiento de los Datos de Carácter Personal por parte de los Sujetos Regulados requerirá del consentimiento previo e inequívoco de los Interesados, salvo cuando la presente Norma prevea expresamente otra cosa.

ART. 7.- CARACTERÍSTICAS DEL CONSENTIMIENTO

7.1 Sin perjuicio de otros requisitos adicionales que pudieran requerirse por esta Norma para determinado tipo de Tratamientos, el consentimiento expreso previsto en el artículo 6 de esta Norma deberá cumplir los siguientes requisitos para ser válido:

(a) Ser libre, esto es desprovisto de coacciones, amenazas, engaños y/o errores; e

(b) Informado, es decir, prestado sobre una información cierta y precisa respecto a las condiciones del Tratamiento de los Datos de Carácter Personal que deberá serle suministrada por el Sujeto Regulado al Interesado de forma previa a la obtención de su consentimiento.

7.2 El requisito previsto en la letra (b) del apartado 7.1 anterior se considerará cumplido mediante el suministro de la información prevista en el artículo 4 de esta Norma, siempre y cuando dicha información sea cierta.

7.3 El consentimiento a que se refiere este artículo será libremente revocable por el Interesado, debiendo comunicar este hecho al Sujeto Regulado, sin que para ello se le exijan mayores formalidades que las requeridas en el momento de su prestación.

Párrafo I: La revocación del consentimiento no tendrá efectos retroactivos.

Párrafo II: Inmediatamente tras el conocimiento por el Sujeto Regulado de la revocación del consentimiento, deberá cesar en el Tratamiento de los Datos de Carácter Personal del correspondiente Interesado, salvo en el caso de que tal Tratamiento sin consentimiento sea posible por aplicación de alguna de las excepciones previstas en el artículo 8 de esta Norma y sin perjuicio de lo allí regulado.

ART. 8.- EXCEPCIONES A LA OBLIGACIÓN DE OBTENER EL CONSENTIMIENTO DE LOS INTERESADOS

8.1 No será preciso obtener el consentimiento de los Interesados, según se prevé en el artículo 6 de esta Norma, en los siguientes supuestos que tendrán naturaleza taxativa:

(a) En tanto en cuanto los Datos de Carácter Personal que sean objeto de Tratamiento correspondan a las partes de un contrato y

sean necesarios para el mantenimiento o cumplimiento del mismo;

(b) Cuando el Tratamiento de los Datos de Carácter Personal responda a una obligación legal o mandato de una autoridad judicial o administrativa que actué en el ejercicio de sus competencias; o

(c) Cuando la presente Norma establezca expresamente que dicho consentimiento no es preciso.

8.2 La excepción a la obtención del consentimiento que se prevé en este artículo no exonerará en ningún caso de la obligación de cumplir otras obligaciones previstas en esta Norma, en particular pero sin limitación, las obligaciones de información reguladas en el artículo 4.

8.3 En los casos en los que no sea necesario el consentimiento del Interesado para el Tratamiento de sus Datos de Carácter Personal, y siempre que una disposición normativa o mandato de una autoridad judicial o administrativa competente no disponga lo contrario, éste podrá oponerse a su Tratamiento cuando existan motivos fundados y legítimos relativos a una concreta situación personal. En tal supuesto, el Responsable del Archivo excluirá del Tratamiento los Datos de Carácter Personal relativos al Interesado.

Párrafo: La oposición del Interesado respecto del Tratamiento de sus Datos de Carácter Personal Tratados por el Sujeto Regulado sin el consentimiento del Interesado al amparo de lo previsto en la letra (a) del apartado 8.1, no será de aplicación respecto del Tratamiento de dichos Datos de Carácter Personal por el Sujeto Regulado a los exclusivos efectos de ejercitar aquellas acciones que en Derecho procediesen frente al Interesado o, en su caso, de defenderse ante las acciones ejercitadas por el Interesado, en ambos casos respecto de la relación contractual en cuyo contexto se Trataron tales Datos de Carácter Personal. Dichos Datos de Carácter Personal no podrán ser Tratados por el Sujeto Regulado más que con la finalidad aquí señalada, siendo eficaz el ejercicio de la oposición respecto a cualquier Tratamiento distinto del aquí expresamente mencionado.

CAPÍTULO II

CONSENTIMIENTO PARA EL TRATAMIENTO DE DATOS DE CARÁCTER PERSONAL ESPECIALMENTE PROTEGIDOS

ART. 9.- CONSENTIMIENTO PARA EL TRATAMIENTO DE DATOS ESPECIALMENTE PROTEGIDOS

9.1 Sólo con el consentimiento expreso y por escrito de los Interesados podrán ser objeto de Tratamiento por los Sujetos Regulados, los Datos de Carácter Personal que revelen la ideología, afiliación sindical, religión, creencias, origen racial, salud o vida sexual del Interesado.

Párrafo: A los efectos de cumplir con lo previsto en el apartado 9.1

anterior, se admitirá el consentimiento expreso prestado mediante la utilización de Documentos Digitales o Mensajes de Datos, siempre que éstos cumplan los requisitos necesarios para ser funcionalmente equivalentes con aquel consentimiento expreso formalizado en papel, de acuerdo con lo dispuesto en la Ley No. 126-02 y otras normas legales aplicables.

9.2 El consentimiento expreso y escrito previsto en este artículo se entenderá, en todo caso, sin perjuicio de la aplicación de los requisitos previstos para el consentimiento en el artículo 7 de la presente Norma.

ART. 10.- EXCEPCIONES AL REQUISITO DEL CONSENTIMIENTO EXPRESO Y ESCRITO

10.1 El consentimiento expreso y escrito previsto en el artículo 9 precedente no será aplicable a los siguientes Tratamientos:

(a) En lo que respecta a los Datos de Carácter Personal relativos a la ideología, afiliación sindical, religión o creencias de los Interesados: los Tratamientos que realicen partidos políticos, sindicatos, iglesias, confesiones o comunidades religiosas y asociaciones, fundaciones y organizaciones sin fines de lucro, cuya finalidad sea política, filosófica, religiosa o sindical, en cuanto a los Datos de Carácter Personal relativos a sus asociados o miembros.

(b) En lo que atañe a los Datos de Carácter Personal relativos a salud de los Interesados: los Tratamientos que realicen las instituciones y los centros sanitarios públicos y privados y los profesionales sanitarios y médicos correspondientes, en el ejercicio de las actividades profesionales que les corresponde desempeñar como tales.

10.2 El Tratamiento de los Datos de Carácter Personal mencionados en el apartado 10.1 anterior por las entidades previstas en dicho apartado 10.1, se someterá, en todo caso, a los requisitos del consentimiento previstos en el artículo 7 de esta Norma así como a las demás disposiciones aplicables.

TÍTULO IV

SEGURIDAD DE LOS DATOS DE CARÁCTER PERSONAL

CAPÍTULO I

OBLIGACIÓN DE ADOPTAR MEDIDAS DE SEGURIDAD

ART. 11.- OBLIGACIÓN DE ADOPTAR MEDIDAS DE SEGURIDAD

11.1 Los Sujetos Regulados, deberán adoptar las medidas de índole técnica y organizativas que se describen en este Título, al objeto de garantizar la seguridad de los Datos de Carácter Personal y evitar su alteración, pérdida, Tratamiento o acceso no autorizado, habida cuenta del estado

de la tecnología, la naturaleza de los Datos de Carácter Personal almacenados y los riesgos a que están expuestos, ya provengan de la acción humana del medio físico o natural.

Párrafo I: Las medidas de seguridad mencionadas en el apartado 11.1 precedente se entenderán sin perjuicio de aquellas que deban ser aplicadas por los Sujetos Regulados en cumplimiento de lo dispuesto en otras disposiciones legales, en particular pero sin limitación, la Ley No. 126-02, el Reglamento de Aplicación y las Normas Complementarias.

Párrafo II: Los procedimientos técnicos y organizativos que los Sujetos Regulados instalen o pongan en práctica al objeto de adoptar las medidas de seguridad previstas en este apartado 11.1, deberán concordar (cuando existan) con los estándares vigentes en la industria en cada momento que definan las mejores prácticas en cuanto a seguridad de la información. En todo caso, en caso de contradicción entre dichos estándares y la presente Norma, será de aplicación preferente esta Norma.

11.2 Las medidas de seguridad previstas en el apartado 11.1 precedente, no serán aplicables a Archivos en papel, cuando dicha aplicación requiera el tratamiento de información en formato digital o electrónico.

11.3 Los Sujetos Regulados no registrarán Datos de Carácter Personal de los Interesados en Archivos que no reúnan las condiciones de seguridad previstas en este Título IV.

11.4 Las medidas de seguridad previstas en el apartado 11.1 deberán ser igualmente aplicadas por los Sujetos Regulados que intervengan en el Tratamiento como Encargados del Tratamiento atendiendo, en todo caso, a las instrucciones que le proporcione el Sujeto Regulado Responsable del Tratamiento de acuerdo con lo dispuesto en el Título VII de esta Norma.

CAPÍTULO II

MEDIDAS DE SEGURIDAD

Sección 1ª

Niveles de Seguridad

ART. 12.- NIVELES DE MEDIDAS DE SEGURIDAD

12.1 Las medidas de seguridad exigibles de acuerdo con lo previsto en el artículo 11 de esta Norma, se clasificarán en los siguientes tres niveles que se establecen atendiendo a la naturaleza de la información tratada, en relación con la mayor o menor necesidad de garantizar la confidencialidad y la integridad de la información:

(a) Todos los Archivos que contengan Datos de Carácter Personal deberán adoptar las medidas de seguridad calificadas como de Nivel Básico previstas en la Sección 2 de este Capítulo II.

(b) Los Archivos que contengan Datos de Carácter Personal

relativos a servicios financieros, morosidad o solvencia patrimonial y crédito, deberán reunir, además de las medidas de seguridad de Nivel Básico arriba mencionadas, aquellas calificadas como de Nivel Medio reguladas en la Sección 3 de este Capítulo II.

(c) Los Archivos que contengan Datos de Carácter Personal sobre ideología, religión, creencias, afiliación sindical, origen racial, salud o vida sexual deberán reunir, además de las medidas de Nivel Básico y Nivel Medio previstas en las dos letras precedentes, las calificadas como de Nivel Alto previstas en la Sección 4 de este Capítulo II.

12.2 Cada uno de los niveles de seguridad descritos en el apartado precedente tendrán la condición de mínimos exigibles, sin perjuicio de las disposiciones legales que puedan establecer requisitos de seguridad adicionales o complementarios, en especial pero sin limitación, la Ley No. 126-02, el Reglamento de Aplicación y las Normas Complementarias, en especial, la titulada "Guía para la Formulación de Medidas de Seguridad".

Sección 2ª

Medidas de Seguridad de Nivel Básico

ART. 13.- DOCUMENTO DE SEGURIDAD

13.1 Los Sujetos Regulados elaborarán e implantarán la normativa de seguridad mediante un documento de obligado cumplimiento para el personal con acceso a los Datos de Carácter Personal y a los Sistemas de Información que los traten. Dicho documento se denominará "Documento de Seguridad".

13.2 El Documento de Seguridad deberá contener, como mínimo, los siguientes aspectos:

(a) Ámbito de aplicación del Documento de Seguridad con especificación detallada de los Recursos protegidos;

(b) Medidas, normas, procedimientos, reglas y estándares encaminados a garantizar el nivel de seguridad que corresponda de acuerdo con lo exigido en este Capítulo II;

(c) Funciones y obligaciones del personal;

(d) Estructura de los Archivos con Datos de Carácter Personal y descripción de los Sistemas de Información que los tratan;

(e) Procedimiento de notificación, gestión y respuesta ante las Incidencias;

(f) Los procedimientos de realización de copias de respaldo y de recuperación de los datos.

13.3 El Documento de Seguridad deberá mantenerse en todo momento

actualizado y deberá ser revisado siempre que se produzcan cambios relevantes en el Sistema de Información o en la organización del mismo.

13.4 El contenido del Documento de Seguridad deberá adecuarse, en todo momento, a las disposiciones vigentes en materia de seguridad de los Datos de Carácter Personal.

13.5 El Documento de Seguridad estará a disposición del INDOTEL para su consulta a requerimiento de éste.

13.6 Siempre que se cumplan todos los requisitos exigidos en este artículo, el Documento de Seguridad podrá incorporarse a aquellas otras políticas de seguridad que deba elaborar el Sujeto Regulado en cumplimiento de lo dispuesto en otras normas de aplicación, en particular, a la Política de Seguridad prevista en la Norma Complementaria titulada "Guía para la Formulación de Procedimientos de Seguridad".

ART. 14.- FUNCIONES Y OBLIGACIONES DEL PERSONAL

14.1 Las funciones y obligaciones de cada una de las personas con acceso a los Datos de Carácter Personal y a los Sistemas de Información que los Tratan deberán ser claramente definidas y documentadas por los Sujetos Regulados en el Documento de Seguridad de acuerdo con lo previsto en la letra (c) del apartado 13. 2 de esta Norma.

14.2 Los Sujetos Regulados adoptarán las medidas necesarias para que dicho personal conozca las normas de seguridad que afecten al desarrollo de sus funciones así como las consecuencias en que pudiera incurrir en caso de incumplimiento.

ART. 15.- REGISTRO DE INCIDENCIAS.

Los Sujetos Regulados deberán disponer de un procedimiento de notificación y gestión de Incidencias que contendrá necesariamente un registro en el que se haga constar, al menos, la siguiente información respecto a cada Incidencia que ocurra:

(a) El tipo de Incidencia;

(b) El momento en que se ha producido;

(c) La persona que realiza la notificación;

(d) A quién se le comunica; y

(e) Los efectos que se hayan derivado de la misma.

ART. 16.- IDENTIFICACIÓN Y AUTENTICACIÓN

16.1 Los Sujetos Regulados se encargarán de que exista una relación actualizada de usuarios que tengan Acceso Autorizado al Sistema de Información y de establecer procedimientos de Identificación y Autenticación para dicho Acceso.

16.2 Cuando el mecanismo de Autenticación que se implante en

cumplimiento de lo previsto en el apartado precedente se base en la existencia de Contraseñas, existirá un procedimiento de asignación, distribución y almacenamiento que garantice su confidencialidad e integridad.

16.3 Las Contraseñas se cambiarán con la periodicidad que se determine en el Documento de Seguridad y mientras estén vigentes se almacenarán de forma ininteligible.

ART. 17.- CONTROL DE ACCESO

17.1 Los usuarios tendrán Acceso Autorizado únicamente a aquellos datos y Recursos que precisen para el desarrollo de sus funciones. Los Sujetos Regulados establecerán mecanismos para evitar que un usuario pueda acceder a datos o Recursos con facultades o derechos distintos de los autorizados.

17.2 La relación de usuarios a la que se refiere el apartado 16.1 de esta Norma contendrá el Acceso Autorizado para cada uno de ellos.

17.3 Exclusivamente el personal autorizado para ello en el Documento de Seguridad podrá conceder, alterar o anular el Acceso Autorizado sobre los datos y Recursos, conforme a los criterios establecidos por el Sujeto Regulado.

ART. 18.- GESTIÓN DE SOPORTES.

18.1 Los soportes informáticos que contengan Datos de Carácter Personal deberán permitir identificar el tipo de información que contienen, ser inventariados y almacenarse en un lugar con acceso restringido al personal autorizado para ello en el Documento de Seguridad.

18.2 La salida de soportes informáticos que contengan Datos de Carácter Personal, fuera de los locales en los que está ubicado el Archivo, únicamente podrá ser autorizada por el Sujeto Regulado.

ART. 19.- COPIAS DE RESPALDO Y RECUPERACIÓN

19.1 El Sujeto Regulado se encargará de verificar la definición y correcta aplicación de los procedimientos de realización de copias de respaldo y de recuperación de los Datos de Carácter Personal.

19.2 Los procedimientos establecidos para la realización de copias de respaldo y para la recuperación de los Datos de Carácter Personal deberá garantizar su reconstrucción en el estado en que se encontraban al tiempo de producirse la pérdida o destrucción.

19.3 Deberán realizarse copias de respaldo, al menos semanalmente, salvo que en dicho período no se hubiera producido ninguna actualización de los Datos de Carácter Personal.

Sección 3ª

Medidas de Seguridad de Nivel Medio

ART. 20.- DOCUMENTO DE SEGURIDAD

El Documento de Seguridad deberá contener, además de lo dispuesto en el artículo 13 de esta Norma, los siguientes extremos:

(a) La identificación del Responsable o Responsables de Seguridad, según se regula en el artículo 21;

(b) Los controles periódicos que se deban realizar para verificar el cumplimiento de lo dispuesto en el propio Documento de Seguridad; y

(c) Las medidas que sean necesarias adoptar cuando un soporte que contenga Datos de Carácter Personal vaya a ser desechado o reutilizado.

ART. 21.- RESPONSABLE DE SEGURIDAD

21.1 El Sujeto Regulado designará uno o varios Responsables de Seguridad encargados de coordinar y controlar las medidas definidas en el Documento de Seguridad.

21.2 En ningún caso esta designación será considerada como una delegación de la responsabilidad que corresponde asumir al Sujeto Regulado de acuerdo con lo dispuesto en esta Norma.

ART. 22.- AUDITORÍA

22.1 Los Sistemas de Información e instalaciones de Tratamiento de Datos de Carácter Personal se someterán al menos, cada dos (2) años a una auditoría interna o externa, que verifique el cumplimiento de las medidas de seguridad previstas en este Título IV.

22.2 Como resultado de la auditoria mencionada en el apartado precedente, los auditores que la hayan llevado a cabo deberán redactar un informe en el que deberá incluirse, al menos, lo siguiente:

(a) Dictamen acerca de la adecuación de las medidas y controles al presente Título IV;

(b) Identificación de las deficiencias encontradas;

(c) Propuesta de las medidas correctoras o complementarias necesarias; y

(d) Datos, hechos y observaciones en que se basen los dictámenes alcanzados y recomendaciones propuestas.

22.3 Los informes de auditoría serán analizados por el Responsable de Seguridad competente, que elevará las conclusiones al Sujeto Regulado para que adopte las medidas correctoras adecuadas.

22.4 Los informes de auditoría quedarán a disposición del INDOTEL para su consulta a requerimiento de éste.

22.5 Siempre que se respeten los requisitos regulados para las mismas, las auditorias reguladas en este artículo podrán incorporarse a aquellas otras que deba llevar a cabo el Sujeto Regulado de acuerdo con lo dispuesto en la normativa que le sea de aplicación, en particular, a las auditorias de gestión anuales previstas en la Norma Complementaria "Normas y Criterios de Auditoría de Servicios de Certificación".

ART. 23.- IDENTIFICACIÓN Y AUTENTICACIÓN

23.1 El Sujeto Regulado establecerá un mecanismo que permita:

(a) Identificar de forma inequívoca y personalizada a todo aquel usuario que intente acceder al Sistema de Información en el que se Traten Datos de Carácter Personal; y

(b) Verificar que dicho usuario está autorizado.

23.2 Se limitará la posibilidad de intentar reiteradamente el acceso no autorizado a los Sistemas de Información en los que se realizan Tratamientos de Datos de Carácter Personal, de tal forma que se imposibilite la obtención de dicho acceso no autorizado mediante la prueba de combinaciones de claves u otros elementos de control de acceso.

ART. 24.- CONTROL DE ACCESO FÍSICO

Exclusivamente el personal autorizado en el Documento de Seguridad podrá tener acceso a los locales donde se encuentren ubicados los Sistemas de Información en los que se Traten Datos de Carácter Personal.

ART. 25.- GESTIÓN DE SOPORTES

25.1 Deberá establecerse un sistema de registro de entrada de soportes informáticos que permita conocer los siguientes extremos respecto a cada entrada:

(a) El tipo de soporte;

(b) La fecha y hora;

(c) El emisor;

(d) El número de soportes;

(e) El tipo de información que contienen;

(f) La forma de envío; y

(g) La persona responsable de la recepción que deberá estar debidamente autorizada por el Sujeto Regulado.

25.2 De forma adicional al sistema de registro de entrada previsto en el

apartado precedente, se deberá disponer de un sistema de registro de salida de soportes informáticos que permita, conocer los siguientes extremos respecto de cada salida:

(a) El tipo de soporte;

(b) La fecha y hora;

(c) El destinatario;

(d) El número de soportes;

(e) El tipo de información que contienen;

(f) La forma de envío; y

(g) La persona responsable de la entrega que deberá estar debidamente autorizada por el Sujeto Regulado.

25.3 Cuando un soporte vaya a ser desechado o reutilizado, se adoptarán las medidas necesarias para impedir cualquier recuperación posterior de la información almacenada en él, previamente a que se proceda a su baja en el correspondiente inventario.

25.4 Cuando los soportes vayan a salir fuera de los locales en que se encuentren ubicados los Archivos como consecuencia de operaciones de mantenimiento, se adoptarán las medidas necesarias para impedir cualquier recuperación indebida de la información almacenada en ellos.

ART. 26.- REGISTRO DE INCIDENCIAS

En el registro de Incidencias regulado en el artículo 15 de esta Norma deberán consignarse, además de lo previsto en dicho artículo, lo siguiente:

(a) Los procedimientos de recuperación de los Datos de Carácter Personal realizados;

(b) La persona que ejecutó el proceso de recuperación;

(c) Los Datos de Carácter Personal restaurados; y

(d) En su caso, qué Datos de Carácter Personal ha sido necesario grabar manualmente en el proceso de recuperación.

ART. 27.- PRUEBAS CON DATOS REALES

Las pruebas anteriores a la implantación o modificación de los Sistemas de Información que traten Archivos con Datos de Carácter Personal no se realizarán con datos reales, salvo que se asegure el nivel de seguridad correspondiente al tipo de Archivo tratado de acuerdo con lo dispuesto en el artículo 12 de esta Norma.

Sección 4ª

Medidas de Seguridad de Nivel Alto

ART. 28.- DISTRIBUCIÓN DE SOPORTES

La distribución de los soportes que contengan Datos de Carácter Personal se realizará cifrando dichos datos o bien utilizando cualquier otro mecanismo que garantice que dicha información no sea inteligible ni manipulada durante su transporte.

ART. 29.- REGISTRO DE ACCESOS

29.1 De cada acceso a los Datos de Carácter Personal se guardará, como mínimo, la siguiente información:

(a) La Identificación del usuario que realiza o intenta el acceso;

(b) La fecha y hora en que se realizó el acceso o el intento de acceso;

(c) El Archivo accedido o al que se intento acceder;

(d) El tipo de acceso; y

(e) Si el acceso fue autorizado o denegado.

Párrafo I: En caso de que el acceso fuera autorizado, será preciso guardar, de forma adicional a lo previsto en el apartado 29.1, la información que permita identificar el registro accedido.

Párrafo II: En caso de que el acceso a los Datos de Carácter Personal se realizase mediante sistemas de comunicación (incluidas, sin limitación, las redes de comunicación), de forma adicional a lo previsto en el apartado 29.1, será preciso conservar información sobre el nodo o la identificación única de la terminal o equipo utilizados para realizar el acceso.

29.2 Los mecanismos que permitan el registro de los datos detallados en el apartado precedente estarán bajo el control directo del Responsable de Seguridad competente sin que se deba permitir, en ningún caso, la desactivación de los mismos.

29.3 El período mínimo de conservación de los datos registrados según lo previsto en este artículo será de dos (2) años.

29.4 El Responsable de Seguridad competente se encargará de revisar periódicamente la información de control registrada y, al menos una (1) vez al mes, elaborará un informe sobre las revisiones realizadas y los problemas detectados. Dicho informe quedará a disposición de las personas responsables del Sujeto Regulado al objeto de que puedan revisarlo y tomar las medidas que consideren convenientes para preservar la seguridad de los Datos.

ART. 30.- COPIAS DE RESPALDO Y RECUPERACIÓN

Deberá conservarse una copia de respaldo y de los procedimientos de recuperación de los Datos de Carácter Personal en un lugar diferente de aquel en que se encuentren los equipos informáticos que Tratan dichos Datos de Carácter Personal cumpliendo, en todo caso, las medidas de seguridad exigidas en este Título IV.

ART. 31.- TELECOMUNICACIONES

La transmisión de Datos de Carácter Personal a través de redes de telecomunicaciones se realizará cifrando dichos Datos o bien utilizando cualquier otro mecanismo que garantice que la información no sea inteligible ni manipulada por terceros durante la transmisión.

CAPÍTULO III

APLICACIÓN DE LAS MEDIDAS DE SEGURIDAD EN SUPUESTOS ESPECIALES

ART. 32.- ACCESO A DATOS A TRAVÉS DE REDES DE COMUNICACIONES

Las medidas de seguridad exigibles a los accesos a Datos de Carácter Personal a través de redes de comunicaciones, deberán garantizar un nivel de seguridad equivalente al correspondiente a los accesos en modo local.

ART. 33.- RÉGIMEN DE TRABAJO FUERA DE LOS LOCALES DE LA UBICACIÓN DEL ARCHIVO

La ejecución de Tratamientos de Datos de Carácter Personal fuera de los locales de la ubicación del Archivo deberá ser autorizada expresamente por el Sujeto Regulado y, en todo caso, deberá garantizarse el nivel de seguridad correspondiente al tipo de Datos de Carácter Personal objeto de Tratamiento de acuerdo con lo previsto en el artículo 12 de esta Norma.

ART. 34.- ARCHIVOS TEMPORALES

34.1 Los Archivos temporales deberán cumplir el nivel de seguridad que les corresponda con arreglo a los criterios establecidos en el artículo 12 de esta Norma.

34.2 Todo archivo temporal será cancelado una vez que haya dejado de ser necesario para los fines que motivaron su creación.

TÍTULO V

DEBER DE SECRETO

ART. 35.- DEBER DE SECRETO

Los Sujetos Regulados y quienes intervengan en cualquier fase del Tratamiento de los Datos de Carácter Personal, están obligados al secreto respecto de los mismos y al deber de guardarlos, obligaciones que, en el caso de los segundos, subsistirán aun después de finalizar sus relaciones con el Sujeto Regulado.

TÍTULO VI

COMUNICACIÓN DE DATOS DE CARÁCTER PERSONAL

ART. 36.- CONSENTIMIENTO PARA LA COMUNICACIÓN DE DATOS

36.1 Sin perjuicio de las excepciones que se prevén en el artículo 37 siguiente, los Sujetos Regulados sólo podrán Comunicar a un tercero los Datos de Carácter Personal objeto de Tratamiento, cuando se cumplan los siguientes requisitos:

(a) La Comunicación se realice al objeto de cumplir fines directamente relacionados con las funciones legítimas del Sujeto Regulado cedente y del tercero cesionario; y

(b) Los Interesados consientan expresamente la Comunicación.

36.2 Al consentimiento exigido en el apartado 36.1 precedente le serán de aplicación los requisitos previstos en el artículo 7 de esta Norma.

Párrafo: En particular, pero sin limitación, será nulo el consentimiento para la Comunicación de los Datos de Carácter Personal a un tercero, cuando la información que se facilite al Interesado no le permita conocer la finalidad a que se destinarán los Datos cuya Comunicación se autoriza y el tipo de actividad de aquel a quien se pretenden comunicar.

ART. 37.- EXCEPCIONES AL CONSENTIMIENTO PARA LA COMUNICACIÓN

El consentimiento exigido en el artículo 36 anterior no será preciso en los siguientes supuestos que tendrán carácter taxativo:

(a) Cuando la presente Norma establezca que tal consentimiento no es preciso, siempre que se cumplan las condiciones previstas para tal supuesto;

(b) Cuando la Comunicación esté autorizada en una disposición normativa aplicable;

(c) Cuando la Comunicación que deba efectuarse responda al requerimiento de una autoridad judicial o administrativa competente que actué en el ejercicio de las funciones que tenga legítimamente atribuidas.

TÍTULO VII

ACCESO A DATOS POR CUENTA DE TERCEROS

ART. 38.- ACCESO A LOS DATOS POR CUENTA DE TERCEROS

38.1 No se considerará Comunicación de Datos, y no será aplicable lo previsto en el Título VI de esta Norma, el acceso por un Encargado del Tratamiento a los Datos de Carácter Personal del Sujeto Regulado siempre que se cumplan los siguientes requisitos:

(a) Dicho acceso sea necesario para la prestación de un servicio por el Encargado del Tratamiento al Sujeto Regulado; y

(b) La realización del Tratamiento por el Encargado del Tratamiento por cuenta del Sujeto Regulado, conste en un contrato de acuerdo con lo dispuesto en el artículo 39 siguiente.

38.2 Una vez cumplida la prestación contratada al Encargado del Tratamiento, los Datos de Carácter Personal deberán ser destruidos o devueltos al Sujeto Regulado, al igual que cualquier soporte o documentos en que conste algún Dato de Carácter Personal objeto del Tratamiento.

38.3 Los Sujetos Regulados, tales como Unidades de Registro o Proveedores de Servicios o Infraestructura de Soporte, podrán actuar como Encargados del Tratamiento de otros Sujetos Regulados que tengan el carácter de Responsables del Tratamiento, siempre y cuando tal actividad no infrinja lo dispuesto en otras disposiciones legales aplicables.

ART. 39.- CONTRATO ENTRE EL ENCARGADO DEL TRATAMIENTO Y EL SUJETO REGULADO

El Tratamiento a realizar el Encargado del Tratamiento por cuenta del Sujeto Regulado según lo previsto en el artículo 38 precedente, deberá constar en un contrato suscrito entre dicho Encargado y Sujeto Regulado que cumpla las siguientes características:

(a) Esté formalizado por escrito y contenga las firmas de todas las partes o sus representantes autorizados;

Párrafo: A los efectos de cumplir con lo previsto en esta letra (a) se admitirá la utilización de Documentos Digitales o Mensajes de Datos, siempre que éstos incluyan una Firma Digital soportada en un Certificado Digital tal que haga al contrato suscrito mediante dichos Documentos Digitales o Mensajes de Datos, funcionalmente equivalente a aquel formalizado en papel con firmas autógrafas de acuerdo con lo dispuesto en la Ley No. 126-02 y otras normas legales aplicables.

(b) Especifique de forma precisa las características de los servicios a realizar por el Encargado del Tratamiento, en particular, aquellos que se refieran al Tratamiento de los Datos de Carácter Personal por cuenta del Sujeto Regulado;

(c) Establezca que el Encargado del Tratamiento sólo tratará los Datos de Carácter Personal de acuerdo con las instrucciones del Sujeto Regulado contenidas en el contrato;

(d) Reconozca la responsabilidad del Sujeto Regulado ante los Interesados y el INDOTEL, en los términos previstos en el artículo 40 de esta Norma;

(e) regule que, salvo en el caso que se prevé en la letra (h) de este apartado, el Encargado del Tratamiento no revelará ni divulgará los Datos de Carácter Personal por ningún motivo distinto del cumplimiento de las instrucciones del Sujeto Regulado mencionadas en la letra (c) de este apartado;

(f) Regule que el Encargado del Tratamiento no llevará a cabo

ningún tipo de Tratamiento de los Datos de Carácter Personal que no se encuentre expresamente prevista en el contrato;

(g) Regule las medidas de seguridad que deberá aplicar el Encargado de Tratamiento al objeto de garantizar el cumplimiento de las medidas de seguridad exigidas para el Sujeto Regulado de acuerdo con lo dispuesto en el Título IV de esta Norma; y

(h) Prevea que en caso de que el Encargado del Tratamiento tenga que dar acceso a terceros subcontratistas a los Datos de Carácter Personal, será preciso que dicho acceso se regule en un contrato que:

(i) Cumpla los requisitos previstos en este artículo;

(ii) En ningún caso, permita realizar un Tratamiento de los Datos de Carácter Personal en condiciones menos restrictivas que las previstas en el contrato principal suscrito con entre el Sujeto Regulado y el Encargado del Tratamiento;

(iii) No otorgue a los subcontratistas mayores prerrogativas que las previstas en dicho contrato;

(iv) Deberá ser revisado y aprobado por el Sujeto Regulado de forma previa a su firma por el Encargado del Tratamiento.

ART. 40.- RESPONSABILIDAD DEL SUJETO REGULADO RESPECTO A ACTOS DEL ENCARGADO DEL TRATAMIENTO

El Sujeto Regulado será responsable ante los Interesados y el INDOTEL, de cualquier infracción que cometa el Encargado del Tratamiento en la realización del Tratamiento de los Datos de Carácter Personal a los que hubiera dado acceso el Sujeto Regulado, sin perjuicio de la posibilidad del Sujeto Regulado de repetir dicha responsabilidad al Encargado del Tratamiento, en caso de que corresponda.

TÍTULO VIII

TRANSFERENCIAS INTERNACIONALES DE DATOS DE CARÁCTER PERSONAL

ART. 41.- CONSENTIMIENTO PARA LA TRANSFERENCIA INTERNACIONAL

41.1 Sin perjuicio de las excepciones que se prevén en el artículo 42 siguiente, los Sujetos Regulados sólo podrán realizar Transferencias Internacionales de Datos de Carácter Personal, cuando los Interesados consientan expresamente tal Transferencia Internacional.

41.2 Al consentimiento exigido en el apartado 41.1 precedente le serán de aplicación los requisitos previstos en el artículo 7 de esta Norma.

Párrafo: En particular, pero sin limitación, será nulo el consentimiento para la Transferencia Internacional de Datos de Carácter Personal, cuando la información que se facilite al Interesado no

le permita conocer la finalidad que persigue la Transferencia Internacional y el país con destino al cual los Datos de Carácter Personal serán Transferidos.

ART. 42.- EXCEPCIONES AL CONSENTIMIENTO PARA LA TRANSFERENCIA INTERNACIONAL

42.1 El consentimiento exigido en el artículo 41 anterior no será preciso en los siguientes supuestos que tendrán carácter taxativo:

(a) Cuando la Transferencia Internacional esté autorizada en una disposición normativa de aplicación;

(b) Cuando la Transferencia Internacional de Datos de Carácter Personal resulte de la aplicación de Tratados o Convenios internacionales en los que sea parte República Dominicana;

(c) Cuando la Transferencia Internacional se haga a efectos de prestar o solicitar auxilio judicial internacional;

(d) Cuando la Transferencia Internacional sea necesaria para la prevención o para el diagnóstico médico, la prestación de asistencia sanitaria o tratamiento médico o la gestión de servicios sanitarios;

(e) Cuando se refiera a transferencias dinerarias o de créditos conforme a su legislación específica;

(f) Cuando la transferencia sea necesaria o legalmente exigida para la salvaguarda de un interés público;

Párrafo: A título meramente enunciativo y no limitativo, tendrá esta consideración la transferencia solicitada por una Administración fiscal o aduanera para el cumplimiento de sus competencias.

(g) Cuando la Transferencia Internacional sea precisa para el reconocimiento, ejercicio o defensa de un derecho en un proceso judicial;

(h) Cuando la Transferencia Internacional se efectúe, a petición de persona con interés legítimo, desde un Registro público y aquélla sea acorde con la finalidad del mismo;

(i) Cuando la Transferencia Internacional responda al requerimiento de una autoridad judicial o administrativa competente que actúe en el ejercicio de las funciones que tenga legítimamente atribuidas;

(j) Cuando la Transferencia Internacional se dirija a un destinatario situado en un Estado que haya sido expresamente declarado por el INDOTEL como país con un nivel de protección adecuado; y

Párrafo: El carácter adecuado del nivel de protección que ofrece el Estado de destino se evaluará por el INDOTEL atendiendo a

todas las circunstancias que concurran en dicho Estado. En particular, pero sin limitación, se tomarán en cuenta las normas de derecho, generales o sectoriales, vigentes en el Estado tercero de que se trate, así como las normas profesionales y las medidas de seguridad en vigor en dicho Estado.

(k) Previa autorización del INDOTEL, cuando, con independencia del Estado donde se ubique el destinatario, tal destinatario se haya comprometido contractualmente tanto frente al Sujeto Regulado que realice la Transferencia Internacional como ante el INDOTEL, a tratar los Datos de Carácter Personal conforme a lo dispuesto en la normativa aplicable de la República Dominicana (en particular, pero sin limitación, la presente Norma) y reconozca contractualmente facultad al INDOTEL para penalizar el incumplimiento de esta obligación en un importe igual al aplicable como sanción bajo dicha normativa. Tal contrato deberá suscribirse por escrito y someterse a la legislación y tribunales de la Republica Dominicana.

Párrafo I: Al objeto de aplicar la letra (k) anterior, aquel Sujeto Regulado que desee llevar a cabo la Transferencia Internacional deberá dirigirse, previamente, al INDOTEL y evidenciar documentalmente la existencia de dicho compromiso contractual, entregando al INDOTEL copia del mismo. Revisado el contenido de la documentación entregada, el INDOTEL procederá a autorizar o no la Transferencia Internacional, debiendo motivar su decisión en caso de ser negativa respecto a la autorización. Dicha decisión será recurrible en los términos previstos en la normativa de aplicación.

Párrafo II: Al objeto de valorar la procedencia o no de autorizar la Transferencia Internacional, el INDOTEL tomará en cuenta todas las circunstancias que concurran en la Transferencia Internacional. En particular, se tomará en consideración la naturaleza de los Datos de Carácter Personal, la finalidad y la duración del Tratamiento o de los Tratamientos previstos, el país de origen y el país de destino final, el contenido y forma de los compromisos contractuales asumidos por el destinatario, las posibilidades de ejecución por el INDOTEL en el Estado del destinatario de las penalizaciones en caso de incumplimiento del compromiso contractual por el destinatario, el historial de Tratamientos de Datos de Carácter Personal realizados por el destinatario, las normas de derecho, generales o sectoriales, vigentes en el Estado del destinatario así como las normas profesionales y las medidas de seguridad en vigor en dicho Estado.

TÍTULO IX

DERECHOS DE LOS INTERESADOS

ART. 43.- DERECHO DE ACCESO

43.1 Los Interesados tienen derecho a solicitar y obtener gratuitamente del Sujeto Regulado la siguiente información:

(a) Datos de Carácter Personal del Interesado que son sometidos a Tratamiento por el Encargado del Tratamiento;

(b) Origen de dichos Datos; y

(c) Comunicaciones realizadas o que se prevén hacer de los mismos.

43.2 La información mencionada en el apartado 43.1 podrá obtenerse mediante los siguientes procedimientos a elección del Interesado:

(a) La mera consulta de los Datos por medio de su visualización; o

(b) La indicación de los Datos que son objeto de tratamiento mediante escrito, copia, telecopia o fotocopia, certificada o no, en forma legible o inteligible, sin utilizar claves o códigos que requieran el uso de dispositivos mecánicos específicos.

43.3 El Sujeto Regulado tendrá la obligación de hacer efectivo el derecho de acceso del Interesado en el plazo de diez (10) días laborables a contar desde la recepción de la solicitud de acceso del Interesado.

43.4 El derecho de acceso a que se refiere este artículo sólo podrá ser ejercitado a intervalos no inferiores a seis (6) meses, salvo que el Interesado acredite un interés legítimo al efecto, en cuyo caso podrá ejercitarlo antes.

ART. 44.- DERECHO DE RECTIFICACIÓN Y CANCELACIÓN

44.1 Los Interesados tienen derecho a que sean rectificados o cancelados, en su caso, los Datos de Carácter Personal cuyo Tratamiento no se ajuste a lo dispuesto en la presente Norma y, en particular, cuando tales Datos resulten inexactos o incompletos.

44.2 Si los Datos rectificados o cancelados hubieran sido Comunicados previamente, el Sujeto Regulado deberá notificar la rectificación o cancelación efectuada a quien se hayan Comunicado, en el caso de que se mantenga el Tratamiento por este último, que deberá también proceder a la rectificación y cancelación siendo en todo caso el Sujeto Regulado responsable ante el INDOTEL y los Interesados en caso de que el cesionario no cancele dichos Datos de Carácter Personal, sin perjuicio de las responsabilidades que el Sujeto Regulado pueda repetir en tal cesionario, en su caso.

44.3 El Sujeto Regulado tendrá la obligación de hacer efectivo el derecho de rectificación o cancelación del Interesado en el plazo de quince (15) días laborables a contar desde la recepción de la solicitud de rectificación y/o cancelación del Interesado.

44.4 La cancelación por el Interesado de sus Datos de Carácter Personal no será de aplicación respecto del tratamiento de dichos Datos de Carácter Personal por el Sujeto Regulado a los exclusivos efectos de ejercitar aquellas acciones que en Derecho procediesen frente al Interesado o, en su caso, de defenderse ante las acciones ejercitadas por el

Interesado. Dichos Datos de Carácter Personal no podrán ser tratados por el Sujeto Regulado más que con la finalidad aquí señalada, siendo eficaz la cancelación respecto a cualquier tratamiento distinto del aquí expresamente mencionado.

ART. 45.- PROCEDIMIENTO DE EJERCICIO DE LOS DERECHOS DE ACCESO, RECTIFICACIÓN O CANCELACIÓN.

45.1 Al objeto de ejercitar los derechos de acceso, rectificación o cancelación, el Interesado deberá remitir al Sujeto Regulado, a la dirección que le hubiese proporcionado éste en cumplimiento de las obligaciones de información previstas en los artículos 4 o 5 de esta Norma, una solicitud escrita y firmada por el Interesado indicando, al menos, lo siguiente:

(a) Derecho o derechos que se ejercitan;

(b) Petición en que se concreta su solicitud;

(c) En el caso de ejercicio del derecho de rectificación, los Datos de Carácter Personal a rectificar;

(d) En el caso de ejercicio del derecho de cancelación, motivos por los que se solicita la cancelación;

(e) Domicilio a efectos de notificaciones;

Párrafo: A los efectos de cumplir con lo previsto en el apartado 45.1 anterior, se admitirá la utilización de Documentos Digitales o Mensajes de Datos, siempre que éstos cumplan los requisitos necesarios para ser funcionalmente equivalentes con una solicitud en papel firmada por el Interesado, de acuerdo con lo dispuesto en la Ley No. 126-02 y otras normas legales aplicables.

45.2 No se exigirá contraprestación alguna por el ejercicio de los derechos de acceso, rectificación o cancelación.

TÍTULO X

INSPECCIÓN Y SANCIÓN

CAPÍTULO I

INSPECCIÓN

ART. 46.- FACULTAD DE INSPECCIÓN

El INDOTEL ejercerá las facultades de inspección que le otorga la Ley No. 126-02; Reglamento de Aplicación y Normas Complementarias, respecto a la actividad de los Sujetos Regulados y el cumplimiento de las obligaciones previstas en la presente Norma.

CAPÍTULO II

FALTAS Y SANCIONES

ART. 47.- COMPETENCIA SANCIONADORA

47.1 El INDOTEL, en el ejercicio de sus competencias, podrá imponer, atendiendo a la naturaleza y la gravedad de la falta, las sanciones que se prevén en el artículo 49 de esta Norma a aquellos Sujetos Regulados que cometan las faltas previstas en el artículo 48.

ART. 48.- FALTAS

48.1 Las faltas a las obligaciones previstas en Norma se clasificarán en muy graves, graves y leves.

48.2 Serán faltas muy graves las siguientes:

(a) La Comunicación de Datos de Carácter Personal, fuera de los casos en que esté permitida;

(b) La Transferencia Internacional de Datos de Carácter Personal, fuera de los casos en que esté permitida;

(c) Recabar y Tratar los Datos de Carácter Personal especialmente protegidos a los que se refiere el artículo 9 de esta Norma, cuando no medie el consentimiento expreso y por escrito del Interesado y éste se requiera;

(d) La vulneración del deber de guardar secreto sobre los Datos de Carácter Personal especialmente protegidos; y

(e) No atender, u obstaculizar de forma sistemática, el ejercicio de los derechos de acceso, rectificación, cancelación cuando deba hacerse;

48.3 Serán faltas graves las siguientes:

(a) Proceder a la recogida de Datos de Carácter Personal sin recabar el consentimiento expreso de los Interesados, en los casos en que éste sea exigible;

(b) El impedimento o la obstaculización del ejercicio de los derechos de acceso y la negativa a facilitar la información que sea solicitada;

(c) Mantener Datos de Carácter Personal inexactos o no efectuar las rectificaciones o cancelaciones de los mismos que legalmente procedan cuando resulten afectados los derechos de los Interesados;

(d) La vulneración del deber de guardar secreto sobre los Datos de Carácter Personal incorporados a Archivos que contengan datos relativos servicios financieros o prestación de servicios de solvencia patrimonial y crédito;

(e) Mantener los Archivos, locales, programas o equipos que contengan Datos de Carácter Personal sin aplicar las medidas de seguridad exigidas en este Norma;

(f) No atender u obstaculizar el ejercicio de los derechos de acceso, rectificación, cancelación cuando no sea infracción muy grave;

(g) La obstrucción al ejercicio de la función inspectora del INDOTEL; e

(h) Incumplir el deber de información que requiere esta Norma cuando los Datos de Carácter Personal hayan sido recabados de fuente distinta del Interesado;

48.4 Serán faltas leves las siguientes:

(a) Proceder a la recogida de Datos de Carácter Personal directamente de los propios Interesados sin proporcionarles la información que señala el artículo 4 de la presente Norma;

(b) Incumplir el deber de secreto establecido en el artículo 35 de esta Norma, salvo cuando constituya Infracción grave;

(c) El incumplimiento de cualquiera de las obligaciones previstas en esta Norma, cuando dicho incumplimiento no se encuentre recogido de forma específica como infracción en el presente artículo.

ART. 49.- SANCIONES

El INDOTEL podrá imponer las siguientes sanciones especificadas en la Ley No. 126-02, a los Sujetos Regulados que comentan alguna de las faltas previstas en el artículo 48 de esta Norma:

(a) Amonestación;

(b) Multas hasta por el equivalente a dos mil (2,000) Salarios Mínimos mensuales. Los infractores multados podrán repetir contra quienes hubieran realizado los actos u omisiones que dieron lugar a la sanción;

(c) Suspender de inmediato todas o algunas de las actividades del infractor;

(d) Destituir en los cargos que ocupan en el Sujeto Regulado sancionado, a los administradores o empleados responsables. También se les prohibirá a los infractores trabajar en empresas similares por un término de hasta diez (10) años;

(e) Prohibir al Sujeto Regulado, prestar directa o indirectamente sus servicios por un término de hasta diez (10) años; y

(f) Revocación definitiva de la autorización del Sujeto Regulado para operar como tal, cuando la aplicación de las sanciones

anteriormente enumeradas no haya sido efectiva y se pretenda evitar perjuicios reales o potenciales a terceros.

ART. 50.- GRADUACIÓN DE LAS SANCIONES

Se impondrán las sanciones aquí previstas considerando:

(a) El carácter intencional o no de la acción u omisión constitutiva de la falta;

(b) La repercusión social de las mismas; y

(c) La reincidencia del infractor.

ART. 51.- INDEPENDENCIA DE LAS ACCIONES CIVILES O PENALES

Las sanciones administrativas a las que se refiere el presente Título serán de aplicación independientemente de la responsabilidad penal o civil en que pudieran incurrir los infractores.

ART. 52.- PROCEDIMIENTO PARA IMPONER SANCIONES

Una vez tomado conocimiento el INDOTEL de los hechos u omisiones presuntamente transgresores de la presente Norma, procederá de la siguiente manera:

(a) Comunicará por escrito al presunto infractor los hechos u omisiones que pudieren llegar a constituir una trasgresión a la Norma, estableciendo, fundamentada y motivadamente, las circunstancias de tiempo, lugar y modo, otorgándole un plazo no menor a cinco (5) días hábiles para que manifieste lo que a su derecho convenga y aporte las pruebas, informes, pericias, testimonios que estime pertinentes; y

(b) Transcurrido el plazo a que se refiere la letra (a) anterior, el INDOTEL emitirá la resolución que en derecho proceda, fundamentada y motivada, en un plazo de quince (15) días calendario.

ART. 53.- MEDIDAS CAUTELARES

53.1 Para los casos que se presuma que la falta puede ser calificada como muy grave, el INDOTEL podrá disponer la adopción de medidas cautelares tales como, la clausura provisional de las instalaciones o la suspensión provisional de la autorización e inscripción en el Registro de Entidades de Certificación; y podrá, en su caso, solicitar judicialmente la incautación provisional de equipos o aparatos.

53.2 Para los efectos de la clausura provisional y decomiso, el INDOTEL hará el requerimiento pertinente al juez que corresponda, transcribiéndose la resolución que autoriza tal medida, para que disponga el diligenciamiento correspondiente, autorizando la rotura de puertas y apoyo de la fuerza pública, en caso de ser necesario.

53.3 Los bienes y equipos que hayan sido incautados como producto de incautaciones y clausuras definitivas pasarán al patrimonio del INDOTEL.

53.4 Tratándose de delitos flagrantes, conforme al Código Penal, el INDOTEL podrá solicitar el apoyo de la fuerza pública y la intervención del Ministerio Público para la realización de su cometido.

TÍTULO XI

DISPOSICIONES FINALES Y DEROGATORIAS

ART. 54.- ENTRADA EN VIGENCIA

La presente Norma entrará en vigencia transcurridos seis (6) meses desde la fecha de su publicación en un periódico de circulación nacional, en la página Web y en el Boletín del INDOTEL.

ART. 55.- DISPOSICIÓN DEROGATORIA

La presente Norma deroga a todas las disposiciones de igual o inferior rango que se le sean contrarias.

TERCERO: 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 _____ 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 veintitrés (23) del mes de marzo del año dos mil seis (2006).

Firmados:

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

David A. Pérez Taveras
Miembro del Consejo Directivo

Leonel Melo Guerrero
Miembro del Consejo Directivo

Juan Antonio Delgado
Miembro del Consejo Directivo

José Alfredo Rizek V.
Director Ejecutivo
Secretario del Consejo Directivo