UNAPEC UNIVERSIDAD APEC	**UNIVERSIDADES DE APEC Y VALENCIA** **MAESTRÍA EN AUDITORÍA INTEGRAL Y CONTROL DE GESTIÓN** **6ª Cohorte**	VNIVERSITAT DE VALÈNCIA

Vicerrectoría de Estudios de Posgrado

Tesis de maestría para optar por el título de:
Maestría en Auditoría Integral y Control de Gestión

Título:

Guía y plan de auditoría interna para el cumplimiento en la Protección de Datos de Carácter Personal en empresas no financieras

Postulantes:

Juan Dorca Lithgow	**2015-3346**
Lisanny González Paulino	**2015-3354**
Beiker Paredes Santiago	**2015-3424**

Tutor(a):

Dra. Iara V. Tejada

Santo Domingo, Distrito Nacional

República Dominicana

JULIO 2017

RESUMEN

Este trabajo de investigación tiene como objeto la elaboración de una guía de implementación de un plan de auditoría interna bajo el enfoque COSO que permita a las empresas del sector no financiero cumplir con la Ley No. 172-13 de la República Dominicana en lo relativo a la protección de datos de carácter personal. El cuerpo del trabajo lo componen tres capítulos, un primer capítulo contentivo del Marco teórico conceptual, en el cual se analiza la legislación de la Ley Orgánica de Protección de Datos (LOPD) con un enfoque al control, cumplimiento y sanciones contemplados tanto en la República Dominicana como en la región Iberoamericana; así como los elementos de por qué utilizar el enfoque de control interno en la confección de un plan de auditoría interna en la actividad de protección de los datos personales. En el segundo capítulo se aborda el Análisis del nivel de conocimiento y nivel de implementación de la LOPD en empresas no financieras de la República Dominica y un tercer capítulo aportando una Guía de implementación de un plan de auditoría interna para la protección de datos de carácter personal con un enfoque COSO, el cual permitirá a las empresas no financieras adecuarse a cumplir con la Ley No. 172-13 y a la vez contar con un plan de auditoría interna que permita a la alta dirección verificar que la empresa cumple con lo dispuesto en la ley y en caso de que no lo hiciere, detectar la oportunidad para hacerlo.

ÍNDICE

LISTA DE GRÁFICOS

LISTA DE TABLAS

INTRODUCCIÓN

La privacidad es un derecho que le corresponde a toda persona y así lo reconocen en su Constitución países como España, Colombia, México y República Dominicana. Estos países cuentan con su respectiva ley destinada para la protección de datos de carácter personal llamadas Ley Orgánica de Protección de Datos de Carácter Personal (LOPD) y qué en la República Dominicana, país donde se desarrolla éste trabajo de investigación, es la Ley 172-13.

La Ley 172-13 fue promulgada por el Poder Ejecutivo el 15 de diciembre del 2013 con fecha de entrada en vigor seis meses luego de su promulgación el pasado 13 de junio del 2014. Esta ley deroga la Ley No. 288-05 que regulaba las Sociedades de Información Crediticia y de Protección al Titular de la Información y modifica cualquier otra ley o parte de ley en cuanto contradiga lo que aquí está estipulado.

El objeto de una LOPD en principio consiste básicamente en resguardar la privacidad de la data particular a los individuos con algunos matices propios a la regulación de cada país como se puede apreciar en los casos de España, Colombia, México comparados con nuestro país.

En España la Ley Orgánica 15/1999 de 13 de diciembre de Protección de Datos de Carácter Personal la cual tiene por objeto "garantizar y proteger, en lo que concierne al tratamiento de los datos personales, las libertades públicas y los derechos fundamentales de las personas físicas, y especialmente de su honor, intimidad y privacidad personal y familiar."

En Colombia la Ley Estatutaria 1581 del año 2012 y reglamentada parcialmente por el Decreto Nacional 1377 de 2013 la cual tiene por objeto "el desarrollar el derecho constitucional que tienen todas las personas a conocer, actualizar y rectificar las informaciones que se hayan recogido sobre ellas en bases de datos o archivos y los demás derechos, libertades y garantías constitucionales a que se refiere el artículo 15

de la Constitución Política; así como el derecho a la información consagrado en el artículo 20 de la misma."

En México la Ley Federal DOF 05-07-2010 de Protección de Datos Personal en Posesión de Particulares, aprobada por el Congreso de la Unión el 27 de abril de 2010 la cual tiene por objeto "la protección de los datos personales en posesión de los particulares, con la finalidad de regular su tratamiento legítimo, controlado e informado, a efecto de garantizar la privacidad y el derecho a la autodeterminación informativa de las personas."

En República Dominicana el objeto de la referida Ley 172-13 es "La protección integral de los datos personales asentados en archivos, registros públicos, bancos de datos u otros medios técnicos de tratamiento de datos destinados a dar informes, sean éstos públicos o privados, así como garantizar que no se lesione el derecho al honor y a la intimidad de las personas, y también facilitar el acceso a la información que sobre las mismas se registre, de conformidad a lo establecido en el Artículo 44 de la Constitución de la República Dominicana."

De los países mencionados anteriormente España es el que desde el año 1999 dispone de la LOPD y sobre esta ha implementado, desarrollado y crecido en procura de que se respete la privacidad, en el sentido más amplio de la palabra, a la que toda persona tiene derecho siempre que esté cubierta por la ley. La República Dominicana es la de más reciente promulgación en fecha 15 de diciembre del 2013.

En la República Dominicana a partir de la ley 172-13 se crea la Agencia Dominicana de Protección de Datos la cuál será, una vez sea puesta en operación, una entidad autónoma que tendrá como finalidad velar por las políticas en materia de protección de los datos de carácter personal y que estas sean cumplidas tanto por las entidades públicas y privadas.

La LOPD 172-13 se sustenta en principios fundamentales como son el de la licitud de los archivos de datos personales, la calidad de los datos, el derecho de información, el consentimiento del afectado, la seguridad de datos, el deber de secreto, la lealtad y la finalidad de los datos.

En este mismo orden, la LOPD de la República Dominicana consigna el derecho al Habeas Data que es el derecho constitucional que tienen todas las personas de poder conocer, actualizar y rectificar los datos que sobre ellas se hayan recopilado en las bases de datos o archivos de las diferentes entidades públicas y privadas.

Las empresas del sector financiero, un sector altamente regulado y donde los datos personales de clientes son resguardados para evitar el acceso a personas no deseadas, cumplen con la LOPD. No así las empresas que no pertenecen a este sector y que también recolectan datos sensibles de carácter personal de los clientes. Es por esto que el trabajo de investigación que aquí se desarrolla parte del pensamiento de cómo afecta a los clientes el que las empresas que no pertenecen al sector financiero y con las que mantienen algún tipo de relación comercial, contractual, etc., no protegiesen adecuadamente los datos de carácter personal. Así mismo las consecuencias que acarrea a las empresas no financieras el no cumplimiento de las leyes que para estos fines existen.

El objetivo general de este trabajo de investigación es desarrollar un plan de auditoría interna que le permita a los directivos de una empresa no financiera validar el cumplimiento de la Ley Orgánica de Protección de Datos de Carácter Personal 172-13 de la República Dominicana luego de que ésta ha adecuado sus procesos al cumplimiento de la referida ley. Para lograr el fin propuesto se desarrollaron tres objetivos específicos los cuales fueron: (a) analizar como regula el gobierno de la República Dominicana la protección de los datos personales en las empresas no financieras versus otros países; (b) analizar la viabilidad de un enfoque de control interno en las empresas no financieras en la actividad de protección de los datos personales recabados de sus clientes y por último, (c) recomendar un plan de auditoría interna para la protección de los datos de carácter personal de clientes que pueda ser replicado en empresas no financieras.

La investigación se desarrolló empleando un enfoque cualitativo debido al estudio a profundidad de leyes, reglamentos y enfoques de ambiente de control que de manera directa o indirecta inciden en el tema en cuestión. Se emplearon métodos empíricos para conocimiento de hechos fundamentales, tales como análisis de

documentos, encuestas aplicadas a personal que labora en las empresas y análisis de la actividad en cuestión.

El trabajo de investigación consta de tres (3) capítulos: el Capítulo I - Marco teórico conceptual resumiendo la Ley orgánica de protección de datos (LOPD) en la República Dominicana y en la región de Iberoamérica; el Capítulo II el cual resume el Análisis del nivel de conocimiento y nivel de implementación de la LOPD en empresas no financieras en la República Dominicana y el Capítulo III el cual contiene la Guía de implementación de un plan de auditoría interna para la protección de datos de carácter personal con un enfoque COSO.

De manera detallada, el capítulo I tiene como finalidad el presentar la teoría, los fundamentos, el origen, entre otros., detrás de una LOPD así como también el enfoque de control interno como herramienta para el desarrollo de un plan de auditoría interna dirigido al cumplimiento de la LOPD. Se divide en cuatro secciones (1.1) Definición de Ley Orgánica de Protección de Datos (LOPD): (1.2) Legislación de la LOPD en República Dominicana; (1.3) Legislación de la LOPD en la región Iberoamericana; (1.4) Control, cumplimiento y sanciones contemplados en la Ley 172-13 comparado con países de la región Iberoamericana y (1.5) Enfoque de control internos en el desarrollo de un plan de auditoría interna en la actividad de protección de los datos personales.

En el capítulo II, el Análisis del nivel de conocimiento y nivel de implementación de la LOPD en empresas no financieras en la República Dominicana, busca mediante la aplicación de encuestas, dar una referencia de como en materia de protección de los datos de carácter personal de los clientes las empresas dominicanas no pertenecientes al sector financiero se encuentran.

Se provee en el capítulo III, la Guía de implementación de un plan de auditoría interna para la protección de datos de carácter personal con un enfoque COSO, el cual dotará a las empresas del sector no financiero de una herramienta de autoevaluación que les permitirá identificar el nivel de cumplimiento y riesgo que poseen para con lo estipulado en la Ley 172-13, un guía para adecuar la empresa al cumplimiento de la ley y por último de un plan de auditoría interna para verificar dicho cumplimiento.

Capítulo I – Ley orgánica de protección de datos en República Dominicana y la región Iberoamericana.

El objetivo de este capítulo es el dotar al lector, de manera resumida y sencilla, del conocimiento sobre el rol que la ley orgánica de protección de datos de carácter personal tiene en la República Dominicana y demás naciones que componen la región Iberoamericana.

1.1 Definición de Ley Orgánica de Protección de Datos (LOPD).

A partir de la revisión de los diferentes objetos de leyes orgánicas de protección de datos de la región iberoamericana, se define la misma como una normativa jurídica orientada a proteger todo lo relativo a las informaciones de carácter personal de cada persona frente al riesgo que supone el manejo y uso inadecuado de sus datos personales, sean estos recopilados en forma manual o aparatos tecnológicos. En virtud de esto la ley orgánica de protección de datos regula la obligación del tratamiento adecuado que deben darles las instituciones públicas y privadas de un país a los datos personales que manejan de terceros, garantizando la seguridad de los datos.

Las LOPD son de alcance territorial para cada país y es de cumplimiento obligatorio para todas las personas, organismos y entidades públicas y privadas que dispongan en sus archivos de informaciones de carácter personal. La LOPD obliga a cada entidad del país a cumplir con una serie de requisitos y aplicar ciertas medidas de seguridad en función de los tipos de datos que posean, que garanticen la seguridad e integridad de los mismos.

El contenido de una LOPD se sustenta en algunos de los principios constitucionales de cada país, sobre el derecho a la privacidad de los datos personales con la que goza cada ciudadano. El objetivo fundamental es garantizar que las informaciones personales de cada individuo independientemente de su formación o estatus, no estén al alcance de cualquier persona o institución sin previa autorización

del ciudadano. Entiéndase como informaciones personales todas aquellas que forman parte de su vida privada y que pueden ser utilizadas para analizar y determinar ciertos aspectos de su personalidad con la intensión de cometer dolo. Las LOPD buscan proteger el honor y la integridad personal y familiar de cada individuo, estableciendo las reglas y pautas que deben seguir las instituciones para garantizar la seguridad y protección de los datos y que estos no sean sustraídos de forma voluntaria o involuntaria por personas que puedan hacer mal uso de la información.

Así como la ley orgánica de protección de datos busca proteger los datos de carácter personal y establece los lineamientos que deben seguir las personas, organizaciones y entidades que manejen informaciones personales, la LOPD también establece los derechos que tienen las personas sobre sus datos como son los de poder acceder, corregir y cancelarlos en cualquier archivo o base de datos que se encuentren. Este derecho es también conocido como el derecho de habeas data.

Por lo visto anteriormente se concluye que el objeto de una ley orgánica de protección de datos en principio es básicamente el mismo, con algunos matices propios de cada país.

1.2 Legislación de la LOPD en República Dominicana.

La República Dominicana cuenta con la ley 172-13, que fue promulgada por el poder ejecutivo el 15 de diciembre del 2013, con fecha de entrada en vigor seis meses luego de su promulgación el pasado 13 de junio del 2014. Esta ley deroga la Ley No. 288-05 que regulaba las Sociedades de Información Crediticia y de Protección al Titular de la Información y modifica cualquier otra ley o parte de ley en cuanto contradiga lo que aquí está estipulado.

Esta es la normativa jurídica que regula y tiene por objeto "La protección integral de los datos personales asentados en archivos, registros públicos, bancos de datos u otros medios técnicos de tratamiento de datos destinados a dar informes, sean éstos públicos o privados, así como garantizar que no se lesione el derecho al honor y a la

intimidad de las personas, y también facilitar el acceso a la información que sobre las mismas se registre". (Ley No. 172-13).

Del mismo modo, esta normativa regula "la constitución, organización, actividades, funcionamiento y extinción de las Sociedades de Información Crediticia (SIC), así como la prestación de los servicios de referencias crediticias y el suministro de la información en el mercado, garantizando el respeto a la privacidad y los derechos de los titulares de la misma, promoviendo la veracidad, la precisión, la actualización efectiva, la confidencialidad y el uso apropiado de dicha información". (Ley No. 172-13).

Esta normativa toma en consideración la declaración universal de derechos humanos, así como los puntos establecidos en el art. 44 de la constitución de la República Dominicana sobre el derecho a la intimidad y el honor que cada persona tiene que se le respete su vida privada, familiar, su hogar y sus correspondencias. Se entiende por intimidad el ámbito privado de la vida de una persona y se entiende por derecho el poder de decisión que tiene dicha persona de decidir sobre la utilización y prohibición de sus datos personales, así como la divulgación en lo concerniente a las informaciones de situaciones que se generen en este ámbito.

La LOPD 172-13 se sustenta en principios fundamentales como son el de la licitud de los archivos de datos personales, la calidad de los datos, el derecho de información, el consentimiento del afectado, la seguridad de datos, el deber de secreto, la lealtad y la finalidad de los datos. En este sentido la LOPD de la República Dominicana consigna el derecho al Habeas Data que es el derecho constitucional que tienen todas las personas de poder conocer, actualizar y rectificar los datos que sobre ellas se hayan recopilado en las bases de datos o archivos de las diferentes entidades públicas y privadas

Esta ley que tiene el objetivo de garantizar que no se lesione el art. 44 de la constitución, es de alcance a todo el territorio dominicano y de aplicación a todas las instituciones públicas y privadas que estén relacionada a la recepción de datos de carácter personal. Como apoyo a esta iniciativa a partir de la ley 172-13 se crea la Agencia Dominicana de Protección de Datos, la cuál será, una vez sea puesta en

operación, una entidad autónoma que tendrá como finalidad velar por las políticas en materia de protección de los datos de carácter personal y que estas sean cumplidas tanto por las entidades públicas y privadas.

Los principios de la LOPD de República Dominicana se fundamentan en que los archivos de datos personales que mantengan las instituciones públicas y privadas no pueden tener fines contrarios a lo establecido en la ley y que los mismos deben apegarse a los principios de calidad que se fundamentan en la veracidad de la información. Desde la solicitud de un reporte o consulta de los datos personales por parte de las entidades dominicana públicas o privadas, hasta la recepción de datos recibido por parte de la persona, estas instituciones están obligadas a contar con la aprobación del titular e informar a este sobre la finalidad y el uso que les darán a sus datos y cuáles pueden ser sus destinatarios, dicha autorización debe ser por escrito y guardada por un periodo de 6 meses de acuerdo a la ley 172-13.

La legislación dominicana de LOPD establece que las empresas deben contar con los controles necesarios que mitiguen los riesgos de que los datos personales sean susceptibles de alteraciones, robos, acceso no autorizado, perdidas y que brinden al usuario la seguridad de que sus datos no serán violados, la normativa prohíbe el registro de datos personales en cualquier archivo o registros que no logren mitigar estos riesgos, así como establece la adopción de un manual interno de políticas y procedimientos que garanticen a la entidad el fiel cumplimiento de la LOPD dominicana.

La LOPD de República Dominicana establece que toda persona tiene el derecho a acceder, rectificar, y de ser necesario suprimir sus datos personales de cualquier institución. Para estos fines el responsable a cargo de los datos tiene un plazo de 10 días hábiles para proceder con la solicitud sea cual fuere. De ser una rectificación de los datos y se deba transferir la información, la entidad cuenta con 5 días hábiles para notificar la actualización de los datos en el sistema.

Del mismo modo la LOPD dominicana presenta que los derechos de acceso, rectificar, cancelar o poner oposición a los datos personales, son independiente uno de otros y no están sujeto entre sí para su aplicación. La única forma en que la

entidad pública o privada puede negarse a cualquier solicitud realizada por el titular de los datos es mediante una resolución judicial que ampare esta negación o cuando estas solicitudes puedan obstaculizar un proceso judicial o administrativo en curso.

Las personas en República Dominicana de acuerdo a la ley orgánica de protección de datos tienen el derecho de acceder a las informaciones de las bases de datos públicas y privadas que contengan datos personales sobre ellos o sobre sus bienes, esta ley le otorga el derecho de poder solicitar a la SIC (sociedad de información crediticia) su historial crediticio no más de 4 veces al año de forma gratuita en un intervalo no menor a 3 meses.

Las empresas del sector financiero, un sector altamente regulado por la Superintendencia de Bancos y donde los datos personales de clientes son altamente resguardados para evitar el acceso a personas no deseadas, cumplen con la LOPD. No así consta para las empresas que no pertenecen a este sector y que también recolectan datos de carácter personal sensibles de los clientes.

Esta ley no es de aplicación para las personas físicas que mantengan archivos de personas que realicen actividades domésticas o personales, tampoco es de aplicación para los organismos de investigación e inteligencia de la República Dominicana, a los archivos de personas fallecidas (cualquier derecho sobre las personas fallecidas recae sobre sus sucesores universales) y ni a los datos suministrados a personas jurídicas en calidad de empleado o prestador de servicio.

Algunos conceptos que se definen en la Ley 172-13 y que se consideran oportunos, para un mejor entendimiento, se listan a continuación:

Afectado o interesado: "Toda persona física cuyas informaciones sean objeto del tratamiento, así como todo acreedor, sea éste una persona física o jurídica, que tiene o ha tenido una relación comercial o de tipo contractual con una persona física para el intercambio de bienes y servicios, donde la persona física es deudora del acreedor".

Archivo de datos personales: "Conjunto organizado de datos de carácter personal, que sean objeto de tratamiento o procesamiento, automatizado o no,

cualquiera que fuere la forma o modalidad de su creación, almacenamiento, organización y acceso".

Archivos de datos de titularidad privada: "Son aquellos archivos de datos personales de los que sean responsables las personas, empresas o entidades de derecho privado, con independencia de quien ostente la titularidad de su capital o de la procedencia de sus recursos económicos, así como los archivos de los que sean responsable las corporaciones de derecho público".

Archivos de titularidad pública: "Son aquellos archivos de datos personales de los que sean responsables los órganos de la administración pública, así como las entidades u organismos vinculados o dependientes de la misma y las entidades autónomas y descentralizadas del Estado".

Cesión o comunicación de datos: "Tratamiento de datos que supone su revelación a una persona distinta del afectado o interesado".

Consentimiento del interesado: "Toda manifestación de voluntad, libre, inequívoca, específica e informada, mediante la que el interesado consiente el tratamiento de datos personales que le conciernen".

Datos especialmente protegidos: "Datos de carácter personal que revelan origen racial y étnico, opiniones políticas, convicciones religiosas, filosóficas o morales, afiliación sindical e información referente a la salud o a la vida sexual".

Datos de carácter personal: "Cualquier información numérica, alfabética, gráfica, fotográfica, acústica o de cualquier otro tipo concerniente a personas físicas identificadas o identificables".

Destinatario o cesionario: "Persona física o jurídica, pública o privada, u órgano administrativo, al que se revelen los datos".

Tercero: "Persona física o jurídica, pública o privada, u órgano administrativo distinto del afectado o interesado, del responsable del tratamiento, del responsable del fichero, del encargado del tratamiento y de las personas autorizadas para tratar los

datos bajo la autoridad directa del responsable del tratamiento o del encargado del tratamiento".

Agentes económicos: "Personas físicas o jurídicas, proveedores de bienes y servicios".

Archivo, registro, ficheros, base o banco de datos: "Indistintamente, designan al conjunto organizado de datos personales que sean objeto de tratamiento o procesamiento, electrónico o no, cualquiera que fuere la modalidad de su formación, almacenamiento, organización o acceso. Incluye también el conjunto de informaciones que proporcionan directamente los aportantes de datos, así como otras informaciones de carácter y dominio público, ya sea por su procedencia o por su naturaleza".

Cedente: "Entidad que cede o transfiere información".

Datos informáticos: "Los datos personales sometidos al tratamiento o procesamiento electrónico o automatizado".

Datos sensibles: "Datos personales que revelan las opiniones políticas, las convicciones religiosas, filosóficas o morales, la afiliación sindical e información referente a la salud o a la vida sexual".

Responsable de archivo, registro, base o banco de datos: "Persona física o jurídica, pública o privada, que es titular de un archivo, registro, base o banco de datos".

1.3 Legislación de la LOPD en la región Iberoamericana.

Los países que para fines de este trabajo engloban lo que se denomina la región Iberoamericana lo conforman el Principado de Andorra, Argentina, Bolivia, Brasil, Chile, Colombia, República de Costa Rica, Ecuador, República de el Salvador, Reino de España, República de Guatemala, República de Haití, República de Honduras, México, República de Nicaragua, República de Panamá, República del Paraguay, República del Perú, República Portuguesa, Uruguay, República Bolivariana de

Venezuela y la República Dominicana. Sobre cada uno de estos países se presentará más adelante, en esta sección, lo que en materia de protección de datos de carácter personal han avanzado, de cómo es consignado este derecho en la Constitución de cada uno de esos países, las legislaciones tanto general como sectorial con las que cuentan y finalmente todo resumido en la Tabla No. 1. La región Iberoamérica cuenta con la Red Iberoamericana de Protección de Datos (RIPD) que reúne a todos los países aquí mencionados y que surge como una iniciativa del acuerdo alcanzado en el Encuentro Iberoamericano de Protección de Datos (EIPD) el cual se celebró en La Antigua ciudad de Guatemala en el mes de junio de 2003. Este encuentro contó con la participación de 14 países iberoamericanos. (Red Iberoamericana de Protección de Datos).

La RIPD, desde su origen contó con el apoyo de los Jefes de Estado y de Gobierno los cuales en la Cumbre celebrada en Bolivia en noviembre de 2003 así lo determinaron. Conscientes de la responsabilidad, importancia y derecho fundamental de la protección de datos personales, así como también de las iniciativas regulatorias de proteger la privacidad de los ciudadanos crean este foro integrador de los diferentes participantes tanto del sector público como privado donde se comparten experiencias y se desarrollan iniciativas relacionadas con la protección de datos personales para la región iberoamericana. Desde esta Red, en los aproximadamente 10 años con los que cuenta, ha promovido varios encuentros y seminarios sobre temas relacionados con el fraude en el sector financiero, sector comercial, en la lucha contra el Spam, nuevas tecnologías y el impacto que representa en la privacidad y transferencias internacionales. Países como Argentina (Ley 25326/2008); Uruguay (Ley 18.331/2008); Perú (Ley 29733/2011); Costa Rica (Ley 8968/2011); Nicaragua (Ley 787/2012), Colombia (Ley 1581/2012) y ahora se añade a este listado la República Dominicana, que ha sido la última en incorporarse al grupo de países que disponen de una normativa específica en esta materia la cuál es la Ley 172 del 15 de diciembre del 2013.

El **Principado de Andorra** en el Artículo 14 de su Constitución establece que "Se garantiza el derecho a la intimidad, al honor y a la propia imagen. Toda persona

tiene derecho a ser protegida por las leyes contra las intromisiones ilegitimidades en su vida privada y familiar". En este mismo orden cuenta con la legislación general Calificada de Protección de Datos Personales (Llei 15 del 18 de diciembre del 2003) y los decretos 9/6/2010 así como el 1/7/2004 el primero de aprobación del Reglamento de la Agencia Andorrana de Protección de Datos y el segundo, de aprobación del Reglamento del Registro de inscripción de los ficheros de datos personales.

Bolivia, en su Constitución establece en tres de sus Artículos el derecho que los ciudadanos de su país tienen a la privacidad y en dos de ellos además del derecho que si tienen el cuándo y por cuáles razones lo pueden perder. El primero es el Artículo 21.2 que establece "Las bolivianas y los bolivianos tienen los siguientes derechos: a la privacidad, intimidad, honra, propia imagen y dignidad". En su Artículo 130 establece que "I. Toda persona individual o colectiva que crea estar indebida o ilegalmente impedida de conocer, objetar la eliminación o rectificación de los datos registrados por cualquier medio físico, electrónico, magnético o informático, en archivos o bancos de datos públicos o privados, o que afecten a su derecho fundamental a la intimidad y privacidad personal o familiar, o a su propia imagen, honra y reputación, podrá interponer la Acción de Protección de Privacidad". "II. La acción de Protección de Privacidad no procederá para levantar el secreto en materia de prensa". En el Artículo 131 establece también que "La acción de Protección de Privacidad tendrá lugar de acuerdo con el procedimiento previsto para la acción de Amparo Constitucional". "II. Si el tribunal o juez competente declara procedente la acción, ordenará la revelación, eliminación o rectificación de los datos cuyo registro fue impugnado". "III. La decisión se elevará de oficio, en revisión ante el Tribunal Constitucional Plurinacional en el plazo de las veinticuatro horas siguientes a la emisión del fallo, sin que por ellos se suspenda la ejecución". Por último, en este Artículo 131, "IV. La decisión final que conceda la Acción de Protección de Privacidad será ejecutada inmediatamente y sin observación. En caso de resistencia se procederá de acuerdo con lo señalado en la Acción de Libertad. La autoridad judicial que no proceda confirme lo dispuesto por este artículo quedará sujeta a sanciones previstas por la Ley".

Brasil, en el Artículo 5 de su Constitución establece que "Se concederá habeas data: a) para asegurar el conocimiento de informaciones relativas a la persona del impetrante que conste en registros o bancos de datos de entidades gubernamentales o de carácter público; b) para la rectificación de datos, cuando no se prefiera hacerlo por procedimiento secreto, judicial o administrativo". En este mismo orden, en este Artículo también establece que "son gratuitas las acciones de habeas corpus y habeas data y, en la forma de la ley, los actos necesarios al ejercicio de la ciudadanía". No cuentan con una legislación general, pero si con legislaciones sectoriales que reglamentan la interceptación de comunicaciones telefónicas, otra del derecho de acceso a la información y reglamenta el "habeas data", otra legislación a nivel del Código Penal relacionada con la de violación del domicilio, de correspondencia, de comunicación telefónica, divulgación de secreto, violación del secreto profesional, una Ley Complementaria de secreto de las operaciones de instituciones financieras y por último la Ley del código de protección y defensa del consumidor.

Chile, en su Artículo 19.4 de la Constitución establece que "La constitución asegura a todas las personas: El respeto y protección a la vida privada y pública y a la honra de la persona y de su familia". Su legislación general es la Ley 19.628 de protección a la vida privada la cuál data del 28 de agosto de 1999 y que ha sufrido modificaciones en los años 2002, 2010, 2011 y 2012. En este mismo orden cuentan con el decreto 779/2000 el cual regula el registro de bancos de datos personales a cargo de los organismos públicos. Al nivel de legislaciones sectoriales cuentan con varias leyes que en algunos de sus artículos tocan el tema relativo a la protección de los datos de las personas como son: a) Relativa a delitos informáticos; b) Protección a los derechos de los consumidores; c) Ámbito sanitario; d) Material laboral y e) Materia financiera y crediticia.

Ecuador, en su Constitución en los Artículos 11, 66 y 92 consignan aspectos tales como el deber del Estado en respetar y hacer respetar los derechos garantizado en la Constitución, el derecho a la protección de datos de carácter personal, el derecho a la intimidad personal y familiar y el derecho a la inviolabilidad y al secreto de la correspondencia física y virtual. El país no cuenta con una legislación general,

pero si con varias legislaciones sectoriales, la del sistema de registros de datos públicos, la de burós de información crediticia, la de comercio electrónico, firmas y mensajes de datos, la ley orgánica de transparencia y acceso a la información pública, la ley especial de telecomunicaciones, la ley de burós de información crediticia y la ley orgánica de transparencia y acceso a la información.

República del Salvador, establece en el Artículo 2 de su Constitución que "Toda persona tiene derecho a la vida, a la integridad física y moral, a la libertad, a la seguridad, al trabajo, a la propiedad y posesión, y a ser protegida en la conservación y defensa de los mismos. Se garantiza el derecho al honor, a la intimidad personal y familiar y a la propia imagen. Actualmente no cuentan con una legislación general, pero si de legislaciones sectoriales como es la ley de acceso a la información pública, el reglamento de la ley de acceso a la información pública, la ley de regulación de los servicios de información sobre el historial de crédito de las personas, la ley de protección al consumidor y la ley de telecomunicaciones y energía. En este mismo orden el Código Penal legisla en relación a los delitos relativos a la intimidad,

Reino de España, establece en su Constitución, en el Artículo 18 que "4. La ley limitará el uso de la informática para garantizar el honor y la intimidad personal y familiar de los ciudadanos y el pleno ejercicio de sus derechos". Su legislación general está conformada por la ley orgánica 15/1999 de protección de datos de carácter personal y el real decreto 1720/2007 de Desarrollo de la ley orgánica de protección de datos de carácter personal. Disponen de legislaciones sectoriales dirigidas a la transparencia como es la ley de acceso a la información pública de buen Gobierno, la ley a los servicios de la sociedad información y comercio electrónico, la ley general de telecomunicaciones, la ley de firma electrónica, la ley básica reguladora de la autonomía del paciente y de derechos y obligaciones en materia de información y documentación clínica, la ley de función estadística pública, la ley contra el terrorismo y blanqueo de capitales y la ley sobre el régimen jurídico de los movimientos de capitales y de las transacciones económicas con el exterior y medidas de prevención del blanqueo de capitales.

Guatemala, establece en su Constitución en el Artículo 24 la "Inviolabilidad de correspondencia, documentos y libros. Se garantiza el secreto de la correspondencia y de las comunicaciones telefónicas, radiofónicas, cablegráficas y otros productos de la tecnología moderna. En el Artículo 30 "Publicidad de los actos administrativos" y por último, en el Artículo 31 en lo relativo a "Acceso a archivos y registros estatales, así como a corrección, rectificación y actualización. Quedan prohibidos los registros y archivos de filiación política, excepto los propios de las autoridades electorales y de los partidos políticos". No cuentan con una legislación general, aunque sí disponen de legislaciones sectoriales como es la ley de acceso a la información pública, la ley de protección al consumidor y usuario, la ley para el reconocimiento de las comunicaciones y firmas electrónicas y la ley de derecho de autor y derechos conexos.

República de Honduras, establece en el Artículo 76 de su Constitución que "Se garantiza el derecho al honor, la intimidad personal, familiar y a la propia imagen". Posteriormente, en el año 2005 reformaron mediante el decreto legislativo 381 el Título IV del Capítulo 1 de la Constitución reconociendo la garantía del Habeas Data que es "Que toda persona tiene el derecho a acceder a la información sobre si misma o sus bienes en forma expedita y no onerosa, ya esté contenida en bases de datos, registros públicos o privados y, en el caso de que fuere necesario, actualizarla, rectificarla y/o enmendarla." No cuentan con una legislación general para estos fines y en legislación sectorial, que esté dirigido al tema en cuestión, solo disponen de la ley de transparencia y acceso a la información pública que en tres de sus Artículos se refiere específicamente al tema. En su Artículo 23 donde trata lo relativo al Hábeas Data, el Artículo 24 lo relativo a la sistematización de los archivos personales y su acceso y por último el Artículo 25 en lo que concierne a la prohibición de la entrega de la información.

México, tres Artículos de su Constitución se dedican al tema de privacidad y protección de los datos personales de las personas. El Artículo 6 establece "La información que se refiere a la vida privada y los datos personales será protegida en los términos y con las excepciones que fijen las leyes". En el Artículo 16 establecen

que “Nadie puede ser molestado en su persona, familia, domicilio, papeles o posesiones, sino en virtud de mandamiento escrito de la autoridad competente, que funde y motive la causa legal del procedimiento”. Por último, en Artículo 73 indica que dentro de las facultades del Congreso está la de legislar en materia de protección de los datos de personales que estén en posesión de terceros. Disponen de varias normas generales tanto en el ámbito Federal como en el de los Estados y de normas sectoriales también. Los detalles de estas normas se podrán ver en la Tabla#1 que más adelante se presenta.

República de Panamá, establece en su Constitución en el Artículo 29 que “La correspondencia y demás documentos privados son inviolables y no pueden ser ocupados o examinados sino por disposición de autoridad competente, para fines específicos y mediante formalidades legales”. En este mismo orden, en sus Artículos del 42 al 44 desarrolla sobre el tema de derecho de acceso a la información. No disponen de Normas Generales, aunque sí de Normas Sectoriales como son la de transparencia y acceso a la información pública que establece acción de Habeas Data en algunos de sus artículos, la ley que regula el servicio de información sobre el historial de crédito y la ley general sobre las infecciones de transmisión sexual, el virus de la inmunodeficiencia humana y el sida.

República del Paraguay, establece en los Artículos 33 y 135 de su Constitución el derecho de las personas a la intimidad y del Hábeas Data respectivamente. No disponen de una legislación general para estos fines, pero si de varias legislaciones sectoriales como la que reglamenta la información de carácter privado, la de validez jurídica de la firma electrónica, la firma digital, mensaje de datos y expediente electrónico. Así mismo, la que legisla en lo relativo al comercio electrónico.

República Portuguesa, establece en su Artículo 35 de la Constitución lo relativo a la utilización de la informática en lo relativo a los derechos de los ciudadanos, al concepto de los datos personales, al límite en la utilización de la informática, a la prohibición en el acceso a los datos personales con excepción de los casos que la ley si lo establezca entre otros. Cuenta con una norma general, la ley de protección de datos personales y de varias normas sectoriales en los sectores de comunicación

electrónica, salud, crimen cibernético, trabajo, identificación civil y criminal, así como también en el sector judicial.

Venezuela, en su Constitución establece el derecho de las personas de acceder a la información y a los datos que sobre si misma o sus bienes se posea en registros oficiales o privados (Artículo 28), al derecho que toda persona tiene a su intimidad, honor, vida privada, confidencialidad entre otros (Artículo 60) y las atribuciones del llamado Defensor del pueblo que tiene el poder de interponer acciones de inconstitucionalidad, habeas data y otras acciones que le son conferida por la ley. No disponen de una norma general, aunque si de varias sectoriales como es la ley de registro de antecedentes penales, la ley sobre protección a la privacidad de las comunicaciones, la ley orgánica para la protección del niño y del adolescente y la ley especial contra delitos informáticos.

Argentina, en el Artículo 43 de su Constitución establece que "Toda persona podrá interponer acción para tomar conocimiento de los datos a ella referidos y de su finalidad, que conste en registro o bancos públicos, o privados destinados a proveer informes, y en caso de falsedad o discriminación, para exigir la supresión, rectificación, confidencialidad o actualización de aquellos. No podrá afectarse el secreto de las fuentes de información periodística. Cuenta con la norma general de protección de datos no así nos consta que en este país cuenten normas sectoriales.

Uruguay, cinco Artículos de la Constitución tocan el tema de la protección de datos. El Artículo 7 "Los habitantes de la República tienen derecho a ser protegidos en el goce de su vida, honor, libertad, seguridad, trabajo y propiedad". En el Artículo 11 en lo relativo al hogar y como éste se considera como un lugar sagrado. El Artículo 28 trata sobre la inviolabilidad de la correspondencia, el Artículo 72 donde enfatiza que además de los derechos y garantías establecidas en la Constitución no se excluyen los inherentes a la personalidad humana o que se derivan de la forma del gobierno y el Artículo 332 donde se reconocen derechos a los individuos, así como los que atribuyen facultades e imponen deberes a las autoridades públicas. Cuentan con una legislación general de protección de datos personales y acción Habeas Data, y varias legislaciones en el ámbito sectorial como son la ley limitante relativa a la

normativa sobre secreto, la ley de intermediación financiera, ley del código de la niñez y la adolescencia entre otras.

República del Perú, en su Constitución establece en el Artículo 2 el derecho que tiene toda persona a solicitar información de cualquier entidad pública con excepción de las informaciones que afecten la intimidad personal y las que se excluyan por motivo de seguridad nacional. Tanto en el Artículo 161 como en el 162 que tocan aspectos relacionados con la defensa de los derechos fundamentales de las personas. En su Artículo 200 las garantías constitucionales a la acción de Hábeas Data. Poseen una legislación general de protección de datos personales y de varias legislaciones sectoriales.

República de Costa Rica, en su Constitución establece en dos de sus Artículos primero, Artículo 23 "El domicilio y todo otro recinto privado de los habitantes de la República son inviolables. No obstante pueden ser allanados por orden escrita de juez competente, o para impedir la comisión o impunidad de delitos, o evitar daños graves a las personas o a la propiedad, con sujeción a lo que prescribe la ley". Segundo, Artículo 24 "Se garantiza el derecho a la intimidad, a la libertad y al secreto de las comunicaciones". Cuenta con una legislación general conocida como ley de protección de la persona frente al tratamiento de sus datos personales. En lo relativo a legislación sectorial como tal, no se ha identificado alguna específica.

Nicaragua, establece en el Artículo 26 de su Constitución que "Toda persona tiene derecho: A su vida privada y la de su familia; A la inviolabilidad de su domicilio, su correspondencia y sus comunicaciones de todo tipo. A conocer toda información que sobre ella hayan registrado las autoridades estatales, así como el derecho de saber por qué y con qué finalidad tiene esa información". Cuentan con una norma general de ley de protección de datos personales no así con normas sectoriales que aborden el tema de este trabajo.

Colombia, en el Artículo 15 de su Constitución establece que "Todas las personas tiene derecho a su intimidad personal y familiar y a su buen nombre, y el Estado debe de respetarlos y hacerlos respetas. De igual modo, tiene derecho a conocer, actualizar y rectificar las informaciones que se hayan recogido sobre ellas en

los bancos de datos y en archivos de entidades públicas y privadas". Cuentan con una legislación general como es la ley que dictan disposiciones generales para la protección de datos personales y la ley que dictan las disposiciones generales del hábeas data y se regula el manejo de la información contenida en bases de datos personales. Cuentan con legislaciones sectoriales en lo relativo a telecomunicaciones, comercio electrónico y firma digital entre otras.

República Dominicana, que es el país sobre el cual se está basando este trabajo establece en su Constitución en el Artículo 44 el derecho a la intimidad y el honor que cada persona tiene de que se le respete su vida privada, familiar, su hogar y sus correspondencias. Cuenta con una legislación general, la Ley 172-13, la cual fue promulgada por el Poder Ejecutivo el 15 de diciembre del 2013 con fecha de entrada en vigor seis meses luego de su promulgación el pasado 13 de junio del 2014. Esta ley deroga la Ley No. 288-05 que regulaba las Sociedades de Información Crediticia y de Protección al Titular de la Información y modifica cualquier otra ley o parte de ley en cuanto contradiga lo que aquí está estipulado. El objeto de la referida ley es "La protección integral de los datos personales asentados en archivos, registros públicos, bancos de datos u otros medios técnicos de tratamiento de datos destinados a dar informes, sean éstos públicos o privados, así como garantizar que no se lesione el derecho al honor y a la intimidad de las personas, y también facilitar el acceso a la información que sobre las mismas se registre, de conformidad a lo establecido en el Artículo 44 de la Constitución de la República Dominicana. Del mismo modo, regula la constitución, organización, actividades, funcionamiento y extinción de las Sociedades de Información Crediticia (SIC), así como la prestación de los servicios de referencias crediticias y el suministro de la información en el mercado, garantizando el respeto a la privacidad y los derechos de los titulares de la misma, promoviendo la veracidad, la precisión, la actualización efectiva, la confidencialidad y el uso apropiado de dicha información."

Tabla No. 1 Resumen Legislación y Consignación en la Constitución LOPD en región Iberoamericana.

País	Const. Art. #	Legislación General	Legislación(es) Sectorial(es)
Principado de Andorra	14	15/2003 18 de diciembre	No
Bolivia	21.2 130 131	No	Código penal
			Ley 28168/2005 18 de mayo; Ley 018/2010 16 de junio
			Ley 164/2011 8 de agosto
			Decreto supremo 1793/2013 13 de noviembre
Brasil	5	No	Código penal; Ley complementaria 105
			Ley 8078/1990; Ley 9.296/1996 24 de junio
			Ley 9.507/1997 12 de noviembre
Chile	19.4	Ley 19.628/1999 28 de agosto	Ley 19.223/1993 7 de junio; Ley 19.628/1999 28 de agosto
		Ley 19.812/2002 13 de junio - modifica 19.628	Ley 19.759/2001 1 de diciembre
		Ley 20.463/2010 25 de octubre - modifica 19.628	Ley 19.812/2002 13 de junio
		Ley 20.575/2012 17 de febrero - modifica 19.628	Ley 19.496/2012 4 de marzo
Ecuador	11 66 92	No	Ley 184/1992 10 de agosto; Ley 67/2002 17 de abril
			Ley Orgánica de Transparencia y Acceso a la Información Pública (LOTAIP)/2004 18 de mayo
			Ley 13/2005 18 de octubre; Ley 162/2010 31 de marzo
República del Salvador	2	No	Decreto legislativo 142/1997 6 de noviembre
			Decreto legislativo 1030/1997 26 de abril
			Reglamento General de Ley Penitenciaria
			Decreto legislativo 166/2005 8 de septiembre
			Decreto 534/2011 30 de mar.; Decreto 136/2012 1 de sept.
Reino de España	18	Ley Orgánica 15/1999 13 de diciembre	Ley 12/1989/2003 21 de mayo; Ley 34/2002 11 de julio
		Real Decreto 1720/2007 21 de diciembre	Ley 41/2002 14 de noviembre; Ley 32/2003 3 de noviembre
			Ley 58/2003 19 de diciembre; Ley 19/2013 9 de diciembre
Guatemala	24 30 31	No	Código penal
			Decreto 33/1998; Decreto 006/2003; Decreto 47/2008
			Decreto 57/2008 del Congreso de la República
República de Honduras	76	No	Ley 170/2006
México	6 16 1973	Ley Federal de Transparencia y Acceso a la Información Pública Gubernamental, 8 junio 2012	Cada Estado cuenta con su Ley de transparencia, acceso y protección de los datos personales
		Ley Federal de Protección de Datos Personales en Posesión de los Particulares 5 julio 2010	
República de Panamá	29 , 42 43 , 44	No	Ley 6/2002 22 de enero
			Ley 24/2002 22 de mayo
República de Paraguay	33 135	No	Ley 3440/2008 16 de julio modif. Ley 1160/97 Código Penal
			Ley 1682/2001 3 de sep.; Ley 4017/2010 23 de diciembre
			Ley 4439/2011 3 de oct. modif. Ley 1160/97 Código Penal
			Ley 4610/2012 modifica y amplia Ley 4017/2010
			Ley 4868/13 26 de febrero; Ley 4989/2013 9 de agosto

Tabla No. 1 Resumen Legislación y Consignación en la Constitución LOPD en región Iberoamericana. (Continuación)

País	Const. Art. #	Legislación General	Legislación(es) Sectorial(es)
República Portuguesa	35	Ley 67/98 26 de octubre	Cibercrimen; Comunicaciones electrónicas
			Identificación Civil y Criminal; Salud
			Sistema Judicial; Trabajo
			Ley 5/2004 10 de febrero; Ley 41/2004 18 de agosto
			Ley 46/2004 19 de agosto; Ley 12/2005 26 de enero
			Ley 7/2007 5 de febrero; Ley 5/2008 12 de febrero
			Ley 32/2008 27 de julio; Ley 7/2009 12 de febrero
			Ley 34/2009 14 de julio; Ley 109/2009 15 de septiembre
			Ley 5/2012 23 de enero
Venezuela	28 60 281	No	Ley de registro de antecedentes penales/1979 3 de agosto
			Ley sobre protección a la privacidad de las comunicaciones/1991 16 de diciembre
			Ley orgánica para la protección del niño y del adolescente /1998 10 de febrero
			Ley especial contra delitos informáticos/2001 30 octubre
			Normas en Proyecto
			Proyecto de tecnología de la información
			Proyecto de ley de protección de datos habeas data
Argentina	43	Ley 25.326/2000 2 de noviembre	No
		Ley 26.343/2008 8 de enero modifica Ley 25.326	
Uruguay	7 11 28 72 332	Uruguay+79:9279:10279:92D7379:8979:10279:92	Ley 15.322/1982 17 de sep.; Ley 16.099/1989 13 de nov.
		Ley 18.381/2008 7 de noviembre	Ley 17.823/2004 7 de sep.; Ley 17.835/2004 23 de sep.
			Ley 18.244/2007 27 de diciembre
			Decreto 258/1992 16 de junio; Decreto 65/1998 10 de marzo
			Decreto 396/2003 20 de sept.; Decreto 37/2005 27 de enero
			Decreto 131/2005 11 de abril; Decreto 246/2005 8 de agosto
			Decreto 399/2006 30 de oct.; Decreto 249/2007 9 de julio
			Decreto 250/2007 9 de julio; Decreto 664/2008 22 de dic.
República del Perú	2 161 162 200	Ley 29733/2011 3 de julio	Ley 26702/1996 9 de diciembre; Ley 27269/2000 28 de mayo
		Código penal	Ley 27309/2000 17 de julio; Ley 27489/2001 28 de junio
			Ley 27806/2002 3 de agosto; Ley 28493/2005 18 de marzo
			Ley 29499/2010 19 de enero; Ley 30024/2013 22 de mayo
			Ley 30096/2013 22 de octubre; Ley 30171/2014 10 de marzo
República de Costa Rica	23 24	Ley 8968/2011 7 de julio	Código penal
		Directriz 046-H-MICITT/2013 9 de abril	
Nicaragua	26	Ley 787/2012 29 de marzo	No
Colombia	15	Ley 1266/2008 31 de diciembre	Ley 1712/2014 6 de marzo; Ley 270/1996
		Ley 273/2009	Ley 527/1999 18 de agosto; Ley 57/1985
		Decreto 1727/2009 15 de mayo	Decreto 575/2002
		Decreto 2952/2010 6 de agosto	Resolución MC 2578/2007
		Ley 1581/2012 17 de octubre	Decreto 2870/2007
República Dominicana	44.2 70	Ley 172/2013 13 de diciembre	Ley 153/1998 27 de mayo
			Ley 126/2002 4 de septiembre
			Ley 200/2004
			Ley 288/2005
			Ley 53/2007 23 de abril

Fuente: Elaboración propia a partir de las leyes de los diferentes países listados en la misma tabla.

Visto todo lo anterior se puede concluir que en la región iberoamericana todos los países que la forman, o las que son objeto de análisis en este trabajo, consignan en su Constitución lo relativo al de derecho de las personas a la protección de sus datos personales, a su intimidad, privacidad entre otros. Así mismo, se pudo observar que cuentan con una LOPD y en el caso de que no, con legislaciones sectoriales suficientes para atender el tema en cuestión.

1.4 Control, cumplimiento y sanciones contemplados en la ley 172-13 comparado con países de la región Iberoamericana.

En esta sección se presentan los mecanismos de control, cumplimiento y sanciones que prevee tanto la Ley 172-13 de la República Dominicana así como las LOPD de los diferentes países que componen la Red Iberoamericana.

En la legislación de la **República Dominicana**, la ley No.172-13 repite, sobre las sanciones e infracciones lo recogido en la normativa sobre SIC, añadiendo: Artículo 84. Sanciones excepcionales. Será sancionado con una multa de diez (10) a cincuenta (50) salarios mínimos vigentes, sin perjuicio de las reparaciones que procedan por los daños y perjuicios que haya sufrido la persona por causa de violación a su derecho a la privacidad, conforme a las normas del derecho común, la persona física que:

1. Insertara o hiciera insertar, a sabiendas, datos falsos en un archivo de datos personales, de manera dolosa o de mala fe.

2. Proporcionase, de manera dolosa o de mala fe, información falsa a un tercero, contenida en un archivo de datos personales.

3. Accediere a sabiendas e ilegítimamente, o violando sistemas de confidencialidad y seguridad de datos, de cualquier forma, a un banco de datos personales.

4. Revelare a otra información registrada en un banco de datos personales cuyo secreto estuviere obligado a preservar por disposición de una ley.

Respecto al establecimiento de una Autoridad de Control para salvaguardar los derechos establecidos por la Ley No 172-13, la legislación dominicana aún no ha establecido la titularidad del organismo pertinente ni sus deberes y responsabilidades.

Al respecto, la Ley sobre Protección de Datos de Carácter Personal se limita a repetir lo que ya se decía en la Ley 288-05 sobre Sociedades de Intermediación Crediticia (SIC) y de Protección al Titular de la Información actualizando la normativa sobre las Sociedades de Información Crediticia.

En la legislación del **Principado de Andorra** el primer incumplimiento por parte de un responsable de fichero se sanciona con una multa de importe máximo de 50,000 euros, y los incumplimientos subsiguientes en que pueda incurrir el mismo responsable se sancionan con una multa de un importe máximo de 100,000 euros, según dispone el art. 33 de la Ley. En los casos en que el responsable de los datos sea un organismo público, el art. 34 de la LQPD prevé que se apliquen el procedimiento y las sanciones establecidos en las disposiciones reguladoras de los regímenes disciplinarios.

Una peculiaridad de la legislación andorrana en materia de protección de datos es que no existe una lista detallada de incumplimientos junto a la sanción correspondiente para cada una de ellas. Se deja total libertad a la APDA para su cuantía teniendo en cuenta una serie de criterios. Esta indeterminación ha propiciado la Sentencia 31/2008 del Tribunal Superior de Justicia del Principat d'Andorra, Sala Administrativa, de 31 de marzo de 20084, que obliga a la APDA a individualizar primero la conducta infractora para evitar incumplir el principio de ne bis in ídem. Una vez hecho esto, según el alto tribunal, ya se modulará la sanción según los criterios establecidos en el art. 33 LQPD.

Cabe mencionar el art. 26 LQPD que recuerda que las sanciones previstas en el capítulo quinto de esta Ley se entienden sin perjuicio de la responsabilidad civil en que pudiera incurrir un responsable del tratamiento en caso de incumplimiento de la misma. Para recurrir las resoluciones de la APDA, el art. 44 LQPD establece que la APDA adecuará en todo momento su actuación al «Codi de l'Administració», las resoluciones de la cual serán impugnables conforme lo que se establece en dicho

cuerpo legislativo. Debe tenerse en cuenta que, según dispone el art. 36.1 del RAPDA, las infracciones tipificadas en la Llei 15/2003, de 18 de desembre, qualificada de protección de dades personals (LQPD), prescriben al cabo de tres años de haberse cometido.

El capítulo séptimo de la LQPD crea la «Agència Andorrana de Protecció de Dades (APDA)», organismo público con personalidad jurídica propia, independiente de las administraciones públicas y con plena capacidad de obrar. También los capítulos del séptimo al undécimo del RAPDA tratan sobre la APDA, centrándose el art. 23 en su ámbito de actuación, el art. 24 en sus competencias y el art. 25 en sus funciones, entre otros muchos temas de detalle. El Director de la Agéncia y los inspectores de protección de datos son designados por el «Consell General d'Andorra» por mayoría cualificada de dos terceras partes en primera votación (…), según dispone el art. 39 LQPD. La APDA se financia exclusivamente de las partidas que cada año establece para su funcionamiento el «Consell General d'Andorra» (vid. art. 39 LQPD.

Entre sus potestades está, entre otras y según dispone el art. 40 de la Ley y el art. 25 RAPDA, velar por el cumplimiento de la misma, gestionar el Registro Público de Inscripción de Ficheros de Datos Personales, publicar anualmente la lista de países con nivel de protección equivalente, ejercer potestad inspectora y sancionadora, proponer mejoras en la normativa de protección de datos, elaborar una memoria anual, emitir informes con carácter consultivo, atender las peticiones que le haga la ciudadanía y coordinarse con otras autoridades de control. En el Principat d'Andorra, según dispone el art. 27 de la LQPD existe la obligación de inscripción de los ficheros de datos personales. Las personas físicas o jurídicas de naturaleza privada que sean responsables del tratamiento de datos, han de inscribir el fichero de datos personales bajo su responsabilidad, antes de crearlo, en el registro público gestionado por la autoridad de control. La creación, modificación o supresión de ficheros por parte de los organismos públicos deberá estar precedida por una Norma de creación, que ha de ser aprobada por la entidad pública responsable de su tratamiento, y que ha de ser publicada en el «Butlletí Oficial del Principat d'Andorra» antes de la creación,

modificación o supresión del fichero, con las excepciones reflejadas en el art. 30 de esta Ley.

El art. 41 de esta Ley establece la posibilidad de que la Agencia inicie una inspección por propia iniciativa (de oficio) y siempre con autorización del director de la APDA, o a solicitud de cualquier persona interesada (tutela de derechos) que considere que sus datos personales se han visto afectados o que un responsable ha infringido las obligaciones que impone la Ley.

La APDA tiene potestad sancionadora de acuerdo con el procedimiento establecido en el «Codi de l'Administració». En cuanto a las sanciones, tratadas en el capítulo quinto de la LQPD, se refieren al incumplimiento de sus disposiciones, estableciendo como principio general que el incumplimiento de esta Ley por parte de personas físicas o de personas jurídicas de naturaleza privada es objeto de sanción administrativa.

El régimen de sanciones en **Argentina** se encuentra normado en los arts. 31 y 32 de la LPDP para los casos de incumplimientos y violaciones a dicha ley. En primer lugar, se establece que el órgano de control podrá aplicar sanciones de: a) apercibimiento; b) suspensión; c) multas entre $ 1.000 y $ 100.000; d) clausura, o e) cancelación del archivo, registro o banco de datos. Las mismas serán aplicadas sin perjuicio de las responsabilidades administrativas que correspondan en el caso de responsables o usuarios de bancos de datos públicos y de la responsabilidad por daños y perjuicios derivados de la inobservancia de la ley, y más allá de las sanciones penales previstas. El decreto reglamentario establece que la cuantía de las sanciones se graduará atendiendo a la naturaleza de los derechos afectados, al volumen de los tratamientos efectuados, a los beneficios obtenidos, al grado de intencionalidad, a la reincidencia, a los daños y perjuicios causados a las personas interesadas y a los terceros y a cualquier otra circunstancia que sea relevante para la determinación. Asimismo, establece las normas de procedimiento a las cuales se deberán ajustar para la aplicación de las sanciones dispuestas. En cuanto a las sanciones penales, el art. 32 de la LPDP incorpora los arts. 117 bis25 y 157 bis26 en el Código Penal Argentino.

La Dirección Nacional de Protección de Datos Personales –DNPDP- es el órgano de control creado en el ámbito Nacional, para la efectiva protección de los datos personales. El art. 29 de la ley 25.326 establece las normas que rigen al órgano de control, el cual deberá velar por el cumplimiento de las disposiciones de la ley y aplicar las sanciones civiles y penales que la misma dispone, e indica las atribuciones y funciones de este órgano. A estos efectos, el decreto reglamentario 1558/2001 crea la Dirección Nacional de Protección de Datos Personales, en el ámbito de la Secretaría de Justicia y Asuntos Legislativos del Ministerio de Justicia y Derechos Humanos.

El Capítulo IV de la LPDP en los art. 21 a 28 se ocupa de los «Usuarios y Responsables de Archivos, Registros y Bancos de Datos» En primer término se establece que todos los archivos, bases o bancos de datos públicos y privados destinados a proveer informes, deben inscribirse en el registro habilitado por el organismo de control, éste es la Dirección Nacional de Protección de Datos Personales.

Para el cumplimiento de esta obligación deberán consignar, como mínimo, la siguiente información: nombre y domicilio del responsable; características y finalidad del archivo; naturaleza de los datos personales contenidos en cada archivo; forma de recolección y actualización de los datos; destino de los datos y personas físicas y de existencia ideal a las que pueden ser trasmitidos; modo de interrelacionar la información registrada; medios utilizados para garantizar la seguridad de los datos, debiendo detallar la categoría de personas con acceso al tratamiento de la información; tiempo de conservación de los datos; forma y condiciones en que las personas pueden acceder a los datos referidos a ellas y los procedimientos a realizar para rectificación o actualización de los datos. Para los archivos, registros o bancos pertenecientes a organismos públicos, su creación, modificación o supresión, deben hacerse por medio de disposición general publicada en el Boletín Oficial de la Nación o diario oficial. En caso de supresión de los registros informatizados también se deberá consignar la forma de destrucción.

A su vez el órgano de control en el cumplimiento de sus funciones, mediante el dictado de la disposición 2/200323 del 20/11/2003 y sus complementarias habilitó el Registro Nacional de Bases de Datos donde se aprueban los formularios de inscripción al mismo y disponen la realización del Censo Nacional de Bases de Datos, con carácter obligatorio. La disposición 6/200524 del 1/9/2005 crea el diseño del isologotipo que identificará a los responsables de bases de datos inscriptos en el registro, quienes una vez aprobados los trámites pertinentes podrán hacer uso de aquel.

La legislación de **Chile** de protección de datos personales, por ahora, no contempla la creación de un órgano de control que vele por el resguardo de los derechos consagrados en ella, y que supervise la gestión de los responsables de los registros o bancos de datos de carácter personal. El único órgano al cual la ley de protección de datos personales chilena le encomienda alguna función relacionada con el tratamiento de esos datos es el Servicio de Registro Civil, el cual debe mantener un Registro de todos los bancos de datos personales a cargo solamente de organismos públicos (art. 22 de la ley en comento). Sin embargo, dicho Servicio (Registro Civil), no posee facultades coactivas respecto de los responsables de los bancos de datos a cargo de organismos públicos, por lo que no puede obligar a éstos a que inscriban sus bases de datos, o sea, su rol queda reducido a ser un ente meramente registral.

La falta de un órgano de control en la materia, quita fuerza y coherencia al sistema de protección de datos chileno, pero las autoridades actuales han visto esto como un elemento de modernización. Es en cualquier caso extraño, al menos, que se obligue inscribir los bancos de datos a cargo de organismos públicos y se deje fuera a los que están bajo la responsabilidad de privados o particulares. Ciertamente este es un tema pendiente y mientras no se resuelva, nuestra legislación carecerá de una efectiva supervisión y control, donde cada banco de datos privado y sus responsables operarán en el «tráfico de datos personales» literalmente. Hasta ahora entonces el que los legisladores chilenos no puedan imponer ante los privados la creación de un registro de bancos de datos personales, ni la obligación de inscribirlos por los particulares que sean responsables de esos bancos de datos poco se podrá avanzar

para lograr una efectiva protección de los derechos de las personas sobre la identificación del registro o banco de datos, así como su finalidad, contenido y personas responsables de éste, dificultando finalmente el ejercicio de los derechos de información, modificación, cancelación y bloqueo de datos personales, al menos.

Es indudable que Chile debe asumir que la legislación nacional sobre la materia tiene dificultades en lo que se refiere al estándar internacional, debiendo incorporar una serie de modificaciones a la legislación con miras a lograr el cumplimiento de dichos marcos. La inadecuada forma en que los organismos públicos y privados, como consecuencia de la pasividad legal normativa, tratan los datos personales permite que los ciudadanos vean hasta como algo normal el que se pueda hacer cualquier cosa con la información de las personas sin considerar, ni conocer que se afectan con ello, derechos fundamentales, como vida privada la honra y otros derechos asociados.

En **Colombia** mediante la Ley 1273 de 2009, por medio de la cual se modifica el Código Penal, se crea un nuevo bien jurídico tutelado —denominado «de la protección de la información y de los datos» y se preservan integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones, entre otras disposiciones; y que es conocida en Colombia como la Ley de delitos informáticos, se establece como bien jurídico tutelado, precisamente la información y los datos; se establecieron de manera positiva y fueron tipificados como delitos – hecho punibles, algunos tipos penales que sancionan, entre otros, ciertos aspectos relacionados con el tratamiento de datos personales como el acceso no autorizado a sistemas de información, la destrucción o manipulación de datos, la suplantación de sitios web para capturar datos personales y la violación de datos personales. Este tipo penal entra a sancionar con prisión de 4 a 8 años y multa de 100 a 1000 salarios mínimos legales mensuales. Se denota: «Artículo 269F: Violación de datos personales. El que, sin estar facultado para ello, con provecho propio o de un tercero, obtenga, compile, sustraiga, ofrezca, venda, intercambie, envíe, compre, intercepte, divulgue, modifique o emplee códigos personales, datos personales contenidos en ficheros, archivos, bases de datos o medios semejantes, incurrirá en pena de prisión

de cuarenta y ocho (48) a noventa y seis (96) meses y en multa de 100 a 1000 salarios mínimos legales mensuales vigentes.»

En otras palabras, se fijan los diversos eventos y conductas que generan responsabilidad penal tratándose del tratamiento de datos personales. El deber de diligencia y cuidado de los responsables, como los encargados del tratamiento de datos personales, deberán desplegar una serie de gestiones y tomar medidas efectivas, para poder evitar incurrir en responsabilidad penal. Se establece un agravante al tipo penal cuando la pena señalada se aumenta de la mitad a las tres cuartas partes si la conducta la cometiere el responsable de la administración, manejo o control de dicha información. A lo anterior se agrega el hecho de que si el infractor se puede hacer acreedor a una pena de prisión de hasta por tres años, y la pena accesoria de inhabilitación para el ejercicio de profesión relacionada con sistemas de información procesada con equipos computacionales.

Sobre este particular, resultan altamente importantes e interesante, las consideraciones que se reseñan en el Sitio Web del Grupo de Estudios en Internet, Comercio Electrónico, Telecomunicaciones & Informática (GECTI), de la Facultad de Derecho de la Universidad de los Andes de Colombia, se reseña de manera precisa, más precisamente en el Sitio Web del observatorio Ciro Angarita Barón sobre protección de datos personales en Colombia, en un interesante artículo realizado por Nelson Remolina Angarita en 2013/04/18, cita:

«Según datos estadísticos del INPEC (Instituto Nacional Penitenciario y Carcelario) 41 personas han sido condenadas por el delito de violación de datos personales. De otra parte, desde el 1 de marzo de 2010 hasta el 22 de marzo de 2013, la Superintendencia de Industria y Comercio (SIC) ha impuesto 544 multas por $4.719.129,675 (US$2.556,408). Las sanciones de la SIC se refieren a situaciones de infracciones de la ley de habeas data financiero (Ley 1266 de 2008). Los principales motivos de las mismas son: (1) No veracidad de la información reportada; (2) Falta de atención debida de reclamos y peticiones de los titulares de los datos; (3) Omisión de la comunicación previa a la persona antes de reportarla a las centrales de riesgo y (4) recolección de datos sin autorización del titular. La información sobre las

condenas penales fue publicada por el INPEC el pasado 5 de abril de 2013 en las estadísticas tituladas: Modalidades delictivas población internos marzo de 2013.»

En un pronunciamiento emitido el veintitrés (23) de enero del año Dos Mil Catorce (2014), y que recoge muchos de los postulados y precedentes dados en reiterada jurisprudencia Colombina, la Superintendencia de Industria y Comercio (SIC), Delegatura para la protección de datos personales, en ejercicio de las facultades jurisdiccionales que le otorgo el código general del proceso, le solicito a la relatoría de la sala penal de la Corte Suprema de Justicia suprimir datos de menores de edad en versiones públicas de las sentencias.

En **Costa Rica**, la Agencia de Protección de Datos de los Habitantes (Prodhab), es la encargada de velar por el cumplimiento de la normativa en materia de protección de datos, tanto para personas físicas como jurídicas y fue creada por la Ley n.º 8968. Dentro de sus funciones está el velar por el cumplimiento de la normativa en materia de protección de datos, incluyendo:

1. Llevar un registro de las bases de datos reguladas por esta ley. Hace referencia a que toda base de datos que no sea registrada en esta Agencia, se tendrá como irregular y no autorizada para existir, sea el sector público o privado quien la maneje.
2. Imponer las sanciones a quienes infrinjan las normas sobre la protección de datos personales y trasladar al Ministerio Público las que se puedan configurar como delito. En la ley y su reglamento se establecen los procedimientos por medio de los cuales se procede a la sanción en el fáctico.
3. Promover y contribuir en la redacción de la normativa tendiente a implementar las normas que regulan esta materia. Acá se faculta para que se proceda a formular cualquier proyecto de reforma de la normativa con el fin de alcanzar los objetivos propios de la Agencia, siempre actualizándose a las nuevas tecnologías.
4. Fomentar entre los habitantes el conocimiento de los derechos concernientes al acopio, el almacenamiento, la transferencia y el uso de sus datos personales. Más que una función, lo considero una obligación, pues dentro de los

proyectos está la de información, asesoría y divulgación de la normativa vigente.

También, podrá acceder a las bases de datos reguladas por la ley, estén o no registradas en la Agencia; con el fin de cumplir la normativa vigente, donde operará de oficio o a solicitud de parte, pudiendo ordenar la supresión, rectificación, adición o restricción en el tráfico de datos personales si no están acordes a los parámetros de la ley. Así mismo debe resolver los reclamos interpuestos ante su fuero, dictar las directrices necesarias.

Esas son muchas de las funciones que permite desarrollar la legislación en el ámbito costarricense sobre protección de datos, no obstante, es un tema que todavía podría considerarse en embrión. Falta más que normativa la concientización de la sociedad.

En la legislación de **España**, las sanciones oscilan entre 900 a 40.000 euros para infracciones leves, 40.001 a 300.000 euros para las graves, y 300.001 a 600.000 euros las muy graves. Estas sanciones son únicamente impuestas a los tratamientos de titularidad privada (empresas, empresarios individuales, otras entidades con personalidad jurídica…), puesto que para los tratamientos de titularidad pública (aquellos gestionados por administraciones e instituciones públicas), conforme a lo dispuesto en el artículo 46 de la LO 15/1999, el órgano sancionador dictará una resolución que recoja las medidas a adoptar para que se corrijan o cesen los efectos de la infracción y, en su caso, podrá iniciar actuaciones disciplinarias. El art. 44 de la LOPD clasifica las infracciones en:

Leves.

- No remitir a la Agencia Española de Protección de Datos las notificaciones previstas en esta Ley o en sus disposiciones de desarrollo.
- No solicitar la inscripción del fichero de datos de carácter personal en el Registro General de Protección de Datos.

- El incumplimiento del deber de información al afectado acerca del tratamiento de sus datos de carácter personal cuando los datos sean recabados del propio interesado.
- La transmisión de los datos a un encargado del tratamiento sin dar cumplimiento a los deberes formales establecidos en el artículo 12 de esta Ley.

Graves

- Proceder a la creación de ficheros de titularidad pública o iniciar la recogida de datos de carácter personal para los mismos, sin autorización de disposición general, publicada en el «Boletín Oficial del Estado» o diario oficial correspondiente.
- Tratar datos de carácter personal sin recabar el consentimiento de las personas afectadas, cuando el mismo sea necesario conforme a lo dispuesto en esta Ley y sus disposiciones de desarrollo.
- Tratar datos de carácter personal o usarlos posteriormente con conculcación de los principios y garantías establecidos en el artículo 4 de la presente Ley y las disposiciones que lo desarrollan, salvo cuando sea constitutivo de infracción muy grave.
- La vulneración del deber de guardar secreto acerca del tratamiento de los datos de carácter personal al que se refiere el artículo 10 de la presente Ley.
- El impedimento o la obstaculización del ejercicio de los derechos de acceso, rectificación, cancelación y oposición.
- El incumplimiento del deber de información al afectado acerca del tratamiento de sus datos de carácter personal cuando los datos no hayan sido recabados del propio interesado.
- El incumplimiento de los restantes deberes de notificación o requerimientos al afectado, impuestos por esta Ley y sus disposiciones de desarrollo.

- Mantener los ficheros, locales, programas o equipos que contengan datos de carácter personal sin las debidas condiciones de seguridad que por vía reglamentaria se determinen.
- No atender los requerimientos o apercibimientos de la Agencia Española de Protección de Datos o no proporcionar a aquélla cuantos documentos e informaciones sean solicitados por la misma.
- La obstrucción al ejercicio de la función inspectora.
- La comunicación o cesión de los datos de carácter personal sin contar con legitimación para ello en los términos previstos en esta Ley y sus disposiciones reglamentarias de desarrollo, salvo que la misma sea constitutiva de infracción muy grave.

Muy graves

- La recogida de datos en forma engañosa o fraudulenta.
- Tratar o ceder los datos de carácter personal a los que se refieren los apartados 2, 3 y 5 del artículo 7 de esta Ley salvo en los supuestos en que la misma lo autoriza o violentar la prohibición contenida en el apartado 4 del artículo 7.
- No cesar en el tratamiento ilícito de datos de carácter personal cuando existiese un previo requerimiento del Director de la Agencia Española de Protección de Datos para ello.
- La transferencia internacional de datos de carácter personal con destino a países que no proporcionen un nivel de protección equiparable sin autorización del Director de la Agencia Española de Protección de Datos salvo en los supuestos en los que conforme a esta Ley y sus disposiciones de desarrollo dicha autorización no resulta necesaria.

Si la infracción se tipifica como leve o grave, y el infractor no hubiera sido sancionado o apercibido con anterioridad, con carácter excepcional, atendiendo a las circunstancias del hecho y previa audiencia de las partes, puede no iniciar el procedimiento sancionador sustituyéndolo por un apercibimiento al infractor en el que se le obligue a acreditar en un plazo determinado, la implantación de medidas

correctoras. Si transcurrido el citado plazo no se hubiera atendido el apercibimiento, el órgano sancionador puede iniciar procedimiento por incumplimiento.

En lo que respecta a la graduación de la cuantía de las sanciones, el artículo 45.4 de la Ley Orgánica 15/1999 establece una serie de criterios para su baremo, como son, el carácter continuado, el volumen de los datos afectados o el beneficio obtenido. También se puede imponer la sanción en la escala precedente en gravedad, si concurre alguno de los supuestos reflejados en el artículo 45.5. Los plazos de prescripción tanto de las infracciones, como de las sanciones son de tres años para las muy graves, dos años para las graves y un año para las leves, computándose los plazos desde el día en que la infracción se ha cometido o la sanción adquiere firmeza.

En la legislación de **México**, las sanciones por motivo del incumplimiento de las obligaciones y disposiciones establecidas en la LFPDPPP podrán ser: Apercibimiento y Multas que van desde los $6,729 a los $2.1 millones de pesos, multas que podrán ser duplicables en caso de reincidencia.

Además de lo anterior también se contemplan delitos que podrán ser sancionados con prisión que podrá ir desde los 6 meses a los 5 años.

La autoridad de control es el Instituto Federal de Acceso a la Información Pública y Protección de Datos (IFAI). Existen tres procedimientos relacionados con la protección de datos personales ante el IFAI, ello ya que el procedimiento de derechos ARCO se lleva a cabo ante el particular:

- Protección de derechos107. La solicitud de protección de datos se presentará ante el IFAI durante los 15 días siguientes a la fecha en que se comunique la respuesta al titular por parte del responsable, ello en relación a las solicitudes de derechos ARCO que se hayan efectuado.
- Si el titular no recibe respuesta por parte del responsable, la solicitud de protección de datos podrá ser presentada a partir de que haya vencido el plazo de respuesta previsto para el responsable.

- De verificación108. Con el fin de vigilar el cumplimiento de las normas en la materia, el IFAI llevará a cabo este procedimiento iniciándolo de oficio o a petición de parte.
- De imposición de sanciones109. El cual procede en caso de que de los procedimientos de protección de derechos o de verificación, se tuviera conocimiento de un presunto incumplimiento de alguno de los principios o disposiciones de las normas en la materia.

En la **República de Perú**, El Ministerio de Justicia y Derechos Humanos es la Autoridad Nacional de Protección de Datos Personales (APDP), la cual debe realizar todas las acciones necesarias para el cumplimiento del objeto y demás disposiciones de la Ley PDP y de su reglamento, para ello goza de una potestad sancionadora. La APDP tiene entre sus principales funciones el de velar por el cumplimiento de la Ley PDP, en caso de infracción a la Ley es el Director de las Sanciones de la Autoridad quien instruye y resuelve en primera instancia y el Director General de Protección de Datos Personales resolverá en segunda y última instancia el procedimiento sancionador. Este procedimiento será promovido siempre de oficio, que puede obedecer a una denuncia de parte o por decisión motivada del Director de la Autoridad. Se han establecido infracciones leves, graves y muy graves. Las sanciones pueden ser pecuniarias, la Autoridad puede mandar medidas correctivas e incluso medidas cautelares en caso de ser necesario.

Respecto a inscripción de los bancos de datos personales, estos deberán ser inscritos en el Registro Nacional de Protección de Datos Personales (actualmente mediante previo pago ante la Autoridad), registró que es de carácter público. En el Registro Nacional también se inscribirán los códigos de conducta, las sanciones, medidas cautelares o coercitivas impuestas por la Autoridad y comunicaciones del flujo transfronterizo de los datos.

En la **República Portuguesa, Portugal**, la Constitución contiene varios comandos dirigidos al legislador ordinario en el campo de la consagración de

protección de datos personales, en particular, la protección a través de una entidad administrativa independiente, cfr. el artículo 35, párrafo 2 del CRP.

Se trata de un órgano administrativo independiente, en Portugal, la Comisión Nacional de Protección de Datos (CNPD), a nivel nacional, que tiene poderes de autoridad y trabaja con la Asamblea Nacional.

El CNPD se compone de siete miembros, incluido el Presidente y dos miembros elegidos por la Asamblea de la República, dos miembros, los jueces designados por los Consejos y fiscales Supremos, respectivamente, y dos personas de reconocido mérito, con un mandato de cinco años, LPDP. Cuenta con amplias facultades (en el sector privado y la administración pública), en particular: el registro; autorización de procesamiento de datos, la interconexión y la utilización para fines que no sean de la colección; emisión de los dictámenes (por ejemplo, códigos de conducta.); así como la vigilancia y sanción. CNPD dispone en su sitio web oficial, varias formas específicas para diferentes tipos de tratamiento.

En la CNPD se preparó también una serie de documentos de orientación sobre cuestiones clave, atolones, como la salud, el trabajo, el acceso a los datos personales, información de crédito, los flujos internacionales, video vigilancia, marketing, nuevas tecnologías, telecomunicaciones, etc., que no son en sí misma obligatoria, pero son una guía importante en cada una de procesamiento de titular de los datos personales.

La Legislación en **Uruguay** crea la Unidad Reguladora y de Control de Datos Personales, como Organismo de Control. De acuerdo a la información que publican, las facultades de esta unidad, respecto a la Ley son:

- Asistir y asesorar a las personas.
- Dictar normas y reglamentaciones.
- Realizar un censo de las bases de datos incluidas en la ley de protección de datos. Mantener registro de los censos.
- Controlar el cumplimiento de las normas sobre integridad, veracidad y seguridad. Solicitar información sobre el tratamiento de los datos.

- Emitir opinión respecto a sanciones administrativas por el incumplimiento de la ley. Asesorar al Poder Ejecutivo en proyectos de ley que refieran a la protección de datos personales.
- Informar a cualquier persona sobre la existencia de bases de datos personales, sus finalidades y la identidad de sus responsables.

Para concluir, la cuantía de las **sanciones que imponen la Ley orgánica de Protección de Datos en los países de Iberoamérica,** se gradúa atendiendo a la naturaleza de los derechos personales afectados, al volumen de los tratamientos efectuados, a los beneficios obtenidos, al grado de intencionalidad, a la reincidencia, a los daños y perjuicios causados a las personas interesadas y a cualquier otra circunstancia que sea relevante para determinar el grado de culpabilidad. Ver a continuación las comparaciones de sanciones de los diferentes países de Iberoamérica:

Los incumplimientos a la LOPD en **La República Dominicana** al igual que **Andorra**, **España**, **Costa Rica**, **Argentina**, **México** y **Colombia**, se sancionan con multas que se deben pagar con un importe que dependerá del grado de la infracción cometida. En la **República Dominicana** será sancionado con una multa de diez (10) a cincuenta (50) salarios mínimos vigentes, sin perjuicio de las reparaciones que procedan por los daños y perjuicios que haya sufrido la persona por causa de violación a su derecho a la privacidad conforme a las normas del derecho común y/o cualquier incumplimiento establecido en el Cap.V. De la Ley 172-13.

En los países **Andorra** y **España**, en los casos en que el responsable de los datos sea un organismo público, se aplican las sanciones y procedimientos establecidos en las disposiciones reguladoras del régimen disciplinarios. En Andorra el primer incumplimiento por parte de un responsable de fichero se sanciona con una multa de importe máximo de $ 50,000 euros, y los incumplimientos subsiguientes en que pueda incurrir el mismo responsable se sanciona con una multa de un importe máximo de $ 100,000 euros según dispone el art. 33 de la Ley.

En España, en la República de Perú al igual que en **Costa Rica** las sanciones se clasifican por grado de infracción, pero con importes diferentes a pagar

dependiendo del incumplimiento cometido. **España**, las sanciones oscilan entre $ 900 a $ 40.000 euros para infracciones leves, $ 40.001 a $ 300.000 euros para las graves, y $ 300.001 a $ 600.000 euros las muy graves. Estas sanciones son únicamente impuestas a los tratamientos de titularidad privada (empresas, empresarios individuales, otras entidades con personalidad jurídica. En **Costa Rica** las sanciones son clasificadas por el grado de incidencia, como lo establece la Ley No. 8968 en su Art. 28. Se clasifican en: a) Para las **faltas leves**, una multa hasta de cinco salarios base del cargo de auxiliar judicial I según la Ley de Presupuesto de la República. b) Para las **faltas graves**, una multa de cinco a veinte salarios base del cargo de auxiliar judicial I, según la Ley de Presupuesto de la República. c) Para las **faltas gravísimas**, una multa de quince a treinta salarios base del cargo de auxiliar judicial I según la Ley de Presupuesto de la República, y la suspensión para el funcionamiento del fichero de uno a seis meses.

En los países como **Argentina** y **México** tienen similitud al aplicar sus sanciones de apercibimiento y multas, mientras que **México** y **Colombia** tienden a sancionar con prisión desde 6 meses a 8 años y diferentes importes por multas. El régimen de sanciones en **Argentina** en primer lugar, se establece que el órgano de control podrá aplicar sanciones de: a) apercibimiento; b) suspensión; c) multas entre $ 1.000 y $ 100.000; d) clausura, o e) cancelación del archivo, registro o banco de datos. En **México**, las sanciones por motivo del incumplimiento de las obligaciones y disposiciones establecidas en la LFPDPPP podrán ser: Apercibimiento y Multas que van desde los $ 6,729 a los $ 2.1 millones de pesos, multas que podrán ser duplicables en caso de reincidencia. Además de lo anterior también se contemplan delitos que podrán ser sancionados con prisión que podrá ir desde los 6 meses a los 5 años. **En Colombia** algunos tipos penales que sancionan, como aspectos relacionados con el tratamiento de datos personales, el acceso no autorizado a sistemas de información, la destrucción o manipulación de datos, la suplantación de sitios web para capturar datos personales y la violación de datos personales. Este tipo penal entra a sancionar con prisión de 4 a 8 años y multa de 100 a 1,000 salarios mínimos legales mensuales. Se denota: «Artículo 269F: Violación de datos personales. El que, sin estar facultado para ello, con provecho propio o de un tercero, obtenga, compile,

sustraiga, ofrezca, venda, intercambie, envíe, compre, intercepte, divulgue, modifique o emplee códigos personales, datos personales contenidos en ficheros, archivos, bases de datos o medios semejantes, incurrirá en pena de prisión de cuarenta y ocho (48) a noventa y seis (96) meses y en multa de 100 a 1,000 salarios mínimos legales mensuales vigentes.»

En la **República de Perú**, **República Portuguesa** y **Uruguay** cuentan con órganos reguladores los cuales deben realizar todas las acciones necesarias para el cumplimiento del objeto y demás disposiciones de la Ley y de su reglamento, para ello goza de una potestad sancionadora.

A continuación, se presenta la Tabla No. 2 la cual muestra los diferentes órganos de control en materia de protección de datos en los países pertenecientes a la llamada Red Iberoamericana.

Tabla No. 2 Organismos y autoridades de control.

Países	Órganos nacionales	Otros organismos
Andorra	L'Agència Andorrana de Protecció de Dades.	
Argentina	Dirección Nacional de Protección de Datos Personales.	Dirección de Protección de Datos Personales de la Defensoría del Pueblo de la Ciudad Autónoma de Buenos Aires.
Colombia	Delegatura de Protección de Datos de la Superintendencia de Industria y Comercio.	
Costa Rica	Agencia de Protección de Datos de los Habitantes	
Ecuador	Superintendencia de Telecomunicaciones	
España	Agencia Española de Protección de Datos.	Autoritat Catalana de Protecció de Dades. Datuak Babesteko Euskal Bulegoa

Tabla No. 2 Organismos y autoridades de control. (Continuación)

Países	Órganos nacionales	Otros organismos
Honduras	Instituto de Acceso a la Información Pública.	
México	Instituto Federal de Acceso a la Información y Protección de Datos	
Perú	Autoridad Nacional de Protección de Datos Personales	
Portugal	Comisión Nacional de Protección de Datos.	
Uruguay	Unidad Reguladora y de Control de Datos Personales.	

Fuente: Elaboración Propia

La importancia que los diferentes países otorgan a su ley de protección de datos de carácter personal queda evidenciado con el nivel de sanciones que por no cumplimiento tienen establecidos en su referida ley.

1.5 Enfoque de control interno en el desarrollo de un plan de auditoría interna en la actividad de protección de los datos personales.

Una implementación de la LOPD debe de estar acompañado de un plan de auditoría interna adecuado con un enfoque de control interno también adecuado. Existen varios enfoques como son el emitido por COSO (Committe of Sponsoring Organitation of the Tradeway Commission) en 1992 conocido como el Enfoque Integrado de Control Interno, también la Guía de Control más bien conocida como el enfoque CoCo publicada en 1995 por el Instituto Canadiense de Contadores Certificados, la Guía de control interno para directores sobre el código combinado conocida también como el Informe Turnbull publicado en el año 1999 por el Instituto de Contadores Certificados de Inglaterra y Gales y por último el enfoque de control interno para la tecnología de la información, COBIT. Este último no constituye un enfoque completo para el enfoque de control interno de una empresa.

Luego de analizar diferentes enfoques de control interno como son COSO, CoCo y Turnbull en el capítulo #5 del libro Auditoría Interna: Servicios de aseguramiento y consultoría de la Fundación de Investigaciones del IIA, se concluye que no existen diferencias sustanciales entre estos enfoques ya que todos incluyen en su definición lo relativo a “proceso que brinda un grado de seguridad razonable para el logro de los

objetivos de la organización en las categorías de eficacia y eficiencia de las operaciones, confiabilidad de la información financiera y cumplimiento de las leyes y regulaciones aplicables a la industria".

El enfoque COSO consta de principios básicos que de definirse y desarrollarse correctamente contribuyen a la implementación de un ambiente de control interno óptimo en cualquier organización, estos son: la definición del entorno de control, la evaluación de riesgos, el establecimiento de las actividades de control, la definición de la información y de la comunicación, así como la actividad de supervisión del ambiente de control.

Será utilizado el enfoque COSO para la elaboración de una guía de implementación de las actividades de control necesarios para la adecuación de una empresa no financiera al cumplimiento de la LOPD 172-13 así como también para el plan de auditoría interna que contribuirá a validar el cumplimiento y a la mejora continua de la organización.

La conclusión final de este capítulo es que tanto en la República Dominicana como en la región de Iberoamérica todos los países consignan en su Constitución el derecho que tiene toda persona a que se le respeten sus datos personales, su derecho de privacidad, su intimidad tanto personal como familiar así como el respeto a su correspondencia. Un total de nueve países de veintiún países estudiados no cuentan con una legislación general destinada a la protección de datos personales de las personas pero sí cuentan con legislaciones sectoriales que atienden esta necesidad.

En el caso de la República Dominicana el país cuenta con la LOPD 172-13 así como con legislaciones sectoriales destinadas a la protección de los datos personales. La aplicación de la ley 172-13 es riguroso en el sector financiero y es monitoreado su cumplimiento por la Superintendencia de Bancos de la República Dominicana no así sucede en el sector no financiero. A la fecha de este trabajo de investigación aún cuando la ley 172-13 crea la Agencia Dominicana de Protección de Datos la misma no está operando y esta será el ente regulador tanto para el sector privado como público, financiero y no financiero que velará por su fiel cumplimiento y de sancionar al que no la cumpla.

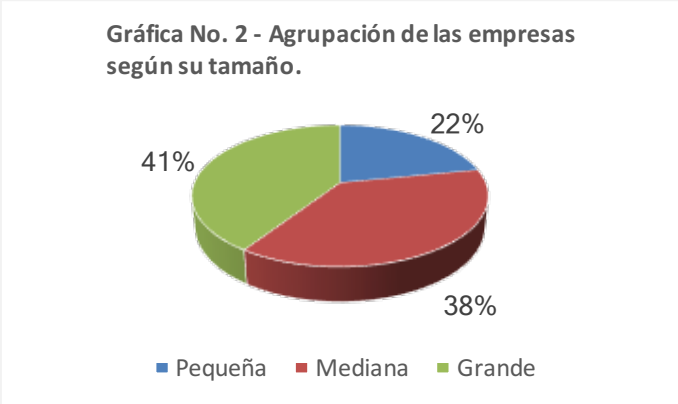
Capítulo II – Análisis del nivel de conocimiento y nivel de implementación de la LOPD en empresas no financieras en la República Dominicana.

La base del análisis para determinar el nivel de conocimiento y de implementación de la LOPD en empresas no financieras en la República Dominicana ha sido mediante la aplicación de la encuesta que para tales fines se confeccionó. La misma está estructurada con 21 preguntas cerradas las cuales se agrupan, para facilitar su análisis, en seis bloques. Un primer bloque que es el que dará el perfil del encuestado, un segundo bloque dedicado a como almacenan los datos de los clientes, un tercero que busca conocer el nivel de autorización que los clientes han otorgado a dichas empresas para que las mismas puedan compartir sus datos personales con terceros como son el caso de buros de crédito, entre otros. Un cuarto bloque para determinar los controles con los que las empresas encuestadas cuentan para la protección de datos de los clientes, el quinto bloque de preguntas enfocado a medir el tiempo con el que la empresa responde al pedido de modificación por parte de sus clientes de algunos de sus datos personales y, por último, un bloque de preguntas que buscan determinar el conocimiento que sobre la LOPD entienden estas empresas tener.

Un total de treintaidós encuestas fueron aplicadas a treinta empresas las cuales fueron agrupadas en 20 sectores de la actividad económica Nacional como se muestra en la Gráfica No. 1 a continuación.

Fuente: Elaboración propia

El 60% de las encuestas aplicadas se concentran en los sectores de: servicios con un 19%, el sector telecomunicaciones con un 9% y con un 6% cada uno los sectores de educación o docencia, mayoristas, fabricación, médica y supermercados. El restante 40% de las encuestas, distribuidas en 13 diferentes sectores económicos que representan el 65% de estos. Otro dato interesante del perfil de las empresas encuestadas es la distribución porcentual de estas en relación a su tamaño como se muestra en la Gráfica No. 2.



Fuente: Elaboración propia

El 41% de las 13 empresas encuestadas se encuentran en el rango de empresas grandes agrupadas en los sectores económicos definidos de fabricación, construcción, hotelería, empresas reguladoras, servicio, distribución, telecomunicaciones, generadores eléctricos, agrícola y supermercados. Un 38 % son de tamaño mediano pertenecientes a los sectores de bienes raíces, servicio, librería, docencia, mayorista, seguridad, importador, supermercados y auditoría. El 22% restante corresponde a las pequeñas distribuidas en los sectores de servicio, médica, mayorista y asegurador. En este análisis los sectores comunes entre los diferentes tamaños de empresas son los de servicio presente en los tres rangos definidos y el de mayorista solo presente en los rangos de mediana y pequeña empresa.

El segundo bloque de preguntas de la encuesta, dirigido al almacenamiento de los datos de carácter personal, lo componen cinco preguntas donde una de ellas busca re confirmar el hecho de que las empresas encuestadas sí llevan archivos de datos de carácter personal. Las otras cuatro preguntas dirigidas a la forma en como lo hacen, sí

son almacenadas en lugares seguros, el tipo de acceso a esos lugares de almacenamiento y al tiempo en que son conservados.

De este bloque la primera pregunta realizada es la que buscaba re confirmar sí las empresas mantienen archivos de datos de carácter personales no importando su tamaño y el tiempo de estas en operación. El resultado obtenido es que efectivamente el 100% de las treintaidós empresas encuestadas si los llevan, generándose así de manera implícita una responsabilidad de parte de ellas sobre estos datos según lo estipula la LOPD 172-13 de la República Dominicana.

La segunda pregunta estaba dirigida a determinar la existencia en las empresas de algún proceso definido de registro y archivo. El resultado es que una, tamaño pequeño perteneciente al sector comercial de mayoristas con menos de cinco años de operación, de las treinta empresas encuestadas no cuenta con un proceso definido para estos fines.

La tercera y cuarta pregunta del bloque estuvieron dirigidas a determinar si los datos personales de los clientes son almacenados en lugares seguros y a como se da el acceso a estos lugares respectivamente. El resultado obtenido se muestra en la Gráfica No. 3 y Gráfica No 4.

Fuente: Elaboración propia

Como se puede observar un 6% de las empresas no almacenan los datos personales de los clientes en lugares seguros. En este mismo orden, igual porcentaje de estas empresas presentan que el acceso a estos lugares de almacenamiento es abierto, o sea, no restringido. Una empresa grande del sector servicios con 5 a 10 años de operación es común en ambas gráficas esto debido a que no almacena los

datos personales de los clientes en un lugar seguro y el acceso a los mismos no es restringido tampoco. Lo mismo no sucede con la empresa que completa el 6% para cada caso. En la tercera pregunta la empresa que lo completa es del sector auditoría, de tamaño mediano con más de 30 años de operación la cual no almacena en lugar seguro pero su acceso es restringido. En el caso de la cuarta pregunta la empresa es del sector agrícola, de tamaño grande con más de 30 años de operación la cual cuenta con acceso no restringido a los lugares donde almacenan, pero en su entendido de que almacena en un lugar seguro.

La quinta y última pregunta del bloque busca determinar el período de tiempo promedio que las empresas conservan los datos de los clientes en sus archivos. El 100% de las empresas encuestadas guardan por años estos archivos. Un total de nueve personas encuestadas además de seleccionar la respuesta colocaron la cantidad de años en que sus empresas almacenan los datos de carácter personal de los clientes como se muestra en la Tabla No. 3 que se presenta a continuación:

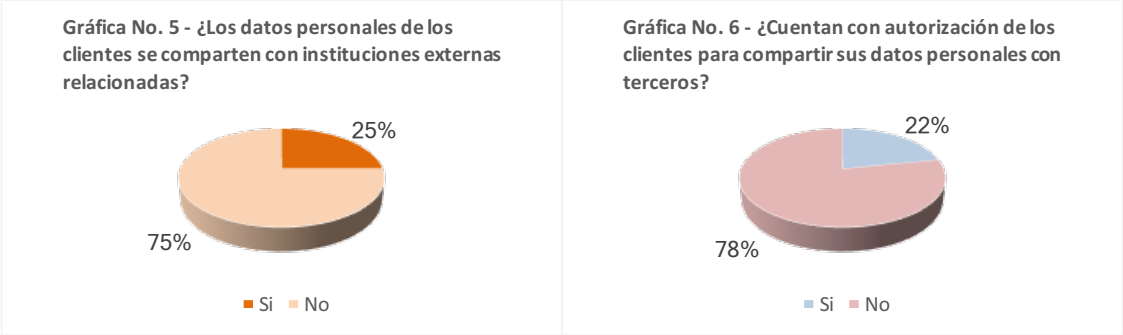
Tabla No. 3 Encuestas donde el encuestado indicó la cantidad de años de almacenamiento en su empresa.

Sector Económico	Tiempo Operación	Tamaño Empresa	Tiempo Almacenamiento (años)
Construcción	Más de 10 años	Grande	10
Mayorista	4 años	Pequeña	10
Reguladora	16 años	Grande	4
Servicios	6 años	Grande	5
Importadora	20 años	Mediana	10
Auditoría	40 años	Mediana	7
Telecomunicación	87 años	Grande	10
Telecomunicación	80 años	Grande	3
Telecomunicación	80 años	Grande	Más de 2

Fuente: Elaboración propia

Un dato importante a resaltar es el de la telecomunicación, por los años que los encuestados indican tiene la empresa se concluye las tres personas laboran para la misma empresa y su conocimiento en relación al tiempo en que los datos son mantenidos varían de uno a otro indicando esto que esta información no es comúnmente compartida a sus colaboradores.

El tercer bloque de preguntas estuvo dirigido a conocer el nivel de autorización que las empresas obtienen de sus clientes para poder compartir y consultar con terceros sus datos de carácter personal. Lo componen tres preguntas, una primera para confirmar si se comparten los datos ver Grafica No. 5, otra que buscaba validar si se cuenta con la autorización correspondiente, ver Gráfica No. 6 y la última si se cuenta con la debida autorización para que la empresa pueda consultar información de sus clientes en los burós de crédito. A continuación, se muestra gráficamente los resultados así también puntualizaciones sobre los mismos.



Fuente: Elaboración propia

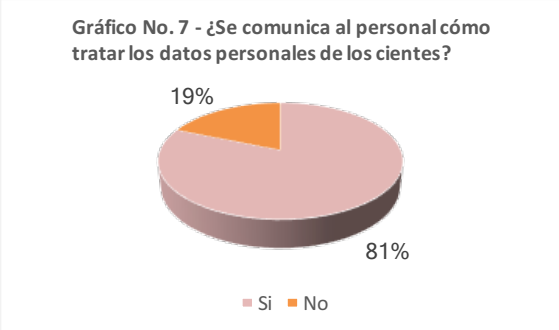
La primera pregunta fue dirigida a establecer si entre empresas relacionadas dentro de un mismo grupo empresarial los datos de los clientes son compartidos obteniéndose que 25% de las empresas si lo comparten y un 75% no. En este mismo orden, la segunda pregunta del bloque buscaba determinar si se obtienen las autorizaciones correspondientes por parte de los clientes para compartir con terceros sus datos observándose que el 78% de las empresas no obtienen autorización versus el 22% que sí la obtienen. El porcentaje de las empresas que, si comparten los datos de sus clientes con empresas relacionadas versus el porcentaje de autorización con el que cuenta para compartir con terceros los datos, un 25% versus un 22% respectivamente, nos muestra que violaciones relacionadas con la ley 172-13 acontecen en empresas del sector no financiero. En este ejercicio cinco de las treintaidós encuestadas pertenecientes a los sectores de seguridad, médica, reguladora, hotelería y docencia no cumplen con el principio de la ley.

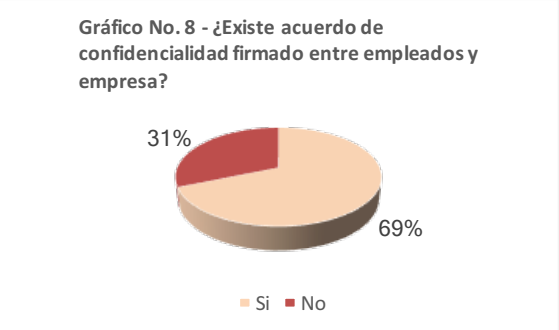
La última pregunta de este tercer bloque está enfocada en ver el cumplimiento de informar y obtener del cliente la autorización correspondiente para consultar sus datos

en los Burós de Crédito con la finalidad de ser depurados. El resultado obtenido es que un 66% de las empresas no cuentan con la debida autorización versus el 34% que sí. El consultar en Burós de Crédito sin el consentimiento escrito previo de los clientes o potenciales clientes atenta contra su privacidad y es considerado una violación a la ley 172-13 con penalidades en ella estipuladas para el infractor.

El cuarto bloque de preguntas estaba dirigido a determinar el control que para con la protección de los datos de los clientes cuentan las empresas del sector no financiero. Está conformado por siete preguntas las cuales evalúan la comunicación y el compromiso que el personal recibe y asume con la empresa. También, si la organización cuenta con controles, procedimientos y ejercicios de evaluación de riegos.

Las primeras dos preguntas de este bloque están relacionadas a la comunicación que los empleados reciben de la empresa de cómo tratar los datos personales de los clientes y la segunda a si entre empleado – empresa existe un acuerdo de confidencialidad establecido. Los resultados presentados en las gráficas de más abajo muestran que el 81% de las empresas, Gráfico No. 7, sí informan a sus empleados la responsabilidad que conlleva el obtener, gestionar y almacenar los datos de los clientes, aunque solo un 69%, Gráfico No. 8, de las empresas analizadas establecen acuerdo de confidencialidad empleado – empleador.

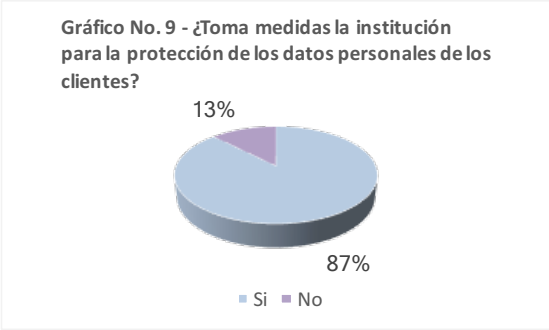


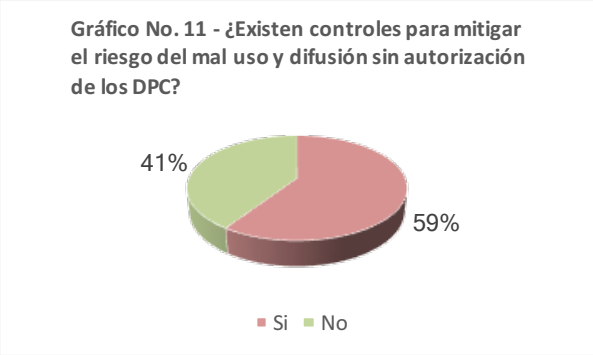


Fuente: Elaboración propia

Las siguientes tres preguntas del bloque están enfocadas en determinar si las empresas toman medidas, si cuenta con procedimiento definidos y si establecen controles para la protección de la data personal de los clientes. El resultado de la

primera de estas preguntas, Gráfico No. 9, es que el 87% de las empresas si toman medidas versus el 13% que no lo hacen. El resultado de la segunda pregunta, Gráfico No. 10, contrasta un poco con los resultados de la pregunta anterior ya que muestran que solo un 62% si cuentan con algún procedimiento establecido para el manejo de los datos de los clientes y un 38% no. El resultado obtenido en la pregunta tres, Gráfico No. 11, contrasta tanto con la pregunta anterior como con la primera de este bloque ya que solo un 59% de las empresas cuenta con controles que mitiguen el riesgo del mal uso y difusión de los clientes versus el 41% que no. Para un mejor entendimiento de lo expuesto en este párrafo se grafican a continuación estos resultados.



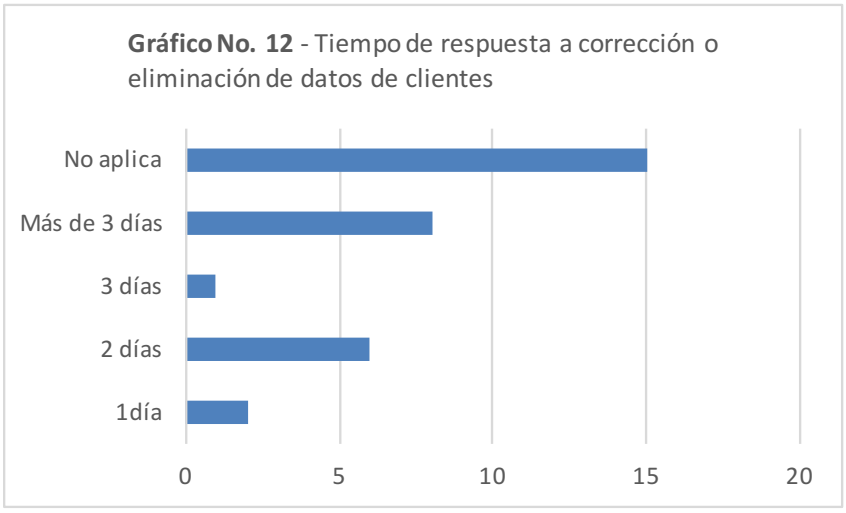


Fuente: Elaboración propia

Como análisis final a estas tres preguntas se puede concluir que aun cuando existe la intención de tomar medidas en el 83% de las empresas, solo un 62% define algún procedimiento y solo un 59% establece controles para mitigar los riesgos de uso no adecuado de los datos de los clientes evidenciándose así una oportunidad en el sector no financiero para con el cumplimiento de la LOPD 172-13.

Las últimas dos preguntas de este cuarto bloque buscan determinar si se identifican los riesgos inherentes al proceso de almacenamiento de datos de los clientes y si se evalúan los controles existentes. El resultado a la primera es que un 78% si identifica los riesgos mientras un 22% no lo hacen. En este mismo orden, un 69% sí evalúa los controles existentes para mitigar estos riesgos versus un 31% que no lo hacen.

El quinto bloque de preguntas dirigido a determinar si los clientes solicitan a las empresas no financieras en algún momento modificación de sus datos personales y en caso afirmativo el tiempo que toma llevar a cabo dicha solicitud. El resultado obtenido a la primera pregunta es que el 56% de las empresas si han recibido de sus clientes solicitud de modificación de sus datos versus un 44% que dice no haber recibido solicitud. Razones varias pueden existir para que este resultado sea así pero no es parte del alcance de éste trabajo determinar estas razones. Lo que sí se puede observar es que una vez se registraron por primera vez los datos de los clientes la actividad de actualización de los mismo no es común en empresas no financieras. El resultado de la segunda pregunta se aprecia en el Gráfico No. 12.



Fuente: Elaboración propia

Con excepción de una empresa perteneciente al sector agrícola, en 15 de las encuestas la respuesta fue no aplica. Esto en relación con el 44% de las empresas que indicaron no haber recibido de parte de sus clientes solicitud de modificación de los

datos personales. De las encuestas restantes el plazo de tiempo mayor se encuentra en 8 de ellas con un plazo de tiempo de más de 3 días para efectuar el cambio solicitado por el cliente.

El último bloque de preguntas de la encuesta dirigido a determinar el conocimiento que de la LOPD 172-13 tienen las empresas del sector no financiero y en caso afirmativo si cuentan con alguna guía, manual o plan de auditoría que les ayude a cumplir con ella. La primera pregunta de este bloque buscaba determinar que tanto se conoce la ley LOPD 172-13 resultando que un 62.5%, un total de 20 encuestas, indicó que sí versus el 37.5%, de las restantes 12 encuestas, que marcaron no. La segunda pregunta estaba enfocada en el nivel de conocimiento que de la ley poseen las empresas encuestadas que respondieron afirmativamente la primera pregunta de este bloque, resultando que 3 poseen un nivel bajo, 10 un nivel medio y 7 un nivel amplio. Por último, se les preguntó si cuentan con un manual que garantice la aplicación y cumplimiento de la ley obteniéndose que solamente 8 empresas, un 26.6%, de las 30 empresas encuestadas si cuentan con un manual que garantice su aplicación. El 75% de estas empresas de tamaño grande pertenecientes a los sectores económicos de fabricación, regulador, hotelería, distribución y telecomunicación. El 25% restante de tamaño mediano y pertenecientes al sector de la auditoría.

La conclusión final del análisis es que es poco el conocimiento que fuera del sector financiero tienen las empresas sobre la ley LOPD 172-13 y se desconoce el alcance de la misma, así como también las consecuencias de no cumplirla. Una guía de implementación que permita de forma ágil adecuar o crear los procedimientos en las empresas del sector no financiero para que en el manejo de los datos de carácter personal de sus clientes cumplan con lo que la ley estipula es de gran importancia, también el difundir este trabajo como un todo entre ellas para crear la conciencia suficiente ya que así estarán en la capacidad de brindar a sus clientes la seguridad de que su privacidad está siendo resguardada así como a contribuir en el nivel de formalización de las operaciones de las empresas.

Capítulo III – Guía de implementación de un Plan de Auditoría Interna para la Protección de Datos de Carácter Personal con un enfoque COSO.

El objetivo de este capítulo, como se mencionó anteriormente, es presentar una guía de implementación para empresas no financieras, que contribuya al logro del cumplimiento de la ley orgánica de protección de datos 172-13 actualmente vigente en la República Dominicana, así como diseñar un plan de auditoria interna que permita evaluar el cumplimiento de esta guía.

La ley 172-13 establece que las empresas deben contar con un manual interno que garantice el cumplimiento de la LOPD. Con la finalidad de elaborar una guía adecuada para tales fines, se trabajará esta guía bajo el enfoque de control interno COSO, ya que el mismo proporciona un marco de referencia que puede ser aplicable en cualquier empresa. El mismo, también es considerado internacionalmente entre los tres mejores enfoques aceptados de control interno tanto por auditores externos e internos, encargados de dirección y contadores, llegando a ser para algunos el estándar de referencia.

Esta guía bajo este modelo de control interno, brindará a las empresas no financieras una seguridad razonable sobre la protección de los datos personales de sus clientes que se encuentren asentados en archivos y registros, cumpliendo así con el artículo 5 de la ley 172-13 que establece la responsabilidad de la entidad sobre los datos personales que posee y enfatiza sobre las medidas de diferentes índoles necesarias que deben adoptar e implementar las empresas para asegurar los datos de carácter personal.

El enfoque COSO está diseñado con el objetivo de brindar una seguridad razonable a la administración y al consejo mediante la identificación de acontecimientos que tienen cierta probabilidad de ocurrencia, que puedan afectar significativamente a la organización y que estos sean administrados de tal manera que mediante la implementación de controles internos mitiguen el riesgo de impacto y probabilidad ayudando al logro de los objetivos de la empresa. Este enfoque de control interno está compuesto por cincos principios básicos identificados como:

Entorno de Control, Evaluación de Riesgos, Actividades de Control, Información y Comunicación y Supervisión. Estos principios serán abordados en detalles más adelante con el desarrollo de la guía de implementación.

Para COSO el control interno es un proceso que se lleva a cabo por el consejo de administración, por su grupo directivo y por todo el personal que labora en la institución. El proceso está diseñado para brindar a la organización seguridad razonable en relación a los objetivos propuestos, y están distribuidos en las siguientes categorías: eficiencia y eficacia de las operaciones, confiabilidad de las informaciones financieras y el cumplimiento de las leyes y regulaciones establecidas. Cabe destacar que para una buena implementación de esta guía de adecuación de una empresa no financiera a la LOPD 172-13, que el control interno es un proceso repetitivo y permanente, donde varios componentes influyen para formar e integrar un sistema que reaccione a las condiciones cambiantes que enfrenta la empresa. Un plan de auditoría interna para verificar la efectividad de la implementación de lo contenido en la guía de adecuación, como se presentará más adelante en este trabajo, es de gran importancia.

La definición de COSO sobre el control interno muestra algunos conceptos fundamentales que se consideran relevantes resaltar, entre ellos, que el control interno es un proceso que representa un medio para poder llegar a un fin, este proceso es ejecutado por personas en todos los niveles de la organización dando a entender que el control interno es algo más que manuales, formularios, políticas etc. Con la implementación de los controles no se espera una seguridad absoluta sobre los riesgos en la organización, sino una seguridad razonable para el consejo y la dirección. Los controles están pensados para ayudar a la organización a alcanzar sus logros y objetivos en diferentes categorías, pero con elementos en común.

A continuación, se desarrollarán los cinco principios de control interno establecidos por COSO. Al final de cada principio se presentará la guía de implementación correspondiente.

3.1 Entorno de control.

Así como la ley orgánica de protección de datos tiene el objetivo de crear un ambiente de control en todo el territorio dominicano que estimule las actividades de datos personales mediante el cumplimiento de la ley 172-13, el objetivo de este principio (Entorno de Control) es establecer un ambiente de control que estimule las actividades realizadas por todo el personal de la organización, con la intención de crear conciencia en cada individuo sobre la importancia del control. Este principio es la base fundamental que va a sostener los demás principios y componentes del control interno que se implementaran. Es en este punto donde se establece el estilo operativo y la filosofía de la dirección, cual es la manera en que la dirección delegara la responsabilidad y autoridad, cuál es el compromiso de la misma con el control interno, como se organiza y desarrolla el personal, la forma en cómo se comunican los valores y principios de la organización. El ambiente de control de una organización se ve influenciado por su historia y su cultura, lo cual influye en sus integrantes para la comprensión de lo importante que es el control interno. Los factores del entorno de control se componen de (a) Integridad y valores éticos; (b) Consejo de Administración; (c) Autoridad y responsabilidad y (d) Recursos Humanos.

a. Integridad y valores éticos.

El objetivo de este factor es desarrollar y dar a conocer en todos los niveles de la organización las normas de conducta que debe seguir todo el personal. La ley 172-13 hace referencia a este factor ya que se sustenta en cinco principios los cuales se mencionan a continuación. Primero, la licitud de los archivos de datos y la calidad con la que deben contar los datos, así como el derecho de informar al titular el tratamiento que le darán a sus datos. Segundo, el deber de secreto profesional que debe tener cada integrante de la empresa con relación a las informaciones de carácter personal que están bajo su cargo. Tercero, la forma en la cual deben ser asentados los datos de carácter personal. Cuarto, el manejo de los mismos para ser compartidos y quinto, los datos de carácter personal no pueden ser utilizados para otro fin que el que se le informo a la persona.

b. Consejo de Administración.

Este factor busca que el consejo comprenda los procesos realizados bajo su supervisión y como se asocia el control interno con estos procesos.

c. Autoridad y responsabilidad.

El objetivo fundamental de este factor es establecer los niveles de responsabilidad adecuada que deben existir dentro de la organización para facilitar y asegurar la eficacia del control interno. Para garantizar un adecuado manejo de los datos de carácter personal y un fiel cumplimiento de la ley 172-13 se hace necesario delegar responsabilidad dentro de la empresa que faciliten la ejecución y supervisión del control interno.

d. Recursos humanos:

Este factor tiene el objetivo de implementar las políticas y prácticas que debe seguir el personal para facilitar el control interno y la eficacia de las operaciones.

A continuación, en la Tabla No. 4, se presenta una guía de implementación del entorno de control en una organización no financiera donde se detallan los aspectos que deben de implementarse, las evidencias que deben obtenerse de los resultados de estas implementaciones así como la responsabilidad de estos aspectos.

Tabla No. 4 - Guía de implementación para empresa no financieras ley 172-13 - Principio entorno de control COSO.

Aspectos a Implementar	Evidencia a Mostrar	Consejo Administración	Dirección	Demás Personal
Compromiso con los objetivos, principios y valores éticos de la institución sobre la protección de datos personales de los clientes.	Carta compromiso firmada por cada empleado.	X	X	X
Proceso de crear y modificar el manual de objetivos, procedimientos, normas y políticas destinado a la protección de datos de carácter personal de los clientes.	Minutas de las reuniones y manual actualizado.	X	X	

Tabla No. 4 - Guía de implementación para empresa no financieras ley 172-13 - Principio entorno de control COSO. (Continuación)

Aspectos a Implementar	Evidencia a Mostrar	Consejo Administración	Dirección	Demás Personal
Evaluación de los riesgos que puedan afectar el logro de los objetivos para la protección de los datos personales..	Resultados taller de autoevaluación de riesgos.	X	X	
Comunicación institucional a toda la organización de las políticas y normas establecidas para la protección de datos de carácter personal de los clientes.	Lista asistencia empleados en actividades de reinducción.		X	
Establecer líneas de denuncias que permitan recibir o identificar violaciones y/o desviaciones de las políticas de protección de datos de carácter personal de los clientes.	Reporte de las líneas de denuncias.	X	X	X
Proceso de revisión de los reportes de violaciones y/o desviaciones del cumplimiento de las políticas de protección de datos de carácter personal.	Plan de acciones para mitigar violaciones y/o desviaciones.	X	X	
Revisiones semestrales del Consejo a la ejecución de la Dirección.	Minutas de las reuniones de revisión.	X		

Fuente: Elaboración propia

Con estos aspectos a implementar se crea un entorno de control interno confiable, que promueve la iniciativa e influencia a todo el personal de la empresa a involucrarse en el logro de los objetivos de salvaguardar los datos de carácter personal de sus clientes. Con esta base se puede pasar a abordar la segunda parte del enfoque COSO: la evaluación de riesgos.

3.2 Evaluación de riesgos.

En toda entidad del sector no financiero existe una gran variedad de riesgos que provienen de fuentes internas y fuentes externas asociados a los datos personales que se manejan. La ley 172-13 busca mitigar los riesgos que supone corren los datos de carácter personal que se encuentran en manos de terceros, riesgos tales como,

malversación de los datos, robo de las informaciones, el uso indebido, alteraciones entre otros. El objetivo fundamental de este principio es identificar en su primera fase los riesgos relevantes inherentes al proceso de registro, almacenamiento, consultas entre otros, que ponen en peligro no solo los datos personales de los clientes, sino también hasta a la misma empresa. La finalidad de identificar estos riesgos es analizarlos y crear las bases para determinar en qué forma éstos pueden ser mitigados a niveles óptimos.

Este principio no solo se enfoca en los riesgos internos de la organización, sino que va más allá, analizando los riesgos que supone el entorno externo, mediante mecanismos efectivos que logren identificarlos y ser evaluados por la gerencia para tomar las acciones de lugar. Con la adecuación de este principio a la guía de adecuación de la ley 172-13 se puede destacar que en toda empresa se hace necesario establecer objetivos y actividades relevantes, con los cuales se permita tener una base sobre la cual se pueda identificar los riesgos de los datos de carácter personal y analizar los factores que amenazan el logro del cumplimiento de la ley. Los factores de la evaluación de riesgos se componen de (a) Objetivos de la protección de datos de carácter personal; (b) Riesgos asociados con el almacenamiento de los datos personales y (c) Riesgo de fraude:

a. Objetivos de la protección de datos de carácter personal.

La ley orgánica de protección de datos busca brindar a los ciudadanos la seguridad de que sus datos son reguardados eficazmente, y se mantienen libres de riesgos. Con la adecuación de este factor a la implementación de la guía que se propone, los directivos de la empresa deben especificar claramente cuál es el objetivo de la protección de los datos personales que mantienen en sus archivos, y cuales criterios deben ser suficientes para hacer posible la identificación de los riesgos que cada día enfrentan sus datos.

b. Riegos asociados con el almacenamiento de los datos personales.

Este factor tiene como objetivo que la empresa en todos los niveles identifique y analice los riesgos asociados a la obtención y manejo de los datos personales

almacenados en la empresa. Esto con el fin de determinar cómo serán gestionados estos riesgos asociados para disminuir al máximo su materialidad y su probabilidad de ocurrencia. En la ley 172-13 se evidencian ciertos riesgos que de no ser tratados pueden llevar a la empresa a caer en sanciones por parte del gobierno y hasta demanda por parte del titular de los datos, es por eso que se hace indispensable identificar estos riesgos establecidos en la ley y analizarlos con el fin de que se establezcan los controles que ayuden a la empresa a cumplir tanto con la ley como con sus clientes.

c. Riesgo de fraude.

La ley orgánica de protección de datos 172-13 establece que existen formas ilícitas y fraudulentas de obtener y manejar los datos de carácter personal dentro y fuera de la empresa. Cabe destacar que el objetivo de este factor es identificar la posibilidad de fraudes que pueden existir al momento de obtener y asentar en los archivos informaciones falsas que no cumplan con el principio de calidad establecido. La administración debe de considerar estos riesgos y evaluarlos para alcanzar el logro de los objetivos que de este respecto persigue la empresa.

Para ayudar a las empresas del sector no financiero a identificar y realizar un análisis de los riesgos que supone son inherentes al proceso de registros y almacenamientos de los datos personales, se presenta una guía que muestra algunos riesgos a considerar que pueden tener cierta probabilidad de ocurrencia dentro y fuera de la empresa, los riesgos aquí identificados fueron obtenidos tomando como parámetro lo dispuesto en la ley 172-13, esto no evita que puedan existir otros riesgos que puedan afectar significativamente el logro de los objetivos de salvaguardar las informaciones personales, en tal sentido se expresa que estos riegos no son de carácter limitativos o definitivos.

Con la intención de involucrar a todo el personal en el proceso de identificación y análisis de los riesgos, se presenta a continuación la Tabla No. 5 que trata sobre los riesgos del proceso de protección de datos personales. En la tabla se presentan cuarenta y dos riesgos identificados, para que en un ejercicio de autoevaluación se analice y asigne el nivel de materialidad y probabilidad determinándose así el

impacto de cada uno de ellos en la organización que esté en proceso de adecuarse a la ley 172-13. Las columnas identificadas con los números 1, 2, 3, 4 y 5 representan el número de empleados que estarían participando en la autoevaluación y en ellas cada empleado colocará su ponderación sobre el riesgo. La evaluación de los riesgos es responsabilidad de todo el personal de la organización que está involucrado en alcanzar los objetivos propuestos sobre los datos de carácter personal. Se recomienda que la empresa realice actividades de autoevaluación de estos riegos, donde participe la mayor cantidad del personal que está involucrado en el manejo de datos de carácter personal. Este ejercicio también ayudará a que el personal tenga una mejor visión de los riegos y hará más fácil establecer el nivel de impacto que estos tienen sobre los objetivos de la empresa. La guía de riesgo debe ser llenada dos veces, una para asignar los niveles de materialidad y la segunda para asignar los niveles de probabilidad.

Tabla No. 5 - Riesgos del proceso de protección de datos personales.

#	Riesgos	# 1	# 2	# 3	# 4	# 5	Promedio
1	No tener un proceso definido de cómo se deben almacenar y registrar los datos personales.						
2	No contar con una política definida sobre el manejo de los datos personales.						
3	No comunicar las políticas sobre el manejo de los datos personales.						
4	El personal desconozca las políticas sobre el manejo de los datos personales.						
5	No tener acuerdos de confidencialidad con sus empleados.						
6	Incumplimiento del acuerdo de confidencialidad mediante divulgación de los datos personales por parte de los empleados.						
7	No contar con área segura y las herramientas adecuadas para la protección y registros de los datos de carácter personal.						
8	Registrar datos de carácter personal en registros que no cumplen las condiciones técnicas de seguridad e integridad.						
9	Registrar datos sin el consentimiento del titular.						

Tabla No. 5 - Riesgos del proceso de protección de datos personales. (Continuación)

#	Riesgos	# 1	# 2	# 3	# 4	# 5	Promedio
10	Recoger informaciones personales por medios fraudulentos o ilícitos.						
11	No informar al titular cual será la finalidad y uso de sus datos.						
12	No informar al titular los destinatarios con los que se va a compartir sus datos.						
13	Acceder a bases de datos para consultar información personales sin autorización del titular.						
14	Compartir información con terceros no autorizados por el titular.						
15	Utilizar los datos personales de terceros para beneficios personales.						
16	Uso de datos personales sin aprobación del titular.						
17	Consulta en los buros de los datos personales sin autorización escrita del titular.						
18	No contar con la autorización de los clientes para compartir sus datos personales.						
19	No guardar las autorizaciones por el tiempo establecido.						
20	Utilizar los datos de carácter personal para finalidades contrarias a las establecidas en la ley 172-13.						
21	Los datos personales recopilados que no sean ciertos, adecuados y pertinentes para la finalidad que se tomó.						
22	Actualización inadecuada en la corrección de datos personales.						
23	Que los datos personales sean susceptibles de alteraciones o modificaciones.						
24	Permitir el acceso a la información a personas que no tienen derecho a ella.						
25	Datos personales sustraídos de las bases de datos por terceros mal intencionados.						
26	No garantizarle al titular de los datos el derecho de habeas datas sin importar las circunstancias.						
27	Negar el acceso al titular de sus datos archivados.						
28	Negar sin ningún fundamento una solicitud de revisión o modificación por parte del titular.						
29	No tramitar las consultas y reclamos realizado por los titulares.						
30	No suprimir o sustituir los datos incompletos o parcialmente inexactos.						

Tabla No. 5 - Riesgos del proceso de protección de datos personales. (Continuación)

#	Riesgos	# 1	# 2	# 3	# 4	# 5	Promedio
31	No cumplir con el tiempo establecido para las correcciones y/o eliminación de los datos personales solicitados por el titular.						
32	Eliminar o corregir los datos personales cuando el titular está en un proceso judicial o administrativo.						
33	Perdida accidental o robo de los datos almacenados.						
34	Destrucción por siniestro o contaminación mediante virus informáticos.						
35	No proceder a tiempo con las reclamaciones de, rectificación, actualización o suspensión de los datos personales.						
36	Realizar cargos por el servicio de actualización, rectificación o supresión de los datos personales incompletos o inexactos.						
37	No contar con una herramienta de contingencia de recuperación de datos personales.						
38	No realizar backup sobre los registros existentes de los datos personales para salvaguardarlo.						
39	Acceder de manera fraudulenta a bases de datos no autorizadas.						
40	Utilizar reportes de datos personales suministrados por otra compañía.						
41	No conocer la ley orgánica de protección de datos 172-13.						
42	No contar con un manual que garantice el cumplimiento de la ley orgánica de protección de datos 172-13.						

Fuente: Elaboración propia

La ocurrencia o probabilidad de estos riesgos se dividen en cinco categorías con niveles ascendentes, ver delante en la Tabla No. 6, los mismos serian: remota (0,1,2), posible (3,4), razonablemente posible (5,6), probable (7,8), casi seguro (9).

Tabla No. 6 – Probabilidad ocurrencia de riesgos

Puntuación	Categoría	Definición
0,1,2	Remota	El evento o situación solamente podría ocurrir en circunstancias excepcionales.
3, 4	Posible	Existe una probabilidad de que la situación ocurra.
5, 6	Razonablemente posible	Se espera que el evento ocurra ocasionalmente en algunos pocos casos.
7, 8	Probable	Se espera que el evento ocurra en muchos de los casos.
9	Casi seguro	Se espera el evento ocurra siempre.

Fuente: Elaboración propia

De igual forma se va a clasificar en cinco categorías con niveles ascendentes el impacto o materialidad de estos riesgos, ver Tabla No. 7, los mismos serian: Insignificante (0,1,2), Moderado (3,4), Significativo (5,6), Alto (7,8), Muy Alto (9).

Tabla No. 7 – Impacto o Materialidad de los Riesgos

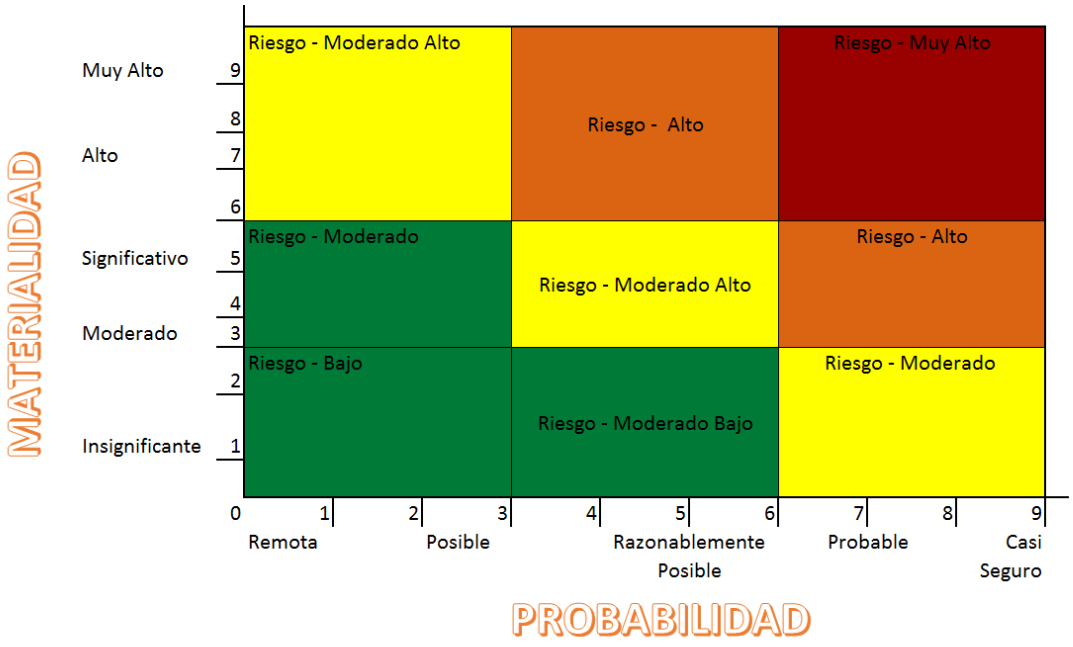
Puntuación	Categoría	Definición
0, 1, 2	Insignificante	Posibilidad de pérdida inmaterial. No requiere atención por parte de la dirección. No se requieren cambios en respuesta a estos riesgos.
3, 4	Moderado	Posibilidad de pérdida financiera moderada, sino se maneja adecuadamente la perdida podría ser significativa. La dirección está envuelta en corrección de problemas oportunos.
5, 6	Significativo	Perdida financiera significativa. La situación no afecta la habilidad de la organización para seguir operando.
7, 8	Alto	Perdida financiera relevante. La situación podría afectar la habilidad de la organización para seguir operando.
9	Muy alto	Perdida financiera considerable. La situación afecta la habilidad de la organización para seguir operando.

Fuente: Elaboración propia

Luego que cada persona o equipo, en el ejercicio de autoevaluación, asigne en la Tabla No. 5 los niveles de probabilidad y materialidad que entiendan corresponden, se realizara un promedio por riesgo en la columna identificada con este nombre en la misma tabla. Este promedio servirá para unir los criterios de todo el personal y sacar un solo resultado final.

Para brindar una mejor visualización de los resultados que se obtengan del ejercicio de autoevaluación, se procederá a graficar la relación que existe entre la materialidad y la probabilidad de cada riesgo, como se muestra en la Gráfica No. 13, para así poder observar en cuales cuadrantes se encuentran los riesgos identificados y analizados.

Gráfica No. 13 – Cuadrante de materialidad y probabilidad del riesgo.



Fuente: Kurt F. 2009

Esta gráfica sirve para ayudar a la dirección y a todo el personal a conocer cuál es la realidad que tienen sobre los riesgos inherentes al proceso de recolección y almacenamiento de datos personales, y arroja luz al nivel de cumplimiento que existe dentro de la empresa sobre la ley orgánica de protección de datos. Los resultados

ayudarán a crear conciencia en todos los niveles y en todo el personal de la empresa sobre la importancia del control interno y facilitará a la dirección la toma de decisiones para crear controles efectivos que logren reducir a su máxima expresión la materialidad y probabilidad de estos riesgos.

Luego de realizada la autoevaluación de los riesgos, la misma debe ser entregada a los auditores internos para su revisión y seguimiento. En caso de no contar con un departamento de auditoria interna, se puede contratar a un externo o asignar a alguien de la empresa la responsabilidad de revisar la autoevaluación y asegurar que la misma corresponden apropiadamente al enfoque, objetivos y alcance de la empresa.

3.3 Actividades de control.

Como se mencionó anteriormente, la ley orgánica de protección de datos establece que las entidades que manejan datos de carácter personales deben de contar con un manual de políticas y procedimientos que les ayude a cumplir con lo establecido en la ley 172-13. Luego de haber identificado algunos riesgos reales o potenciales que pueden tener ocurrencia en la empresa se hace imprescindible crear las actividades de control que se deben desarrollar para mitigar esos riesgos. Este principio se centra en las actividades que debe desarrollar la gerencia y todo el personal de la empresa para poder cumplir cada día con las actividades asignadas a sus puestos. Dichas actividades suelen estar expresadas en los procedimientos, políticas y los sistemas instalados. Las actividades de control deben de ser llevadas a cabo en todos los niveles y funciones de la empresa por todo el personal. Las actividades de control son muy diversas y dependerán del tipo de organización y enfoques. Por ejemplo, se pueden citar actividades de control como son autorizaciones, revisiones, aprobaciones, verificaciones, etc.

Algunas de las características de las actividades de control es que la misma pueden ser administrativas u operacionales, pueden ser generales o específicas, manuales o computarizada, así como pueden ser preventivas con la intención de prevenir la ocurrencia de los riesgos o de detección con la intención de detectar los

riesgos. Lo importante de esto es que sin importar las categorías todas ellas apuntan al mismo objetivo que son los riesgos, sean estos riesgos potenciales o riesgos reales. El objetivo primordial de este principio es ayudar alcanzar el logro de los objetivos de la empresa, así como salvaguardar los recursos propios y los recursos ajenos que la empresa tiene bajo su poder, en este caso los recursos ajenos que la empresa posee son las informaciones de carácter personal de terceros que se encuentran registradas en sus sistemas de información, sean estos manuales o computarizados.

La importancia de la actividad de control radica en que la mismas enseñan y fomenta la forma correcta de hacer las cosas y que son el medio que reúne las condiciones necesarias para asegurar en el nivel más alto el logro de los objetivos. Los factores de las actividades de control se componen de: (a) Políticas y procedimientos y (b) Tecnología de la información.

a. Políticas y procedimientos.

El objetivo de este factor es establecer y comunicar las políticas y procedimientos relacionados con el tratamiento de las informaciones de carácter personal en todos los niveles de la empresa. Las políticas y procedimientos ayudaran a que todo el personal conozca y ejecute su actividad de forma eficaz cumpliendo con las normas de la empresa y logrando alcanzar la seguridad razonable sobre las informaciones de carácter personal frente a los riesgos. Las políticas y procedimientos establecidos deben obedecer a la prevención de uno o varios riesgos.

A todos los niveles en las empresas existen personas que ejecutan diversas actividades por lo que se hace necesario que todo el personal conozca cuales son las policitas y procedimientos aplicables a su actividad. Como en esta guía se hace un enfoque en las actividades de recolectar, almacenar, proteger y compartir los datos de carácter personal de los clientes, las políticas (Tabla No. 8) y procedimientos (Tabla No. 9) que se describirán más adelante solo estarán basados en esta actividad.

b. Tecnología de la información.

Este factor es de aplicación para las empresas que utilizan sistemas informáticos para registra y almacenar los datos de carácter personal, no aplica para las empresas

que llevan registros manuales. El objetivo de este factor es diseñar e implementar los controles pertinentes para el funcionamiento de las herramientas tecnológicas utilizadas, que contribuyan a la protección de los datos personales y el logro de los objetivos de la empresa.

A continuación se presenta la Tabla No. 8 en la cual se listan las políticas que en esta guía se recomiendan implementar así como el riesgo que de no implementarlas pudiera estar sometida la organización.

Tabla No. 8 – Guía de implementación para empresa no financieras ley 172-13 - Principio actividades de control COSO – Políticas

#	Políticas	Riesgos
1	Manejo de los datos de carácter personal de los clientes.	No cumplir con lo consignado en la LOPD
2	Comunicación y distribución interna de las políticas y procedimientos relacionados con los datos de carácter personal.	Violaciones a lo consignado en la LOPD
3	Amonestación y sanciones por violación al cumplimiento de lo establecido por la empresa para el cumplimiento de la LOPD.	Que se pierda el compromiso de los empleados de la organización.
4	Acceso a los sistemas informáticos y/o areas físicas donde se almacenen los datos de carácter personal de los clientes.	Que los datos personales sean susceptibles de alteraciones o modificaciones. Permitir el acceso a la información a personas que no tienen derecho a ella.
5	Captura, consulta y distribución de los datos de carácter personal de los clientes,	Recoger informaciones personales por medios fraudulentos o ilícitos. Acceder a bases de datos para consultar información personales sin autorización del titular. Utilizar los datos personales de terceros para beneficios personales. Utilizar los datos de carácter personal para finalidades contrarias a las establecida en la ley 172-13

Fuente: Elaboración propia

El siguiente paso luego de establecidas las políticas para el cumplimiento de la LOPD es el establecimiento de los procedimientos. A continuación se presenta la Tabla No. 9 en la cual se listan los procedimientos que en esta guía se recomiendan implementar así como el riesgo que de no implementarlos pudiera estar sometida la organización.

Tabla No. 9 – Guía de implementación para empresa no financieras ley 172-13 - Principio actividades de control COSO – Procedimientos.

#	Procedimientos	Riesgos
1	Captación y registro de las informaciones de carácter personal en la planilla física o sistema computarizado destinado para los fines.	**a.-** No tener un proceso definido de cómo se deben almacenar y registrar los datos personales. **b.-** Registrar datos de carácter personal que no cumplen las condiciones técnicas de seguridad e integridad. **c.-** Registrar datos sin el consentimiento del titular. **d.-** No informar al titular cual será la finalidad y uso de sus datos. **e.-** No informar al titular los destinatarios con los que se va a compartir sus datos. **f.-** No destruir adecuadamente los datos de carácter personal de los clientes incompletos o parcialmente inexactos. **g.-** Utilizar reportes de datos personales suministrados por otra compañía.
2	Consulta y compartir con terceros los datos de carácter personal de los clientes.	**a.-** Uso de datos personales sin aprobación del titular. **b.-** No contar con la autorización de los clientes para compartir sus datos personales. **c.-** Acceder a bases de datos para consultar información personales sin autorización del titular. **d.-** Utilizar los datos personales de terceros para beneficios personales. **e.-**Compartir información con terceros no autorizados por el titular. **f.-** Consulta en los buros de los datos personales sin autorización escrita del titular.

Tabla No. 9 – Guía de implementación para empresa no financieras ley 172-13 - Principio actividades de control COSO – Procedimientos. (Continuación)

#	Procedimientos	Riesgos
3	Actualización y verificación con el cliente de los registros de datos de carácter personal de los clientes.	**a.-** Los datos personales recopilados desactualizados y no adecuados para la finalidad que se tomó. **b.-** Actualización inadecuada en la corrección de datos personales. **c.-** Negar el acceso al titular de sus datos archivados. **d.-** Negar sin ningún fundamento una solicitud de revisión o modificación por parte del titular. **e.-**No tramitar las consultas, solicitudes de corrección y reclamos de los titulares en el tiempo previso en el procedimiento. **f.-** No destruir adecuadamente los datos de carácter personal de los clientes incompletos o parcialmente inexactos. **g.-** Eliminar o corregir los datos personales cuando el titular está en un proceso judicial o administrativo. **h.-** Realizar cargos por el servicio de actualización, rectificación o supresión de los datos personales incompletos o inexactos. **i.-**Utilizar reportes de datos personales suministrados por otra compañía.
4	Control de acceso y resguardo del área física así como del sistema de información donde se almacenan los datos de carácter personal de los clientes.	**a.-** Que los datos personales sean susceptibles de alteraciones o modificaciones. **b.-** No guardar las autorizaciones por el tiempo establecido. **c.-** Permitir el acceso a la información a personas que no tienen derecho a ella. **d.-** Datos personales sustraídos de las bases de datos por terceros mal intencionado. **e.-** Destrucción por siniestro o contaminación mediante virus informáticos.
5	Respaldo de los archivos que almacenan los datos de carácter personal de los clientes.	**a.-** No contar con una herramienta de contingencia de recuperación de datos personales. **b.-** No realizar backup sobre los registros existentes de los datos personales para salvaguardarlo. **c.-** Perdida accidental parcial de los datos almacenados. **d.-** No contar con área segura y las herramientas adecuadas para la protección y registros de los datos de carácter personal.
6	Elaborar un manual que garantice el cumplimiento de la ley orgánica de protección de datos 172-13.	No contar con un manual que garantice el cumplimiento de la ley orgánica de protección de datos 172-13.

Fuente: Elaboración propia

3.4 Información y comunicación.

El objetivo principal de la comunicación es elaborar un plan estratégico de comunicación coherente con la estrategia de la empresa. Las comunicaciones permiten y respaldan la comprensión y ejecución de los objetivos, procesos y responsabilidades individuales del control interno en todos los niveles de la organización. Es un deber el comunicar a todos los involucrados en el tratamiento de los datos personales (internos y externos) la importancia de cumplir las políticas y procedimientos de gestión de datos personales de la institución y conocer los objetivos y principios establecidos en la Ley de Protección de datos personales No.172-13.

a. Comunicación interna.

Es recomendable que la entidad cuente con un sistema de información que capture todos los datos relevantes para el desarrollo de las operaciones y se comuniquen adecuadamente a los destinatarios correspondientes y que además contenga los niveles de accesos controlados.

El departamento de Auditoría Interna debe obtener y gestionar el respaldo de la alta dirección, mediante una comunicación formal de cuál será la metodología que se debe seguir para tratar los datos personales y darla a conocer a todas las áreas de la empresa. Con esto se procura que al momento en que esta unidad de auditoría realiza el trabajo de campo sea de conocimiento general de todo el personal de que se cuenta con las autorizaciones para el acceso a las áreas y a las informaciones.

Entre los principales objetivos del factor de comunicación interna están: Seguridad de la información del personal, datos, hardware, software e instalaciones, asegurar una mayor integridad, confidencialidad y confiabilidad de la información mediante la recomendación de seguridades, controles y cumplimiento de la ley 172-13 para asegurar que la información que circulará sea la apropiada para la organización.

El personal no solo debe captar una información sino también intercambiarla para desarrollar, gestionar y controlar sus operaciones. Por lo tanto, este componente hace referencia a la forma en que las áreas operativas, administrativas y financieras de la organización identifican, capturan e intercambian información. La información es necesaria para que la entidad lleve a cabo las responsabilidades de control interno que apoyan el cumplimiento de los objetivos. La gestión de la empresa y el progreso hacia los objetivos establecidos implican que la información es necesaria en todos los niveles de la empresa, por esto se debe tener un buen manejo de la información de carácter personal y darle el tratamiento adecuado como lo establece la Ley orgánica de protección de Datos Ley No. 172-13. La mayoría de las organizaciones poseen de manera consciente o no, de manera documentada o no, uno o más procesos que involucran el tratamiento de datos personales; estos procesos deben ser identificados y controlados.

La ley 172-13 en su artículo 5-C establece que "Fuera de los fines establecidos en esta ley, se prohíbe la divulgación, la publicación, la reproducción, la transmisión y la grabación del contenido parcial o total de un reporte de cualquier tipo proveniente de una Sociedad de Información Crediticia (SIC), referente a un titular de los datos, en cualquiera de sus manifestaciones, en cualquier medio de comunicación masivo, sea impreso, televisivo, radial o electrónico". Es imprescindible dar a conocer en todas las instituciones no financieras la existencia de esta ley y cuál es su objetivo en cuanto a la protección y tratamiento de datos de carácter personal, para evitar usurpación, alteración y mal manejo de la información.

Para una adecuada información y comunicación interna se debe tener en cuenta el aspecto a implementar que se indica en la Tabla No. 10 así como la evidencia que se debe mostrar como prueba de su realización.

Tabla No. 10 - Guía de implementación para empresa no financiera ley 172-13 - Principio información y comunicación - Interna

Aspectos a Implementar	Evidencia a Mostrar	Consejo Administración	Dirección	Demás Personal
Plan estratégico de comunicación interna alineado con la estrategia de la empresa.	Plan estratégico	X	X	

Fuente: Elaboración propia

La elaboración de este plan estratégico de comunicación interna queda a criterio de la empresa la cual decidirá de acuerdo a su tamaño y recursos la mejor forma de comunicarlo.

b. Comunicación externa

Se puede realizar a través de canales de comunicación abiertos para clientes y proveedores, así como para entidades de control. Esto permite recibir mejoras en la entrega de bienes y servicios y también un desarrollo normal de las actividades, no viéndose afectadas por limitaciones legales como la ley 172-13 sobre la protección de datos de carácter personal. La comunicación recibida por las partes externas de la entidad permite tener visibilidad de cómo está funcionando el Sistema de Control Interno, cual es el entendimiento y visión que tienen los auditores externos, así como las entidades de control. Adicional a esto la comunicación externa también permite proporcionar información relevante para los accionistas, analistas financieros y demás partes externas para que en una forma amigable puedan entender la situación de la compañía, así como los riesgos por los que atraviesa.

La comunicación externa es una herramienta muy importante para las empresas ya que en esta se debe también comunicar al exterior la imagen de transparencia y respeto de la institución hacia sus clientes, proveedores e inversionistas. Una comunicación externa efectiva y eficiente con el objetivo no sólo de mejorar la imagen de la empresa sino también de conservarla, además de dar confiabilidad a los clientes, proveedores y relacionados.

La comunicación externa es parte fundamental en una organización, es una transmisión y recepción de datos que son esenciales para el buen funcionamiento de

la empresa, principalmente con los clientes, intermediarios, proveedores, competencia, etc. Gracias a esta comunicación externa se da a conocer en el campo externo cuales son las cualidades, características, productos y/o servicios que conforman una institución. De la comunicación externa dependerá la imagen que tendrán los clientes principalmente y de que tanto estén dispuestos a adquirir los productos y/o servicio.

Para una adecuada información y comunicación interna se debe tener en cuenta el aspecto a implementar que se indica en la Tabla No. 11 así como la evidencia que se debe mostrar como prueba de su realización.

Tabla No. 11 - Guía de implementación para empresa no financiera ley 172-13 - Principio información y comunicación - Externa

Aspectos a Implementar	Evidencia a Mostrar	Consejo Administración	Dirección	Demás Personal
Plan estratégico de comunicación externa alineado con la estrategia de la empresa.	Plan estratégico	X	X	

Fuente: Elaboración propia

La elaboración de este plan estratégico de comunicación interna queda a criterio de la empresa la cual decidirá de acuerdo a su tamaño y recursos la mejor forma de comunicarlo.

3.5 Supervisión.

Para una adecuada supervisión y evaluación de que se cumpla lo establecido en la LOPD a continuación se muestra un plan de auditoria que tiene por objetivo evaluar la eficacia, eficiencia de los controles establecidos así como también verificar el cumplimiento de las politicas y procedimientos definidos en la empresa.

a. Evaluaciones continuas y separadas.

La evaluación del control interno tiene como objetivo primordial evaluar el sistema de control interno, su aplicabilidad y su funcionalidad. Se debe reconocer que los procedimientos de supervisión continua se incorporan a las actividades normales

y recurrentes de las entidades. Dado que se realizan en tiempo real, reaccionando dinámicamente ante las condiciones cambiantes, y que están arraigados en la entidad, son más eficaces que los procedimientos llevados a cabo para las evaluaciones separadas. Debido a que las evaluaciones separadas tienen lugar después de los hechos, frecuentemente las rutinas de supervisión continua identificaran con mayor rapidez los problemas. Se deben hacer evaluaciones periódicas a todo el personal que trabaja directamente e indirectamente con datos personales evaluando si están aplicando las políticas y los procedimientos establecidos por la empresa, así como si cumplen lo establecido en la ley de protección de datos 172-13.

Si bien los procedimientos de supervisión continua generalmente brindan una respuesta importante acerca de la eficacia de otros componentes del control, las evaluaciones separadas proporcionan una perspectiva nueva en ocasiones, al concentrarse directamente en la eficacia del sistema de control interno. Esto también proporciona la oportunidad de considerar la eficacia constante del procedimiento de supervisión continua. El auditor interno o la persona encargada debe realizar una verificación de los procesos para determinar en qué grado la Dirección de la empresa está cumpliendo su función de supervisión. Además, identificar cuáles son los sistemas de información claves y de dónde provienen las fuentes de los datos, estableciendo prioridades de acuerdo a las informaciones obtenidas.

Las evaluaciones continuas y separadas le permiten a la dirección determinar si existe y funciona el control interno sobre los informes emitidos luego de las evaluaciones. Durante la supervisión continua y las evaluaciones separadas, es posible que se identifiquen deficiencias en el sistema de controles interno de la organización. COSO define en término generales una deficiencia como “un elemento del sistema de control interno que merece atención”. COSO indica que “una deficiencia, por tanto, puede representar un defecto percibido, potencial o real, o la oportunidad para reforzar el sistema de control interno para favorecer el logro de los objetivos de la entidad”. La deficiencia (también designadas observaciones de auditoria) que se identifican como resultado de la supervisión continua y de las evaluaciones separadas deben informarse de forma oportuna a las partes

correspondiente de la organización para que esta tome las medidas necesarias para corregirla. Se debe supervisar el desarrollo e implantación de políticas, procedimientos de administración y mantener el manual de políticas y los procedimientos actualizado sobre el proceso de protección de datos personales.

b. Deficiencia de los informes.

Todas las deficiencias que puedan afectar la consecución de los objetivos de la entidad deben ponerse en conocimiento de las personas que pueden tomar las medidas necesarias para determinar qué deficiencias se deben comunicar, así como también examinar el impacto de las mismas. Las deficiencias del control interno se identifican y comunican de forma oportuna a las partes responsables de tomar la medida correctiva, a la dirección y al consejo según corresponda.

Los asuntos de los que trata el informe escrito deben tener suficiente importancia para justificar su inclusión y la atención de la persona al que va dirigido. Deben evitarse los temas de una importancia relativa menor, para ello se deben considerar los conceptos de deficiencias significativas y otras deficiencias a comunicar. El informe debe dar cuenta de todos los aspectos comprendidos y resultantes de la labor de la evaluación, brindando la información necesaria sin alteración y para una adecuada interpretación de los temas tratados, evitando que contenga información falsa.

3.6 Plan de auditoría interna

Luego de adecuar la empresa a la LOPD 172-13 habiendo utilizando la guía de implementación es necesario posteriormente realizar auditorías que permitan verificar el cumplimiento con la ley. El objetivo principal del plan de auditoria es evaluar la eficacia y eficiencia de los controles establecidos, e identificar las oportunidades de mejoras que pueden existir. El alcance del plan de auditoria debe ser sobre la totalidad de los procesos existentes para el manejo de los datos de carácter personal. Este plan puede ser desarrollado dentro de la empresa por áreas o por procesos. Con este plan se pretende ayudar a las empresas no financieras a realizar las revisiones del

cumplimiento de sus políticas y procedimientos establecidos. A continuación, en la Tabla No. 12, se presenta un plan de auditoría interna para estos fines.

Tabla No. 12 - Plan de auditoria interna para la guía de implementación del cumplimiento de la ley 172-13 para empresa no financieras.

Procedimientos de auditoria	Realizado Por	Observaciones	Fecha
Principio de Entorno de Control			
Verificar que todo el personal esta comprometido con los objetivos, principios y valores éticos de la institución sobre la protección de datos personales de los clientes.			
Verificar que todo el personal utiliza los datos de carácter personal solo para los fines solicitados, no para fines contrarios.			
Verificar la evaluación de los riesgos por parte de la dirección.			
Verificar si el personal respeta el principio de calidad de los datos.			
Verificar que la dirección proporciona las herramientas necesarias para cumplir con el objetivo de la protección de datos personales.			
Verificar que se establecen los mecanismos necesarios para comunicar y mantener informado a todo el personal sobre las políticas y normas establecidas.			
Verificar que la dirección y demás personal cumplen y hacen cumplir las políticas establecidas sobre el registro, manejo, y divulgación de los datos personales de los clientes.			
Verificar que se establecen las líneas de denuncias necesarias que permitan el flujo de comunicación sobre la violaciones y desviaciones de las políticas de protección de datos.			
Verificar que se establecen y comunican en todos los niveles de la organización, los estándares de conducta que debe seguir todo el personal que manejen información de carácter personal, sean estos internos o externos.			
Verificar que se comunican las violaciones y/o desviaciones del cumplimiento de las políticas y normas establecidas.			
Verificar que se supervisa las labores realizadas por la dirección.			
Verificar que la dirección crea los procedimientos que se deben seguir para el manejo adecuado y el control interno de las informaciones de carácter personal.			
Verificar que la dirección crea los controles pertinentes que logren mitigar los riesgos inherentes al proceso de registro, modificación, robo, manipulación y divulgación de los datos personales.			

Tabla No. 12 - Plan de auditoria interna para la guía de implementación del cumplimiento de la ley 172-13 para empresa no financieras. (Continuación)

Procedimientos de auditoria	Realizado Por	Observaciones	Fecha
Verificar que RRHH crea e implementa las políticas y medidas que ayuden a salvaguardar las informaciones personales del personal que labora.			
Principio de Evaluación de Riegos			
Verificar se haya realizado el taller de evaluación de riegos con la frecuencia definida por el Consejo de Dirección así como también que se generó el informe con los resultados.			
Principio de Actividades de Control			
Verificar que todos los empleados firmaron una copia de las políticas y procedimientos comunicados, como constancia de que los recibieron.			
Verificar que se revisan y actualizan las políticas y procedimientos establecidos para cumplir con la ley 172-13 y sus modificaciones.			
Verificar que RRHH crea los acuerdos de confidencialidad que debe firmar cada empleado sobre las informaciones de la empresa.			
Verificar que cada empleado en todos los niveles y sin importar su jerarquía, firmo los acuerdos de confidencialidad al momento de ser contratado.			
Verificar que los empleados que violaron el acuerdo de confidencialidad fueron sancionados o despedido.			
Verificar que todo el personal llenó el cuestionario periódico sobre la ley 172-13 y sus modificaciones.			
Verificar que Las claves de acceso al sistema informático no fueron compartidas y que se cambiaron cada cierto tiempo.			
Verificar que solo se recogieron informaciones personales en los formularios o sistemas establecidos. Todo medio fuera del establecido se considera ilícito.			
Verificar que no se consultó ninguna información personal sin antes tener firmada la carta de autorización para tales fines.			
Verificar que no se utilizaron informaciones de carácter personal para otro fin que no sea para el cual fueron tomados.			
Verificar que todos los documentos firmados por el titular están firmados como firma en su documento de identidad.			
Verificar que el supervisor y otra persona evalúan las áreas y las herramientas que cuenten con informaciones de carácter personal.			

Tabla No. 12 - Plan de auditoria interna para la guía de implementación del cumplimiento de la ley 172-13 para empresa no financieras. (Continuación)

Procedimientos de auditoria	Realizado Por	Observaciones	Fecha
Verificar que se le solicita al titular todas las informaciones necesarias y luego se le informa sobre todas las informaciones registradas.			
Verificar se Imprime un resumen para el titular de las informaciones registradas y se le informa cual será el uso que se le dará.			
Verificar que se Imprimen y entregan al titular para que firme el documento de autorización para compartir sus datos.			
Verificar que ponen al titular a firmar la autorización que otorga a consultar sus datos personales.			
Verificar que se imprime y entrega al titular para que firme el documento de autorización para compartir sus datos.			
Verificar que se comunica el uso indebido de las informaciones personales.			
Verificar que se guardan el original y copia de la autorización firmada por el titular por un periodo mínimo de 6 meses.			
Verificar que se comunican con el titular de los datos para proceder con su corrección, de no ser posible, se suprimen los datos del sistema o trituran sin son físicos.			
Verificar que se imprime un resumen para el titular de las informaciones registradas, y entregan al titular para su revisión y autorización.			
Verificar que mantienen restringida las áreas que contienen informaciones personales. Que se bloquean las computadoras y herramientas de registros al no estar.			
Verificar que no se deja fuera ningún documento que contenga informaciones personales.			
Verificar que se cambian las contraseñas periódicamente o cuando esta fuere de conocimiento para otros.			
Verificar que se dan a conocer al titular de los datos todas las informaciones sobres sus datos que se poseen.			
Verificar que las solicitudes de corrección o eliminación son respondidas en un plazo máximo de 10 días.			
Verificar que los datos incompletos o parcialmente inexactos son triturados.			
Verificar que se agota el proceso correspondiente para corregir o eliminar los datos personales.			
Verificar que no se realizan cargos por los servicios de actualización, rectificación o suspensión de los datos personales.			
Verificar la funcionabilidad de la herramienta de recuperación de datos.			
Verificar que se realizan los backup diariamente.			

Tabla No. 12 - Plan de auditoria interna para la guía de implementación del cumplimiento de la ley 172-13 para empresa no financieras. (Continuación)

Procedimientos de auditoria	Realizado Por	Observaciones	Fecha
Verificar que las páginas de consultas no autorizadas están bloqueadas.			
Verificar que se valida la veracidad de las informaciones suministradas por terceros.			
Verificar que los parámetros establecidos en la base datos para que genere alarmas cuando sea detectado acceso o intento de acceso al sistema por terceros o fuera de hora este activo.			
Verificar que se realizan copia de seguridad diariamente			
Verificar que la licencia del antivirus está vigente y que el mismo es efectivo.			
Verificar si la dirección da el adecuado tratamiento a la información privada. Verificar si identifican y controlan el proceso mediante el cual la información es recolectada, hasta que se bloque, se borra o se destruye.			
Verificar que se comunican las deficiencias de control a las personas encargadas para que tomen medidas correctivas.			
Verificar que se hacen evaluaciones al cumplimiento de compromisos contractuales sobre el manejo de datos confidenciales.			
Verificar que se evalúa que se cumpla la autorización requerida para distribuir información dentro o fuera de la organización.			
Verificar que se realiza la evaluación de los procesos para determinar en qué grado la Dirección de la empresa está cumpliendo su función de supervisión.			
Verificar que se evalúa que se clasifican los documentos como confidencial, y colocan una nota en cada uno de los documentos cuya distribución secundaria no esté autorizada sin permiso.			
Verificar que se evalúa el impacto y la ocurrencia de las deficiencias y toman las medidas necesarias para evitar que ocurran.			
Principio de Información y Comunicación			
Verificar que se comunica en todos los niveles de la empresa las políticas y procedimientos relacionados con los datos de carácter personal.			
Verificar que por departamentos o vía intranet, se deja una copia de las políticas y procedimientos establecidos para consulta del personal.			
Verificar que antes de negarle al titular cualquier solicitud, se confirmó que existe una razón jurídica para hacerlo.			
Verificar que se comunica a la dirección los resultados de las evaluaciones y supervisión hecha al personal que manejan datos de carácter personal.			

Tabla No. 12 - Plan de auditoria interna para la guía de implementación del cumplimiento de la ley 172-13 para empresa no financieras. (Continuación)

Procedimientos de auditoria	Realizado Por	Observaciones	Fecha
Verificar que se comunica de manera formal cuál será la metodología que se debe seguir para tratar los datos personales.			
Verificar que se comunica si se cumple o no las políticas, procedimientos, leyes, reglamentaciones y otras cuestiones legales en el proceso de protección de datos personales.			
Principio de Supervisión			
Verificar el enfoque, alcance y objetivo de las actividades de autoevaluación.			
Verificar que se supervisan las políticas y procedimientos de administración y mantienen el manual de políticas y procedimientos actualizado sobre el proceso de protección de datos personales.			
Verificar si se supervisa que se conozcan y se cumplan los principios establecidos en la ley 172-13, sobre la obtención y divulgación de los datos personales de los clientes y empleados.			
Verificar si se han implementado controles sobre el manejo y protección de los datos personales que fueron recomendados.			
Verificar si se supervisa el cumplimiento de las leyes, reglamentaciones y normas gubernamentales o del sector económico aplicables a la protección de datos personales.			
Verificar si supervisa la capacitación y desarrollo del personal (por ejemplo, selección o desarrollo de cursos de formación, y administración de los procesos relacionados al manejo de Datos personales).			
Verificar si se supervisa que haya acceso restringido a la información de carácter personal.			
Verificar que se hacen evaluaciones al proceso de administración de los datos personales al menos una vez al año.			

Fuente: Elaboración propia

En la actualidad, todas las organizaciones necesitan llevar a cabo prácticas de control, esta guía está especialmente orientada a aquellas instituciones no financieras, las cuales requieren y están en condiciones de aplicar mecanismos formales y preestablecidos de control para evitar o reducir los fraudes, riesgos y conductas inadecuadas que puedan surgir, tanto por parte del personal, como de clientes y

proveedores, para el manejo de los datos de carácter personal.

Al implementar los pasos sugeridos en la presente guía basada en la ley 172-13 y que tiene como parámetro el enfoque COSO, las organizaciones podrán controlar más eficiente, eficaz y transparentemente sus operaciones.

CONCLUSIÓN

En la actualidad, la Información es uno de los recursos más preciados en cualquier organización. El contar con información íntegra, accesible, consistente, confiable y oportuna, es fundamental para que dicha organización pueda subsistir, desarrollarse y tomar decisiones correctas en el dinámico mundo actual, no obstante las personas también corren el riesgo de que sus datos personales no le den el tratamiento adecuado violando así uno de sus derechos de privacidad, sea esto por desconocimiento o por una mala intensión.

En las comparaciones de los diferentes países de Iberoamérica se concluye que cada país tiene por objeto garantizar, proteger y que se le dé un adecuado tratamiento a los datos de carácter personal. Más de un ochenta por ciento (80%) de los países cuentan con una ley de protección de datos personales y un órgano de control que la regula, estas leyes cuentan con diferentes sanciones que dependerá de la magnitud del incumplimiento, estas se caracterizan en leves, graves y muy graves, otra se multan con salarios, apercibimiento y otros delitos pueden ser sancionados con prisión dependiendo lo establecido en la ley de cada país.

En el análisis de esta investigación se determinó que es limitado el conocimiento que tienen la mayoría de los encuestados del sector no financiero sobre la ley LOPD 172-13 y se desconoce el alcance de la misma, así como también las consecuencias de no cumplirla. Por todo esto surge la necesidad de que las organizaciones no financieras lleven a cabo prácticas de control, la guía que se propone está especialmente orientada a aquellas instituciones no financiera, las cuales requieren y están en condiciones de aplicar mecanismos formales y preestablecidos de control para evitar o reducir los fraudes, riesgos y conductas inadecuadas que puedan surgir, tanto por parte del personal, como de clientes y proveedores, para el manejo de los datos de carácter personal.

Al implementar los pasos sugeridos en la guía propuesta basada en la ley 172-13

la cual tiene como parámetro el enfoque COSO las organizaciones conseguirán controlar más eficiente, eficaz y transparentemente sus operaciones. Una de las grandes ventajas de COSO reside en que al parametrizar y formalizar las técnicas de medición, el control resulta simple y efectivo. Otra ventaja importante es su dinamismo para ser revisado y actualizado según los cambios que va experimentando la organización ya que la interrelación de los cinco componentes: Ambiente de control, Evaluación de riesgos, actividades de control, Información y comunicación y supervisión genera una sinergia conformando un sistema integrado que responde dinámicamente a los cambios del entorno. Sus cinco componentes son nuevos elementos que se aportan al sistema, se integran entre sí y se implementan de forma interrelacionada, influenciados por el estilo de dirección.

El plan de auditoria propuesto se encargará de supervisar y verificar que se cumpla adecuadamente los pasos establecidos en la guía, permitirá evaluar la eficacia y eficiencia de los controles establecidos e identificar las oportunidades de mejoras que puedan existir para las empresas no financieras.

Por todo lo anterior, se constata que se cumple con el objetivo general de este trabajo de investigación de desarrollar un plan de auditoría interna que le permita a los directivos de una empresa no financiera validar el cumplimiento de la Ley Orgánica de Protección de Datos de Carácter Personal 172-13 de la República Dominicana luego de que ésta ha adecuado sus procesos al cumplimiento de la referida ley.

REFERENCIAS

1. Agencia Española de Protección de Datos (2014) *Protección de Datos y Habeas Data: Una visión desde Iberoamérica.* Recuperado de https://www.agpd.es/portalwebAGPD/canaldocumentacion/publicaciones/common/premios_2015/Proteccion_de_datos_y_habeas_data.pdf

2. Asamblea Constituyente de Bolivia. (7 de febrero de 2009). *Constitución Política del Estado (CPE).* Recuperado de https://www.oas.org/dil/esp/Constitucion_Bolivia.pdf

3. Asamblea Constituyente de la República Portuguesa. (2 de abril de 1976). *Constitución de Portugal de 2 de abril de 1976.* Recuperado de http://www.redipd.org/legislacion/common/legislacion/portugal/Constitucion_Portugal.pdf

4. Asamblea General de la República Oriental del Uruguay. (15 de febrero de 1967). *Constitución de la República Oriental del Uruguay.* Recuperado de http://pdba.georgetown.edu/Parties/Uruguay/Leyes/constitucion.pdf

5. Asamblea General de la República Oriental del Uruguay. (20 septiembre de 2003). *Decreto No. 396/003 - Trata acerca de los datos personales relativos a la salud.* Recuperado de http://www.redipd.es/legislacion/common/legislacion/uruguay/decreto-396-003.pdf

6. Asamblea General de la República Oriental del Uruguay. (30 de octubre de 2006). *Decreto No. 399/006 - Se crea el Registro de Bases de datos, archivos, registros y otros medios similares autorizados, destinados a brindar informes de carácter comercial.* Recuperado de http://www.redipd.es/legislacion/common/legislacion/uruguay/decreto-399-006.pdf

7. Asamblea General de la República Oriental del Uruguay. (27 de diciembre de 2007). *Ley No. 18.244 - Se establecen normas para el tratamiento de datos de los deudores alimentarios morosos.* Recuperado de http://www.redipd.es/legislacion/common/legislacion/uruguay/ley-18244.pdf

8. Asamblea General de la República Oriental del Uruguay. (31 de agosto de 2009). *Ley No. 18.381 de Protección de Datos Personales y Acción de "Habeas Data".* Recuperado de http://www.redipd.es/legislacion/common/legislacion/uruguay/decreto-414-009.pdf

9. Asamblea Legislativa de la República de Costa Rica. (5 de septiembre de 2011). *Ley No.8968 - Protección de la persona frente al tratamiento de sus datos personales.* Recuperado de http://www.redipd.es/legislacion/common/legislacion/costa_rica/Ley_8968_Costa_Rica.pdf

10. Asamblea Legislativa de la República de El Salvador. (26 de abril de 1997). *Decreto Legislativo No. 1030 - Código Penal.* Recuperado de http://www.redipd.es/legislacion/common/legislacion/elsalvador/CODIGO_PENAL.pdf

11. Asamblea Legislativa de la República de El Salvador. (8 de septiembre de 2005). *Decreto Legislativo No. 166 - Ley de Protección al Consumidor.* Recuperado de http://www.redipd.es/legislacion/common/legislacion/elsalvador/Ley_proteccion_al_consumidor_ElSalvador.pdf

12. Asamblea Legislativa de la República de Panamá. (22 de enero de 2002). *Ley No. 6 - Normas para la transparencia en la gestión pública, la acción de Habeas Data y otras disposiciones.* Recuperado de http://www.redipd.es/legislacion/common/legislacion/panama/ley_num_6.pdf

13. Asamblea Legislativa de la República de Panamá. (22 de mayo de 2002). *Ley No. 24 - Que regula el servicio de información sobre el historial de crédito de los consumidores o clientes.* Recuperado de http://www.redipd.es/legislacion/common/legislacion/panama/ley_num_24.pdf

14. Asamblea Legislativa Plurinacional de Bolivia. (16 de junio de 2010). *Ley No. 018 - Ley del Órgano Electoral Plurinacional.* Recuperado de http://www.redipd.es/legislacion/common/legislacion/Bolivia/Ley_N_018_Organo_Electoral_Plurinacional.pdf

15. Asamblea Legislativa Plurinacional de Bolivia. (08 de agosto de 2011). *Ley No. 164 - Ley General de Telecomunicaciones, Tecnológicas de Información y Comunicación.* Recuperado de http://www.redipd.es/legislacion/common/legislacion/Bolivia/Ley_N_164_Telecomunicaciones.pdf

16. Asamblea Legislativa Plurinacional de Bolivia. (13 de noviembre de 2013). *Decreto Supremo No.1793 - Reglamento de la Ley Nº 164 sobre Telecomunicaciones, Tecnología de Información y Comunicación.* Recuperado de http://www.redipd.es/legislacion/common/legislacion/Bolivia/DS_1793_Telecomunicaciones.pdf

17. Asamblea Nacional de la República Bolivariana de Venezuela. (30 de octubre de 2001). *Ley Especial Contra los Delitos Informáticos.* Recuperado de http://www.redipd.es/legislacion/common/legislacion/venezuela/13-leydelitosinformaticos.pdf

18. Asamblea Nacional de la República de El Salvador. (30 de marzo de 2011). *Decreto No. 534 - Ley de acceso a la información pública.* Recuperado de http://www.redipd.es/legislacion/common/legislacion/elsalvador/Decreto_N534.pdf

19. Asamblea Nacional de la República de Honduras. (30 de diciembre de 2006). *Decreto No. 170-2006 - Ley de Transparencia y Acceso a la Información Pública.* Recuperado de https://www.ccit.hn/wp-content/uploads/2013/12/LEY-DE-TRANSPARENCIA-Y-ACCESO-A-LA-INFORMACION1.pdf

20. Asamblea Nacional de la República de Nicaragua. (29 de marzo de 2012). *Ley No. 787 - Ley de Protección de Datos Personales.* Recuperado de http://www.redipd.es/legislacion/common/legislacion/nicaragua/Ley__787.pdf

21. Asamblea Nacional de la República de Nicaragua. (2014). *Constitución Política de la República de Nicaragua.* Recuperado de http://www.oas.org/juridico/spanish/mesicic3_nic_const.pdf

22. Asamblea Nacional de la República de Panamá. (11 de octubre de 1972). *Constitución Política de la República de Panamá.* Recuperado de http://www.legalinfo-panama.com/legislacion/Constitucion/Constitucion.pdf

23. Asamblea Nacional de la República Oriental de Uruguay. (11 de agosto de 2008). *Ley No.18.331 - Ley de Protección de Datos Personales y Acción Habeas Data.* Recuperado de http://www.redipd.es/legislacion/common/legislacion/uruguay/ley_18331.pdf

24. Asamblea Nacional Constituyente de la República de Ecuador. (20 de octubre de 2008). *Constitución de la República de Ecuador de 2008.* Recuperado de http://pdba.georgetown.edu/Parties/Ecuador/Leyes/constitucion.pdf

25. Asamblea Nacional Constituyente de la República de Ecuador. (31 de marzo de 2010). *Ley No. 162 - Ley del Sistema Nacional de Registro de Datos Públicos.* Recuperado de http://www.redipd.es/legislacion/common/legislacion/ecuador/Ley_N_162.pdf

26. Asamblea Nacional Constituyente de la República de Colombia. (4 de julio de 1991). *Constitución Política de Colombia.* Recuperado de http://www.corteconstitucional.gov.co/inicio/Constitucion%20politica%20de%20Colombia%20-%202015.pdf

27. Asamblea Nacional Constituyente de la República de Costa Rica. (7 de noviembre de 1949). *Constitución Política de Costa Rica.* Recuperado de http://pdba.georgetown.edu/Parties/CostaRica/Leyes/constitucion.pdf

28. Asamblea Nacional Legislativa de la República de Honduras. (20 de enero de 1982). *Constitución Política de la República de Honduras de 1982.* Recuperado de https://www.oas.org/dil/esp/Constitucion_de_Honduras.pdf

29. Boletín Oficial del Estado (BOE). (12 de julio de 2002). *Ley 34/2002 de servicios de la sociedad de la información y de comercio electrónico.* Recuperado de https://boe.es/buscar/act.php?id=BOE-A-2002-

13758&p=20140510&tn=2

30. Boletín Oficial del Estado (BOE). (14 de noviembre de 2002). *Ley 41/2002 básica reguladora de la autonomía del paciente y de derechos y obligaciones en materia de información y documentación clínica.* Recuperado de https://boe.es/buscar/act.php?id=BOE-A-2002-22188&p=20150922&tn=2

31. Boletín Oficial del Estado (BOE). (21 de mayo de 2003). *Ley 12/2003 de prevención y bloqueo de financiación del terrorismo.* Recuperado de http://www.boe.es/buscar/act.php?id=BOE-A-2003-10289

32. Boletín Oficial del Estado (BOE). (3 de noviembre de 2003). *Ley 32/2003 General de Telecomunicaciones.* Recuperado de https://www.boe.es/buscar/act.php?id=BOE-A-2003-20253

33. Boletín Oficial del Estado (BOE). (19 de diciembre de 2003). *Ley 58/2003 General Tributaria.* Recuperado de http://boe.es/buscar/act.php?id=BOE-A-2003-23186&tn=2

34. Boletín Oficial del Estado (BOE). (5 de marzo de 2011). *Ley Orgánica 15/1999 de España, de 13 de diciembre, de Protección de Datos de Carácter Persona.* Recuperado de https://www.agpd.es/portalwebAGPD/canaldocumentacion/legislacion/estatal/common/pdfs/2014/Ley_Organica_15-1999_de_13_de_diciembre_de_Proteccion_de_Datos_Consolidado.pdf

35. Boletín Oficial del Estado (BOE). (8 de marzo de 2012). *Real Decreto 1720/2007, por el que se que se aprueba el Reglamento de desarrollo de la Ley Orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal.* Recuperado de https://www.boe.es/buscar/pdf/2008/BOE-A-2008-979-consolidado.pdf

36. Boletín Oficial del Estado (BOE). (9 de diciembre de 2013). *Ley 19/2013 de transparencia, acceso a la información pública y buen gobierno.* Recuperado de https://www.boe.es/buscar/act.php?id=BOE-A-2013-12887&p=20131221&tn=2

37. Comisión Ortúzar, Consejo de Estado y Junta Militar de Gobierno. (21 de octubre de 1980). *Constitución Política de la República de Chile.* Recuperado de http://www.camara.cl/camara/media/docs/constitucion_politica.pdf

38. Congreso Constituyente de Brasil. (5 de octubre de 1988). *Constitución Política de 1988.* Recuperado de http://pdba.georgetown.edu/Constitutions/Brazil/esp88.html

39. Congreso Constituyente de los Estados Unidos Mexicanos. (5 de febrero de 1917). *Constitución Política de los Estados Unidos Mexicanos.* Recuperado de http://www.diputados.gob.mx/LeyesBiblio/pdf/1_240217.pdf

40. Congreso Constituyente Democrático de la República del Perú. (29 de diciembre de 1993). *Constitución Política del Perú.* Recuperado de http://portal.jne.gob.pe/informacionlegal/Constitucin%20y%20Leyes1/CONSTITUCION%20POLITICA%20DEL%20PERU.pdf

41. Congreso de Colombia. (17 de octubre de 2012). *La Ley Estatutaria No. 1581 - Por cual se dictan disposiciones generales para la protección de datos personales.* Recuperado de http://www.redipd.es/legislacion/common/legislacion/Colombia/Ley_1581_2012_COLOMBIA.pdf

42. Congreso de la Nación de Paraguay. (20 de junio de 1992). *República de Paraguay - Constitución de 1992.* Recuperada de http://pdba.georgetown.edu/Constitutions/Paraguay/para1992.html

43. Congreso de la Nación de Paraguay. (16 de septiembre de 2001). *Ley No. 1628 - Que reglamenta la Información de Carácter Privado.* Recuperado de http://www.redipd.es/legislacion/common/legislacion/paraguay/Ley_1682_de_2001.pdf

44. Congreso de la Nación de Paraguay. (9 de agosto de 2013). *Ley No. 4989 - Que crea el marco de aplicación de las tecnologías de la información y comunicación en el sector público y crea la Secretaría Nacional de Tecnologías de la Información y Comunicación.* Recuperado de http://www.redipd.es/legislacion/common/legislacion/paraguay/Ley_4989

.pdf

45. Congreso de la República de Perú. (3 de agosto de 2002). *Ley No. 27806 - Ley de Transparencia y Acceso a la Información Pública.* Recuperado de http://www.redipd.es/legislacion/common/legislacion/peru/ley_27806.pdf

46. Congreso de la República de Venezuela. (3 de agosto de 1979). *Ley de Registro de Antecedentes Penales.* Recuperado de http://www.defiendete.org/html/de-interes/LEYES%20DE%20VENEZUELA/LEYES%20DE%20VENEZUELA%20II/LEY%20DE%20REGISTRO%20DE%20ANTECEDENTES%20PENALES.htm

47. Congreso de la República de Venezuela. (16 de diciembre de 1991). *Ley sobre Protección a la Privacidad de la Comunicaciones.* Recuperado de http://lac.derechos.apc.org/clegislacion.shtml?x=9724

48. Congreso de los Estados Unidos Mexicanos. (11 de junio de 2002). *Ley Federal de Transparencia y Acceso a la Información Pública Gubernamental.* Recuperado de http://www.redipd.es/legislacion/common/legislacion/mexico/normas_generales/Ley_Federal_Transparencia_Acceso_Informacion_Publica_Gubernamental1.pdf

49. Congreso de los Estados Unidos Mexicanos. (5 de julio de 2010). *Ley Federal de Protección de Datos Personales en Posesión de los Particulares.* Recuperado de http://www.redipd.es/legislacion/common/legislacion/mexico/normas_generales/LFPDPPP3.pdf

50. Congreso Directivo del poder Judicial de Perú. (16 de marzo de 2016). *Resolución Administrativa No. 065-2016-CE-PJ.* Recuperado de http://www.redipd.es/legislacion/common/legislacion/peru/Directiva_PJudicial_Peru_TratamientoDatosPersonales.pdf

51. Congreso General de Andorra. (2 de febrero de 1993) *La Constitución del Principado de Andorra.* Recuperado de https://www.unodc.org/tldb/pdf/Constitucon_de_Andorra_1993_Es_texto_ntegro.pdf

52. Congreso General de Andorra. (18 de diciembre de 2003). *Llei 15/2003 - qualificada de protecció de dades personals [Ley 15/2003 - calificada de protección de datos personales].* Recuperado de http://www.redipd.es/legislacion/common/legislacion/Andorra/Llei_qualificada_de_proteccio_de_dades_personals.pdf

53. Congreso General Constituyente Argentino. (22 de agosto de 1994). *Constitución de la Nación Argentina.* Recuperado de http://www.constitution.org/cons/argentin.htm

54. Congreso General Constituyente Argentino. (02 de noviembre de 2000). *Ley 25.326 - Ley Protección de Datos Personales.* Recuperado de http://www.redipd.es/legislacion/common/legislacion/Argentina/ley_25326.pdf

55. Congreso General Constituyente Argentino. (24 de noviembre de 2005). *Ley CABA No. 1845/2006 - Ley de Protección de Datos Personales.* Recuperado de http://www.redipd.es/legislacion/common/legislacion/Argentina/ley_1845_proteccion_datos_personales.pdf

56. Congreso Nacional de Brasil. (11 de septiembre 1990). *Lei No. 8078 - Dispõe sobre a proteção do consumidor e dá outras providências [Ley No. 8078 Dispone sobre la protección del consumidor y da otras providencias].* Recuperado de http://www.redipd.es/legislacion/common/legislacion/Brasil/ley_8078_1990_pt.pdf

57. Congreso Nacional de Brasil. (24 de junio de 1996). *Lei No. 9.296 - Interceptação do fluxo de comunicações em sistemas de informática e telemática. [Ley No. 9.296 - Interceptación del flujo de comunicaciones en sistemas informáticos y telemáticos].* Recuperado de http://www.redipd.es/legislacion/common/legislacion/Brasil/lei_9296_pt.pdf

58. Congreso Nacional de Brasil. (12 de noviembre de 1997). *Lei No. 9.507 - Regula o direito de acesso a informações e disciplina o rito processual do habeas*

data [Ley No. 9.507 - Regula el derecho de acceso a informaciones y disciplina el rito procesal del habeas data]. Recuperado de http://www.redipd.es/legislacion/common/legislacion/Brasil/Lei_9507_1997_pt.pdf

59. Congreso Nacional de Brasil. (10 de enero de 2001). *Lei No. 105 - Dispõe sobre o sigilo das operações de instituições financeiras e dá outras providências [Ley No. 105 - Dispone sobre el secreto de las operaciones de instituciones financieras y da otras providencias]*. Recuperada de http://www.redipd.es/legislacion/common/legislacion/Brasil/lei_complementaria_105_pt.pdf

60. Congreso Nacional de Chile. (28 de agosto de 1999). *Ley 19628 sobre la Protección de la Vida Privada.* Recuperado de http://www.oas.org/juridico/spanish/cyb_chi_ley_19628.pdf

61. Congreso Nacional de Chile. (25 de octubre de 2010). *Ley No. 20.463 - Modifica Ley No. 19.628, suspendido por el plazo que indica la información de las personas cesantes.* Recuperado de http://www.redipd.es/legislacion/common/legislacion/Chile/legislacion/Ley_20463.pdf

62. Congreso Nacional de Chile. (23 de julio de 2011). *Ley No. 20.521 - Modifica la Ley No. 19.628, sobre protección de datos de carácter personal para garantizar que la información entregada a través de predictores de riesgo sea exacta, actualizada y veraz.* Recuperado de http://www.redipd.es/legislacion/common/legislacion/Chile/legislacion/Ley_20521.pdf

63. Congreso Nacional de la República de Ecuador. (10 de agosto de 1992). *Ley No. 184 - Ley Especial de Telecomunicaciones y su Reforma.* Recuperado de http://www.redipd.es/legislacion/common/legislacion/ecuador/Ley_184_10081992_Teleco_reforma_Ecuador.pdf

64. Congreso Nacional de la República de Ecuador. (17 de abril de 2002). *Ley de Comercio Electrónico, Firmas Electrónicas y Mensaje de Datos. (Ley No. 2002-67). R*ecuperado de http://www.redipd.es/legislacion/common/legislacion/ecuador/ecuador_ley_2002-67_17042002_comelectronico.pdf

65. Congreso Nacional de la República de Ecuador. (18 de mayo de 2004). *Ley de Orgánica de Transparencia y Acceso a la Información Pública.* Recuperado de http://www.redipd.es/legislacion/common/legislacion/ecuador/ley_organica_de_acceso_a_la_informacion_en_ecuador.pdf

66. Congreso Nacional de la República de Ecuador. (18 de octubre de 2005). *Ley de Burós de Información Crediticia No. 13.* Recuperado de http://www.redipd.es/legislacion/common/legislacion/ecuador/ley_buros_informacion_crediticia_Ecuador.pdf

67. Congreso Nacional de la República de Guatemala. (23 de septiembre de 2008). *Ley para el Reconocimiento de las Comunicaciones y Firmas Electrónicas. - Decreto Número 47-2008.* Recuperado de http://www.redipd.es/legislacion/common/legislacion/guatemala/Acuerdo_47-2008_Firmas_Electronicas_Guatemala.pdf

68. Congreso Nacional de la República de Guatemala. (11 de marzo de 2003). *Decreto No. 006-2003 - Ley de Protección al Consumidor y Usuario.* Recuperado de http://www.redipd.es/legislacion/common/legislacion/guatemala/decreto_006_2003_Guate.pdf

69. Congreso Nacional de la República de Guatemala. (5 de julio de 1963). *Código Penal de Guatemala - Decreto No. 17-73.* Recuperado de http://www.redipd.es/legislacion/common/legislacion/guatemala/Codigo_Penal_Guatemala.pdf

70. Congreso Nacional de la República del Perú. (3 de julio de 2011). *Ley No. 29733 - Ley de Protección de Datos Personales.* Recuperado de http://www.redipd.es/legislacion/common/legislacion/peru/Ley-29733.pdf

71. Congreso Nacional de la República del Perú. (21 de marzo de 2013). *Aprueban Reglamento de la Ley No. 29733, Ley de Protección de Datos Personales. - Decreto Supremo No. 003-2013-JUS.* Recuperado de http://www.redipd.es/legislacion/common/legislacion/peru/Decreto_Supremo_003_2013_JUS.pdf

72. Congreso Nacional de la República Dominicana. (2013). *Ley 172-13 sobre la protección de Datos de Carácter personal.* Recuperado de http://www.phlaw.com/imagen?file=articulos/419/ley-no-172-13-sobre-proteccion-integral-datos-personales

73. Congreso Nacional de la República Dominicana. (26 de enero de 2010). *Constitución Política de la República Dominicana.* Recuperado de http://www.redipd.es/legislacion/common/legislacion/rep_dominicana/constitucion_dominicana_2010.pdf

74. Congreso Nacional de la República Dominicana. (23 de abril de 2007). *Ley No. 53-07 sobre Crímenes y Delitos de Alta Tecnologías.* Recuperado de https://www.dgii.gov.do/legislacion/leyesTributarias/Documents/53-07.pdf

75. Congreso Nacional de la República Dominicana. (14 de agosto de 2002). *Ley No.126-02 sobre Comercio Electrónico, Documentos y Firma Digital.* Recuperado de http://www.bancentral.gov.do/normativa/leyes/Ley_126-02_Comercio_Electronico.pdf

76. Congreso Nacional de la República Portuguesa. (26 de octubre de 1998). *Ley 67/98 de Protección de Datos Personales.* Recuperado de http://www.redipd.es/legislacion/portugal-ides-idphp.php

77. Diputados de la Asamblea Constituyente de la República Bolivariana de Venezuela. (20 de diciembre de 1999). *Constitución de la República Bolivariana de Venezuela.* Recuperado de https://www.oas.org/juridico/mla/sp/ven/sp_ven-int-const.html

78. Diputados de la Asamblea Constituyente de la República de El Salvador. (15 de diciembre de 1963). *Constitución.* Recuperado de http://pdba.georgetown.edu/Constitutions/ElSal/constitucion.pdf

79. Diputados de la Asamblea Nacional Constituyente de la República de Guatemala. (14 de energo de 1986). *Constitución Política de la República de Guatemala.* Recuperado de https://www.oas.org/juridico/mla/sp/gtm/sp_gtm-int-text-const.pdf

80. Kurt F. (2009). *Auditoria Interna: Servicio de Asesoría y Consultoría.* Estados Unidos, Cris Riddle, M.A.

81. Ministerio de Justicia. Dirección General de Asuntos Jurídicos. (s.f.). *Código Penal Bolivia, modificado por la Ley Nº 1768, de 10 de Marzo de 1997.* Recuperado de http://www.redipd.es/legislacion/common/legislacion/Bolivia/codigo_penal_bolivia.p

82. Moeller, R. R. (2013) *Executive's Guide to COSO Internal Controls [Guía Ejecutiva de los Controles Internos del COSO].* (s.l.). Wiley.

83. Padres de la Constitución. (6 de diciembre de 1978). *Constitución Española.* Recuperado de http://www.lamoncloa.gob.es/documents/constitucion_es1.pdf

84. Palacio Nacional y Ministros de Estado de Bolivia. (18 de mayo de 2005). *Decreto Supremo No. 28168.* Recuperado de http://www.redipd.es/legislacion/common/legislacion/Bolivia/D_S_28168_mayo_2005.pdf

85. Piazza, M.L. (2013) *COSO 2013 Quick Reference Guide [COSO 2013 Guía de Referencia Rápida].* (s.l.). Professional Development Associates.

86. Presidente de la República de Brasil. (7 de diciembre de 1940). *Código Penal [Código Penal]* Recuperado de http://www.redipd.es/legislacion/common/legislacion/Brasil/Brasil_codigo_penal.pdf

87. Presidente de la República del Salvador. (1 de septiembre de 2012). *Reglamento de la Ley de Acceso a la Información Pública - Decreto No. 136.* Recuperado de http://www.oas.org/juridico/PDFs/mesicic4_slv_regla.pdf

88. Red Iberoamericana de Protección de Datos (RIPD). (2009). *Legislación.* Recuperado de http://www.redipd.es/legislacion/index-ides-idphp.php

89. Rodrigo Estupiñan Gaitan. (2015). *Administración de riesgos E.R.M. y la*

Auditoria interna, segunda edición. Recuperado de https://www.ecoeediciones.com/wp-content/uploads/2015/07/Administracion-de-riesgos-ERM-y-la-auditor%C3%ADa-interna-2da-Edición.pdf

90. Tarantino, A. (2006). *Manager's Guide to Compliance [Guía del Administrador para el Cumplimiento].* Nueva Jersey: John Wiley & Sons, Inc.

ANEXOS

(A) Encuesta – Analizar el conocimiento de la ley 172-13 sobre la protección de datos personales en República Dominicana.

Analizar el conocimiento de la ley 172-13 sobre la protección de datos personales en República Dominicana

Datos de la Institución o Empresa:

- Razón Social: (Opcional)

- Actividad económica:

- Tiempo de operación:

- Tamaño de la institución:

Pequeña ◯ Mediana ◯ Grande ◯

Encuesta sobre el manejo de los datos personales y conocimiento de ley 172-13

1-¿Llevan archivos, registros de datos personales?

Sí ⬭ No ⬭

2-¿Existe un proceso definido sobre la forma de registrar y archivar los datos personales que se obtienen de los clientes?

Sí ⬭ No ⬭

3-¿Los datos recopilados de los clientes se registran y archivan en lugares seguros y confiables?

Sí ⬭ No ⬭

4-¿El lugar donde se almacenan los datos de los clientes es de acceso abierto o restringido?

Abierto ⬭ Restringido ⬭

5-¿Cuáles datos personales se les solicitan a los clientes:

- Dirección
- Cédula
- Teléfono
- Correo electrónico
- Tarjeta de crédito
- Otros

6-¿Las informaciones recopiladas de los clientes se comunican o comparten con instituciones externas o relacionadas?

Sí ⬭ No ⬭

7-¿Cuentan con alguna autorización de la persona para compartir sus datos personales con terceros?

Sí ⬭ No ⬭

Encuesta sobre el manejo de los datos personales y conocimiento de ley 172-13

8-¿se le solicita al cliente firmar alguna autorización para consultar en los buros de crédito sobre sus informaciones personales?

Sí ⬭ No ⬭

9-¿Se comunica a todo el personal como deben ser tratados los datos personales de los clientes?

Sí ⬭ No ⬭

10-¿Hay acuerdos de confidencialidad firmados entre sus empleados y el empleador?

Sí ⬭ No ⬭

11-¿Por qué periodo la institución mantiene archivada los datos personales de los clientes?

Años ⬭ Meses ⬭ Semanas ⬭

12-¿Con que periodicidad se actualizan los datos almacenados de los clientes?

13-¿La institución toma medidas para la protección de datos personales de los clientes?

Sí ⬭ No ⬭

14-¿Tienen algún procedimiento establecido para el manejo de los datos personales?

Sí ⬭ No ⬭

15-¿Existen controles en la institución que mitiguen el riesgo del mal uso y la difusión sin autorización de los datos personales?

Sí ⬭ No ⬭

Encuesta sobre el manejo de los datos personales y conocimiento de ley 172-13

16-¿Se evalúan los controles existentes sobre el manejo de los datos personales?

Sí ⬭ No ⬭

17-¿Se identifican los riesgos inherentes al proceso de almacenamiento de datos personales?

Sí ⬭ No ⬭

18-¿Se le ha solicitado a la institución la corrección o eliminación de datos personales de clientes archivados: en qué tiempo responden a la solicitud?

Sí ⬭ No ⬭

Tiempo de respuesta: ▭

19-¿La institución conoce la ley orgánica de protección de datos 172-13?

Sí ⬭ No ⬭

20-¿Qué nivel de conocimiento de la LOPD tiene: Amplio, Medio, Bajo?

Amplio ⬭ Medio ⬭ Bajo ⬭

21-¿Tienen algún manual que garantice la aplicación de la LOPD?

Sí ⬭ No ⬭

(B) Glosario de siglas y abreviaturas

GLOSARIO DE SIGLAS Y ABREVIATURAS

SIGLA	SIGNIFICADO
APDA	Agencia Andorrana de Protección de Datos
APDP	Autoridad Nacional de Protección de Datos Personales
ARCO	Acceso, Rectificación, Cancelación y Oposición
CNPD	Comisión Nacional de Protección de Datos
COBIT	Control Objectives for Information and Related Technologies
CoCo	Criteria of Control Committe
COSO	Committe of Sponsoring Organization of the Tradeway Commission
DNPDP	Dirección Nacional de Protección de Datos Personales
EIPD	Encuentro Iberoamericano de Protección de Datos
GECTI	Grupo de Estudios en Internet, Comercio Electrónico, Telecomunicaciones & Informática
IFAI	Instituto Federal de Acceso a la Información Pública y Protección de Datos (IFAI)
INPEC	Instituto Nacional Penitenciario y Carcelario
LFPDPPP	Ley Federal de Protección de Datos Personales en Posesión de los Particulares
LOPD	Ley Orgánica de Protección de Datos
LPDP	Ley de Protección de Datos Personales
LQPD	Llei Qualificada de Protecció de Dades Personals
PDP	Protección de Datos Personales
PRODHAB	Agencia de Protección de Datos de los Habitantes
RIPD	Red Iberamericana de Protección de Datos
SIC	Sociedad de Información Crediticia (en la República Dominicana)
SIC	Superintendencia de Industria y Comercio (en la República de Colombia)