UNIVERSIDAD NACIONAL DEL ALTIPLANO

FACULTAD DE CIENCIAS JURÍDICAS Y POLÍTICAS

ESCUELA PROFESIONAL DE DERECHO

"IT COMPLIANCE, PRIVACIDAD Y PROTECCIÓN DE DATOS PARA EMPRESAS PÚBLICAS EN EL PERÚ"

TESIS

PRESENTADA POR:

LUIS FERNANDO GARCÍA VILLALTA

PARA OPTAR EL TÍTULO PROFESIONAL DE:

ABOGADO

PUNO – PERÚ

2019

UNIVERSIDAD NACIONAL DEL ALTIPLANO

FACULTAD DE CIENCIAS JURÍDICAS Y POLÍTICAS

ESCUELA PROFESIONAL DE DERECHO

IT COMPLIANCE, PRIVACIDAD Y PROTECCIÓN DE DATOS PARA EMPRESAS PÚBLICAS EN EL PERÚ

TESIS PRESENTADA POR:

LUIS FERNANDO GARCÍA VILLALTA

PARA OPTAR EL TÍTULO PROFESIONAL DE:

ABOGADO

APROBADA POR EL JURADO REVISOR CONFORMADO POR:

PRESIDENTE : _____
Dr. Sc. JAVIER SÓCRATES PINEDA ANCCO

PRIMER MIEMBRO : _____
M. Sc. WILDER IGNACIO VELAZCO

SEGUNDO MIEMBRO : _____
Abog. GUILLERMO ALBERTO PIZARRO FLORES

DIRECTOR / ASESOR : _____
Abog. JULIO JESÚS CUENTAS CUENTAS

ÁREA : Ciencias Sociales
LÍNEA : Derecho
SUB LÍNEA : Derecho Administrativo
TEMA : Sistemas Administrativos

FECHA DE SUSTENTACIÓN: JUEVES 18 DE JULIO DE 2019

DEDICATORIA

En recuerdo de Julián Villalta Luna.

AGRADECIMIENTOS

A mis padres: Mario García Tejada y Yolanda Villalta Ticona, por su apoyo incondicional.

A mis hermanos: Rodrigo Milán y Marleny por acompañarme en este gran desafío.

A los jurados de la presente investigación: Dr. Javier Sócrates Pineda Ancco; M. Sc. Wilder Ignacio Velazco; Mg. Guillermo Alberto Pizarro Flores y al Director de Tesis Abog. Julio Jesús Cuentas Cuentas.

Mi gratitud a la Universidad Nacional del Altiplano, en especial a la Facultad de Ciencias Jurídicas y Políticas, Escuela Profesional de Derecho.

ÍNDICE GENERAL

ÍNDICE DE FIGURAS

ÍNDICE DE TABLAS

ÍNDICE DE ACRÓNIMOS

AEPD : Agencia Española de Protección de Datos

ANPDP : Autoridad Nacional de Protección de Datos Personales

DPD : Delegado de Protección de Datos

FONAFE : Fondo Nacional de Financiamiento de la Actividad Empresarial del Estado

LOPDCP : Ley Orgánica 15/1999 de Protección de Datos de Carácter Personal

LOPDPGDG : Ley Orgánica 3/2018, de Protección de Datos Personales y Garantía de los Derechos Digitales

LORTA : Ley Orgánica 5/1992, de Regulación del Tratamiento Automatizado de los Datos de Carácter Personal

LPDP : Ley de Protección de Datos Personales – Perú

LPDPA : Ley de Protección de Datos Personales – Argentina

OCDE : Organización para la Cooperación y el Desarrollo Económico

PDPAHD : Ley de Protección de Datos Personales y Acción de "Habeas Data" – Uruguay

RGPD : Reglamento General de Protección de Datos de la Unión Europea

SBS : Superintendencia de Banca, Seguros y AFP

SEAR : Sistema Efectivo de Análisis de Riesgo

TIC : Tecnologías de la Información y Comunicación

UE : Unión Europea

UIT : Unidad Impositiva Tributaria

RESUMEN

El trabajo de investigación describe la problemática existente en el manejo de la información por parte de las empresas públicas en el Perú, debido a la ausencia de controles del Estado en el tratamiento de datos. En ese sentido, nuestra legislación establece que las entidades incorporen en el tratamiento medidas de seguridad, sin embargo, no aseguran que las compañías actúen en el marco de la legalidad mediante la implementación del It Compliance, Privacidad y Protección de Datos, como instrumento de cumplimiento del buen gobierno corporativo. Es por ello que el estudio pretende describir el It Compliance, Privacidad y Protección de Datos para empresas del sector público en el Perú; asimismo, determinar el estado actual del It Compliance, Privacidad y Protección de Datos en el Perú; comparar el It Compliance, Privacidad y Protección de Datos en los sistemas jurídicos del Perú con la Unión Europea, España, Argentina y Uruguay. Se utilizó el diseño de investigación cualitativa, y los métodos comparativo y propositivo. Los resultados obtenidos nos permiten observar importantes similitudes entre la regulación de los datos personales de la Unión Europea y el Compliance, pues mediante un sistema jurídico de autorregulación exige a las entidades la adopción de programas de cumplimiento normativo en el tratamiento de datos, estas disposiciones han sido homogenizadas en España e influenciando en Argentina, Uruguay y Perú, sin embargo, nuestra legislación débilmente desarrolló estos dispositivos. Concluimos, que en la actualidad nuestro ordenamiento jurídico carece de incentivos y normas que garanticen la seguridad en el tratamiento de datos. Si bien, la normativa sectorial establece la incorporación de medidas de seguridad en el tratamiento, éstas han demostrado ser insuficientes para incentivar una cultura de cumplimiento y crear condiciones para que las

empresas se autorregulen mediante la implementación del It Compliance, Privacidad y Protección de Datos.

Palabras clave: Autorregulación Regulada, Compliance, Diseño por Defecto, Gobierno Corporativo, It Compliance de Privacidad y Protección de Datos.

ABSTRACT

The research paper describes the problem in the management of information by public companies in Peru, due to the absence of state controls in the processing of data. In that sense, our legislation establishes that entities incorporate security measures into the treatment, however, they do not ensure that companies act within the framework of legality through the implementation of It Compliance, Privacy and Data Protection, as a compliance instrument of good corporate governance. That is why the study aims to describe It Compliance, Privacy and Data Protection for public sector companies in Peru; also, determine the current status of It Compliance, Privacy and Data Protection in Peru; Compare It Compliance, Privacy and Data Protection in the legal systems of Peru with the European Union, Spain, Argentina and Uruguay. The qualitative research design, and the comparative and propositive methods were used. The results obtained allow us to observe important similarities between the regulation of personal data of the European Union and Compliance, because through a legal system of self-regulation requires entities to adopt regulatory compliance programs in the processing of data, these provisions have been homogenized in Spain and influencing in Argentina, Uruguay and Peru, however, our legislation weakly developed these devices. We conclude that, at present, our legal system lacks incentives and regulations that guarantee the security of data processing. Although, the sector regulations establish the incorporation of security measures in the treatment, they have proved insufficient to encourage a culture of compliance and create conditions for companies to self-regulate through the implementation of It Compliance, Privacy and Data Protection.

Keywords: Regulated Self-Regulation, Compliance, Default Design, Corporate Governance and Privacy, Data Protection Compliance.

I. INTRODUCCIÓN

La presente investigación intitulada: *"It Compliance, Privacidad y Protección de Datos para empresas públicas en el Perú"* aborda un problema latente en la actualidad, relacionada con el tratamiento de la información por parte de las entidades, ya sean públicas o privadas; si bien es cierto nuestra legislación establece la adopción de medidas técnicas, organizativas y legales en el tratamiento de datos, éstas no aseguran que las empresas se autorregulen mediante un sistema de cumplimiento normativo y así garantizar seguridad en el manejo de datos.

De acuerdo a los procedimientos administrativos sancionadores tramitados ante la Dirección General de Protección de Datos Personales del Ministerio de Justicia, en el 2015 se sancionaron administrativamente a 27 entidades, el 2016 a 41, el 2017 a 47 y en el 2018 a 19, otras se encuentran en etapa de apelación y, conforme a lo establecido por el ente fiscalizador de la Dirección, la infracción más recurrente está vinculada al incumplimiento de las medidas de seguridad en el tratamiento de datos.

Acorde a la problemática actual, destacamos que diversos organismos internacionales han establecido un sistema de responsabilidad de la persona jurídica, disponiendo que se autorregulen y que cooperen con los poderes públicos, mediante la adopción de "programas de cumplimiento", "compliance", "códigos de buenas conducta", "programas de prevención de delitos", entre otros. Estas medidas se ven orientadas a lograr una gestión empresarial que evite la comisión de ilícitos y promueva valores éticos en la empresa.

De acuerdo con (García, 2013), el término compliance se utiliza para significar el mecanismo empresarial de evitación y detección de infracciones legales en general, algunos estudios lo particularizan en función del ámbito jurídico específico, por ejemplo, se habla,

del "*anti-trust-compliance"*, en relación a la defensa de la competencia, "*tax compliance"* referido a la regulación tributaria o del "*criminal compliance"*, relacionado al cumplimiento normativo jurídico-penal. Bajo esta lógica, se hace uso de la expresión "*It Compliance, Privacidad y Protección de Datos"*, para referirse a aquel sistema relacionado con la seguridad y protección de la información.

En ese sentido, se desarrollará la privacidad y protección de datos como uno de los controles fijos en la matriz de aplicabilidad y cumplimiento normativo de las empresas públicas; para los fines del presente estudio se hará un análisis comparativo entre nuestro marco legislativo con la Unión Europea, España, Argentina y Uruguay. Finalmente, se presentará un Manual de Gestión Integral de Riesgos, el mismo que facilitará los lineamientos que debe adoptar una empresa pública del sector energético para prevenir infracciones legales relacionadas con las brechas en la seguridad de la información.

1.1. PLANTEAMIENTO DEL PROBLEMA

1.1.1. DESCRIPCIÓN DEL PROBLEMA

El gran porcentaje de informalidad en el tratamiento de la privacidad y protección de datos por parte de las entidades, ya sean públicas o privadas ha generado que la legislación comparada en gran acierto adopte un sistema de organización por defecto mediante la incorporación de mecanismos de prevención y control en el manejo de datos, además de imponer multas elevadas en caso de irregularidades e incumplimiento de la normativa sectorial. En ese sentido, se exige a las personas jurídicas que fomenten una cultura de cumplimiento y adopten un modelo de autorregulación regulada en el manejo de la información mediante la implementación del It Compliance, Privacidad y Protección de Datos.

La legislación peruana no es ajena a esta tendencia, mediante la ley N° 29733 “Ley de Protección de Datos Personales”, modificada por el Decreto Legislativo 1353; su Reglamento, aprobado por el Decreto Supremo N° 003-2013-JUS y la “Directiva sobre protección de datos personales y programas sociales”, Resolución Directoral N° 060-2014-JUS/DGPDP, establece la incorporación de medidas técnicas, organizativas y legales en el tratamiento de datos, sin embargo, estas disposiciones no se ajustan a las actividades económicas de las entidades, ni propician su cumplimiento para que las empresas públicas en el Perú se autorregulen mediante la implementación del It Compliance, Privacidad y Protección de Datos como instrumento del buen gobierno corporativo.

1.1.2. JUSTIFICACIÓN DEL ESTUDIO

La investigación justifica su importancia debido a la escasez de estudios acerca de las políticas del compliance en el tratamiento datos por parte de las personas jurídicas, siendo muy necesario que los titulares del banco de datos y encargados del tratamiento implementen

dispositivos de seguridad en el manejo de la información con la finalidad de generar confianza y credibilidad dentro de las instituciones.

En ese sentido, al existir un alto grado de informalidad en el manejo de la información por parte de las entidades, es muy necesario que las empresas del sector público en el Perú adopten lineamientos y mecanismos de control en el tratamiento de la información, mediante la implementación de programas de cumplimiento normativo en su organización interna, cuya finalidad contribuiría al correcto funcionamiento de los mercados.

En efecto, es imprescindible en la gestión empresarial que las compañías implementen el It Compliance, Privacidad y Protección de Datos a fin de cumplir el marco legal establecido en la normativa sectorial de protección de datos y eximirse de multas administrativas en caso se cometa alguna irregularidad en la seguridad de la información, e incentivar la aplicación de un sistema de autorregulación regulada.

Por último, los estudios que sustentan la presente investigación serán un nuevo aporte académico para la Escuela Profesional de Derecho, Facultad de Ciencias Jurídicas y Políticas de la Universidad Nacional del Altiplano, debido a la ausencia de investigaciones similares en nuestra casa de estudios, de esta manera contribuimos a la difusión de la implementación de las leyes blandas en las organizaciones, observándolas desde un punto de vista diferente.

1.2. OBJETIVOS DE LA INVESTIGACIÓN

1.2.1. OBJETIVO GENERAL

Describir el It Compliance, Privacidad y Protección de Datos para las empresas del Sector Público en el Perú.

1.2.2. OBJETIVOS ESPECÍFICOS

- Determinar el estado actual del It Compliance, Privacidad y Protección de Datos en el Perú.

- Comparar el It Compliance, Privacidad y Protección de Datos en los sistemas jurídicos del Perú con la Unión Europea, España, Argentina y Uruguay.

- Formular Políticas de It Compliance, Privacidad y Protección de Datos para las empresas públicas del Sector Energético en el Perú.

II. REVISIÓN DE LITERATURA

2.1. ANTECEDENTES DE LA INVESTIGACIÓN

2.1.1. A NIVEL INTERNACIONAL

De acuerdo al ámbito en el que se desarrolló la investigación y de la búsqueda realizada se encontró estudios relacionados con la presente, siendo los siguientes:

- **Artículo científico:** *"Hacia un nuevo sistema europeo de protección de datos: Las claves de la reforma"* de Artemi Rallo Lombarte (2012), cuyo planteamiento se refiere al análisis de las reformas europeas de protección de datos, cuyo planteamiento se relaciona en dos proyectos normativos presentado por la Comisión Europea: **(i)** Primero, el Proyecto de Reglamento del Parlamento Europeo y del Consejo para la protección de los ciudadanos en relación con el tratamiento de los datos personales y la libre circulación de dichos datos. **(ii)** Segundo, el proyecto de directiva del parlamento europeo y del consejo sobre protección de los ciudadanos en relación al tratamiento de los datos personales por las autoridades competentes con la finalidad de prevenir, investigar, detectar y perseguir delitos, y sobre el libre movimiento de la información.

El autor concluye que, las iniciativas de la Unión Europea están llamadas a revolucionar el marco global europeo de la protección de datos y a provocar un extraordinario impacto en el sistema español al resultar de directa e inmediata aplicación el reglamento 2016/679 de la (UE).

- **Artículo científico**: *"La transparencia en el nuevo Reglamento General de Protección de Datos"* de Elena García-Cuevas Roque (2018), cuyo planteamiento se desarrolla en los riesgos y peligros que se asiste en el tratamiento y difusión de las informaciones personales, la autora hace referencia a la Directiva 95/46 del Parlamento Europeo como hito principal en materia de protección de datos personales y describe los aspectos más relevantes del nuevo

Reglamento General de Protección de Datos 2016/679 (UE), fruto del compromiso asumido por el Parlamento Europeo y el Consejo de la Unión Europea.

La autora resalta la importancia de la aplicación del nuevo Reglamento General de Protección de Datos en las instituciones, tomando como puntos importantes los siguientes: que, **(i)** los datos personales deben tratarse de un modo que garantice una seguridad y confidencialidad adecuada, **(ii)** los datos personales solo deben tratarse si la finalidad del tratamiento no pudiera lograrse razonablemente por otros medios, **(iii)** las personas físicas deben tener conocimiento de los riesgos, las normas, las salvaguardias y los derechos relativos al tratamiento de datos personales, así como del modo de hacer valer sus derechos en relación con el tratamiento, **(iv)** debe fomentarse el establecimiento de mecanismos de certificación y sellos y marcas de protección de datos, que permitan a los interesados (conocer, de un modo sencillo y automatizado), y evaluar, con mayor rapidez, el nivel de protección de datos.

- Tesis Doctoral: *"La protección de datos personales en España: evolución normativa y criterios de aplicación",* de Emilia Zaballos Pulido (2013), la autora efectúa un análisis de la naturaleza y el contenido del derecho a la intimidad y la protección de datos, asimismo describe el efecto de las Tecnologías de la Información y las Comunicaciones en la evolución de la protección de datos personales, incluyendo la aparición de medios que permiten la gestión automatizada de la información, el tratamiento y el análisis discriminado de ingentes volúmenes de datos.

Las conclusiones que se arribaron a la investigación establecen que la normativa en materia de protección de datos de carácter personal debe ser preventiva, ello con la finalidad de minimizar el impacto de los avances tecnológicos y desarrollo social de la información. También resalta que el derecho a la protección de los datos de carácter personal ha seguido

un proceso de estandarización en el ámbito de la (UE), los países miembros han combinado un régimen de "listas blancas" de estados que garantizan la protección adecuada con una serie de requisitos que en ocasiones no son fáciles de aplicar.

2.1.2. A NIVEL NACIONAL

Se tomaron en cuenta los siguientes:

- Artículo científico: *"Programas de Cumplimiento como mecanismo de lucha contra la corrupción: Especial referencia a la autorregulación de las empresas"* de Guillermo Astudillo Meza y Sandra Jiménez Montes (2015), cuyo planteamiento refiere la importancia de la regulación estatal hacia las empresas debido a que los problemas financieros y de corrupción ocasionan perjuicio a la sociedad, para combatir este fenómeno diversos organismos internacionales han venido recomendando una serie de medidas para mejorar la gestión empresarial, tales como el Compliance o también llamado programa de cumplimiento.

Asimismo, señala que la autorregulación de las empresas en nuestro país no es nueva, pues ya existen normas en el ámbito de la prevención de riesgos laborales, de prevención de lavado de activos y la Ley de Protección de Datos Personales, las cuales exigen a las empresas que implementen ciertas medidas y capaciten a sus empleados en todo aquello que tenga que ver con el cumplimiento de la legalidad de dichas normas.

Los investigadores concluyen que la introducción de la responsabilidad penal de las personas jurídicas en nuestra legislación, por ejemplo en caso de soborno transnacional, ayudaría a sancionar a las personas jurídicas por emplear malas prácticas corporativas, además de incorporar un mecanismo preventivo y de control que sirva de incentivo para que las empresas se autorregulen acudiendo a los programas de cumplimiento y así concretar una verdadera cultura de cumplimiento de la legalidad al interior de sus organizaciones.

- **Artículo científico:** *"El derecho a la protección de datos personales. Algunos temas relevantes de su regulación en Perú"* de Francisco José Eguiguren Praeli (2015), cuyo planteamiento gira en torno al derecho a la protección de datos establecido en nuestra Constitución Política, además el autor analiza si el precepto normativo fundamental es tutelado adecuadamente por nuestra Carta Magna, asimismo se describe los aspectos más relevantes contenidos en la Ley 29733, Ley de Protección de Datos Personales y el reglamento de la misma, aprobado por Decreto Supremo 003-2013- JUS.

A manera de conclusión, el autor considera que la protección de los datos personales como un derecho fundamental resulta un suceso relativamente reciente en el ámbito jurídico. Por ello, la expedición de la Ley de Protección de Datos Personales y su reglamento, son un paso muy positivo para el desarrollo y aplicación del derecho estipulado en el inciso 6 del artículo 2 de la Constitución, "A que los servicios informáticos, computarizados o no, públicos o privados, no suministren informaciones que afecten la intimidad personal y familiar (…)".

Por último, el autor sugiere que la Autoridad Nacional de Protección de Datos Personales no debería ser una instancia dentro de la estructura interna del Ministerio de Justicia por lo que deberíamos tomar en cuenta la experiencia de instituciones similares en otros países, tales como España, México o en el caso de Latinoamérica, debiendo ser dotada con adecuados niveles de autonomía funcional y proyección institucional, acorde a los estándares internacionales.

2.2. MARCO TEÓRICO

2.2.1. CUESTIONES GENERALES DEL COMPLIANCE

2.2.1.1. CONCEPTO

Diferentes teorías explicativas de la criminalidad empresarial, destacan la importancia de los mecanismos de control interno y externo como factor preventivo de infracciones legales. Otras investigaciones afirman que uno de los motivos más trascendentales para que se incurra en actividades ilícitas, es el escaso o deficiente control interno dentro de las empresas. En este sentido tanto el control estatal como el control interno de la empresa resultan imprescindibles.

Es por ello, que de acuerdo con Kuhlen (2013) se denomina "compliance" a las medidas mediante las cuales las empresas pretenden asegurarse de que sean cumplidas las reglas vigentes para ellas y su personal, que las infracciones se descubran y que eventualmente se sancionen.

Asimismo, el término Compliance se refiere al verbo "to comply". En el diccionario inglés-alemán, la traducción que figura es "sith fügen" (N. de la T: en castellano: obedecer, someterse, plegarse). En inglés Americano aparece como explicación esencial: "to comply=to act in accordance with a command, request, rule, wish, or the like". El derivado interesante, que al final tiene su origen en el "complere" latino, da un rodeo por el "complire" italiano y el "cumplir" español. Como se aprecia, la traducción casi literal de la palabra compliance al español se encuentra distante del concepto relacionado a los valores éticos que suelen encontrarse en la reciente bibliografía que se escribieron recientemente. En suma, el término "cumplimiento" al que se hizo referencia sólo nos ofrece una sencilla noción de su significado, **el cumplimiento de lo que es legal o de lo que es conforme a derecho.** Prittwitz, citado por Kuhlen & Montiel (2013:208).

Por otro lado, al término “Compliance” se le puede atribuir diferentes aplicaciones, siendo utilizado por diferentes empresas y profesionales dentro del ámbito de actuación de cada uno, por eso encontramos vertientes y sectores tales como “criminal Compliance”, “finance Compliance”, corporate Compliace” o “it Compliance”, éste último vinculado a la privacidad y protección de datos personales.

Pues bien, en la función de Compliance no sólo se suelen englobar las leyes y directrices de derecho positivo obligatorias de cumplir por los sujetos afectados (conocidos como hard law), sino que también se suelen englobar recomendaciones y estándares de voluntaria adopción (conocidos como soft law).

En efecto, de acuerdo con la propia ISO 19600 (guía de referencia internacional para dotar a las organizaciones de un Sistema de Gestión de Compliance), “un sistema de gestión de Compliance eficaz y que aborde a toda la organización permite que la organización demuestre su compromiso de cumplir con la normativa, incluyendo los requisitos legales, los códigos de la industria y los estándares de la organización, así como con los estándares de buen gobierno corporativo, las mejores prácticas, la ética y las expectativas de la comunidad en general” Sáiz (2016:39).

De acuerdo con Reyna (2018:573-574), existen tres momentos importantes en la evaluación del compliance: (1) negativo, (2) positivo; (3) integración de las tesis de gobernanza, riesgo y *compliance* (GRC). La (1) concepción negativa se restringe a la elaboración de políticas corporativas preventivas, volcadas a la detección, determinación y **reaccionante** las infracciones económicas, desde una mentalidad preventiva. Hasta entonces, *compliance* se interpretaba en los límites de las estrategias de defensa ex ante y ex post en relación con el comportamiento desviante. En un segundo momento, fase (2) positiva, surgieron esfuerzos más imaginativos, orientados al comportamiento corporativo prosocial.

Se difunde que la importancia de los programas de compliance está más allá de la simple noción defensiva y debe promover prácticas efectivas de integridad, priorizando no solamente la intolerancia frente a lo que está errado, sino también enalteciendo las buenas prácticas desarrolladas en el ambiente empresarial.

En la fase (3) se destaca la integración de las estrategias de GRC, en función de que se desarrollan estrategias de perfeccionamiento de la gestión empresarial. También es verdad que la profesionalización de la gestión promovida por las estrategias GRC garante mejores padrones de defensa, permitiendo mejor conducir las operaciones de comunicación, documentación y los mecanismos de protección de intereses de terceros.

En esa línea evolutiva los programas de Compliance pueden ser entendidos como un programa organizado para incrementar la gestión organizacional y la capacidad regulatoria para prevención de infracciones económicas y control de riesgos.

Por último, el Compliance ya no es solamente un instrumento que asegura el valor de la empresa, sino un criterio que se utiliza decisivamente en la determinación de las responsabilidades jurídicas, por lo que el estado debe generar condiciones para que las corporaciones lo implementen, por medio de una coordinación con los poderes públicos y otros agentes sociales. Nieto, citado por García (2013).

2.2.1.2. PRECISIONES ACERCA DEL COMPLIANCE

Existen ideas equivocadas acerca de las funciones del Compliance, creando confusión en el mundo jurídico y las empresas que implementan un programa de cumplimiento normativo, a continuación, explicaré los enfoques más comunes.

2.2.1.2.1. EL COMPLIANCE SE DEDICA EXCLUSIVAMENTE A PREVENIR RESPONSABILIDAD PENAL EN LAS EMPRESAS

La prevención de ilícitos penales es muy usada para significar al Compliance, sin embargo, diferentes estudios sectoriales definen que ésta no suele ser la única responsabilidad que las corporaciones suelen tener encomendada. Desde un punto de vista de cumplimiento legal, la función de Compliance puede tener competencias para el cumplimiento de la normativa de protección de datos, prevención de blanqueo de capitales, protección del medio ambiente, derecho de la competencia, mercado y consumidores, sociedad de la información, etc.

En efecto, lo usual es que las corporaciones cuenten con un programa de cumplimiento general, en el que la observancia de la ley engloba diversos sectores jurídicos. La distinción de los ámbitos jurídicos implicados poco importa en la conformación del compliance, en la medida en que lo que le interesa a la dirección de la empresa es simplemente evitar las multas de las infracciones legales en general. Nieto, citado por García (2013).

Por otro lado, la función de Compliance está muy asociada en otras compañías con materias del Buen Gobierno Corporativo, Gestión de Riesgos Corporativos, Ética y Responsabilidad Social Corporativa. De hecho, en grandes multinacionales, especialmente con origen anglosajón, cada vez es más común encontrarse con Áreas de Ética y Compliance, donde al componente normativo se le suma un importante componente cultural y de comportamiento empresarial que va más allá de la vinculación de la empresa a las leyes (Sáiz, 2016).

2.2.1.2.2. ELABORAR UN CÓDIGO DE CONDUCTA SIGNIFICA CUMPLIR CON LAS OBLIGACIONES DEL COMPLIANCE

Es cierto que los códigos de ética o de conducta, son elementos que exponen una serie de principios que las empresas deben implementar, a fin de dar cumplimiento a los planes del compliance, ya que contendrá un resumen de las principales pautas de comportamiento que se esperan de los empleados.

Pero este estos códigos, son apéndices dentro de una alta gama de actuaciones tendentes a crear una auténtica cultura corporativa del cumplimiento normativo, podríamos resumirlo en los siguientes:

- Definición del alcance y del ámbito de las materias a incluir. (finanzas, contratos, protección de datos, etc).
- Estructura organizativa, nombramiento de la función de Compliance, colocación en la estructura jerárquica de la compañía, dotación de competencias y recursos, etc.
- Establecimiento y aprobación del marco normativo, procedimientos, cláusulas y guías que van a regir con empleados, proveedores, accionistas, etc.
- Implantación de controles concretos que en los procesos de negocio se van a implantar para detectar actuaciones que contravengan el Programa de Compliance.
- Definición de las funciones de revisión y auditoría para comprobar la eficacia de las medidas de control debido adoptadas, e implantación de mejores en el sistema.
- Esquematización de los niveles y periodicidad de los informes a la Dirección de la compañía.

Como se puede apreciar, hablamos de algo que va más allá de redactar un Código ético y distribuido. En ese sentido cabe citar la Circular 01/2011 de la Fiscalía General del Estado de España, relativa a la responsabilidad penal de las Personas Jurídicas conforme a la

reforma del Código Penal efectuada por Ley Orgánica número 5/2010, que establece que "lo importante no es la adquisición de un código de autoregulación", sino la acreditación de que "los gestores o los órganos de gobierno de la persona jurídica han ejercido por sí o por delegación en otras personas todas las medidas exigibles para la prevención, detección y reacción ante posibles delitos" (Sáiz, 2016: 35-39).

2.2.1.2.3. EL COMPLIANCE SÓLO SE TRATA DE CUMPLIR EL MARCO NORMATIVO

La irrupción del Compliance en todo tipo de compañías y sectores se está haciendo de forma muy diversa a nivel organizativo dependiendo del volumen, actividad, sector e historia de cada empresa: como un área independiente, dentro de área Legal y Compliance, más vinculado a Auditoría interna, Control Interno o Gestión de Riesgos, e incluso dentro de las áreas de responsabilidad de ética y Responsabilidad Social Corporativa.

Y efectivamente se trata de hacer cumplir leyes, pero no sólo leyes, ya que dentro de la función de Compliance podemos encontrar competencias para controlar el cumplimiento de normativas internas, código de conducta, códigos de autorregulación sectorial, obligaciones y contratos, así como puntos de control derivados de estándares internacionales no obligatorios.

Asimismo, existen tres características que, de nuevo, podrían considerarse como diferentes a la habitual función de la Asesoría Jurídica de una empresa y son:

- Carácter autónomo e independiente del área del Compliance, para que cualquier conducta pueda ser investigada de forma nítida y sin interrupciones ni impedimentos por otras áreas o intereses dentro de la organización.
- Carácter más preventivo y asociado al análisis y la gestión de riesgos. Mientras que en muchas compañías el papel de la Asesoría en muchos casos contractual y después

contenciosa, la función del compliance realiza análisis de riesgos, evaluaciones de impacto de nuevos requisitos normativos, estudio del retorno de inversión antes de acometer un proyecto de cumplimiento normativo, medición de los niveles de cumplimiento ante una norma, etc.

- Capacidad de investigación interna ante una denuncia interna, con el objetivo de esclarecer los hechos acaecidos y evaluar si los mismos suponen un quebrantamiento de las normas o políticas corporativas, así como los riesgos que los mismos suponen para la compañía (Sáiz, 2016:36-38).

2.2.1.3. EL COMPLIANCE EN LAS EMPRESAS

La complejidad de la estructura normativa que rige a todos los niveles, desde el ámbito más local al entorno más globalizado, hace importante que todas las organizaciones que realizan actividades económicas en la sociedad, ya sean empresariales o no, ya sean públicas o privadas deban gestionar y controlar el cumplimiento tanto de normas externas (legislación general y regulación sectorial) como de regulaciones internas, propias o sectoriales (políticas corporativas, reglamentaciones relacionadas con la ética y la conducta) (Sáiz, 2016: 56).

Por ello, y con tal finalidad, se justifica el establecimiento, en la organización de estructuras de gestión complejas de una función de Compliance que identifique los riesgos de incumplimiento normativos, asesore como resultado de la evaluación del riesgo, alerte sobre posibles incumplimientos y realice el seguimiento de su corrección, informado al órgano de dirección de la organización sobre sus comprobaciones y conclusiones.

Además, la implementación de esta función trasciende los aspectos prácticos de prevención y control de riesgos normativos y llegar a convertirse en una cuestión de cultura corporativa que impregna toda la organización, dando valor y confiabilidad a la propia

estructura organizativa, que estará en mejores condiciones de asegurar la adecuación de su actividad a los requisitos normativos de su entorno y a sus propios códigos de conducta, cuanto más desarrollada y definida resulte esta función en el esquema de gestión de sus áreas funcionales.

2.2.1.3.1. DEL CUMPLIMIENTO EN LAS EMPRESAS PÚBLICAS

El término compliance significa **"cumplimiento",** "observancia", "conformidad con determinados mandatos", y hace alusión en este contexto a procedimientos para la "transposición de prescripciones legales" con la pretensión de evitar la criminalidad empresarial. Bermejo citado por Kulhen (2016).

El cumplimiento de las regulaciones aplicables y la integridad de la conducta en las empresas son elementos esenciales para cualquier empresa y **especialmente en aquellas compañías que operan en sectores regulados, como son la banca, la electricidad** y la energía, el suministro de agua, el transporte o las telecomunicaciones.

El Compliance se convierte en una cuestión crítica ya que, a diferencia del resto de los sectores regulados en los que el objeto de negocio viene dado por el suministro de un servicio en condiciones justas de mercado y precios competitivos, en la banca o en los seguros, la naturaleza del éxito radica en la confianza de sus clientes.

Es por ello, que el **cumplimiento** de estos programas tiene una mayor aceptación en la cultura jurídica continental, siendo necesario implementar una cultura corporativa con buenas prácticas empresariales no sólo por un cumplimiento obligado sino por el espíritu de la ley con la vista puesta a la evolución y progresiva elevación a la categoría de normas imperativas de las llamadas leyes blandas (significa que su contenido no es jurídicamente vinculante) o códigos de conducta (Sáiz, 2016).

2.2.1.3.2. LA FINALIDAD DEL COMPLIANCE EN LAS ENTIDADES

Llegado a este punto, podemos verificar que, el compliance constituye un mecanismo interno de supervisión en las empresas, cuya finalidad es asegurar la observancia del marco normativo en las actividades comerciales de las corporaciones. Esta finalidad esencial se dimensiona, en dos funciones diferenciables: La función de prevención y la función de confirmación del Derecho (García, 2013).

La función de prevención, conlleva la implementación de un conjunto de medidas organizativas y de vigilancia al interior de las empresas, tendentes a evitar que se produzcan infracciones legales. Se lleva a cabo una prevención situacional de dichas infracciones a nivel de estructura empresarial, pues es previsible que las empresas cuenten con los recursos y el conocimiento suficiente para monitorear y controlar adecuadamente los riesgos de infracciones legales.

Es decir, la empresa está obligada a implementar medidas que garanticen que sus actividades estén acorde al marco legal y que evite que sea la propia organización empresarial la que provoque que la conjunción de los aportes individuales, por sí mismos inocuos, devenga en una infracción a la norma (García, 2013:23).

La otra labor, es la función de confirmación del Derecho, esta función se materializa en el establecimiento de diversos mecanismos confiables y seguros para la detección interna de irregularidades cometidas, así como para la realización de actos de reparación y, de ser el acaso, de denuncia a las instancias correspondientes.

2.2.1.4. DEL OFICIAL DE CUMPLIMIENTO

La responsabilidad de cumplimiento normativo corresponde en la obligación de las entidades a adoptar políticas y procedimientos que sean necesarios para garantizar el cumplimiento de la norma, así como de tomar las medidas necesarias para reducir el riesgo de incumplimiento.

A efectos organizativos, esta responsabilidad de cumplimiento normativo debe recaer en la más alta dirección de la empresa, siendo ésta la responsable de crear la organización adecuada para verificar la eficacia del cumplimiento.

Por su parte, el órgano de verificación del cumplimiento normativo debe ser considerado como un órgano permanente, independiente y eficaz que ayude a la alta dirección a controlar y evacuar regularmente la adecuación de las medidas y procedimientos establecidos de conformidad con el párrafo anterior, así como las medidas correctoras implantadas, ya asesorar y asistir a dichos gestores para el cumplimiento de las obligaciones de la empresa.

La mencionada distinción debe tenerse presente al analizar, no solo los roles de cada una de las funciones dentro de la empresa, sino también la relación entre los distintos trabajadores que están involucrados en el cumplimiento normativo de la empresa. Por ejemplo**,** el Directorio será habitualmente el órgano en quien recaiga la responsabilidad última del cumplimiento normativo en la empresa y probablemente la persona a la que reportará (directa o indirectamente), el responsable de verificación de cumplimiento normativo, mientras que será dicho responsable de verificación de cumplimiento normativo quien se encargará de impartir formación al resto de áreas de la organización y de monitorear que los procedimientos y controles definidos para que el plan de cumplimiento sea efectivo, se desarrollen e implanten conforme han sido diseñados. (En relación al tratamiento de datos en la Unión Europea, al compliance officer se denomina Delegado de Protección de Datos).

En la legislación peruana, al Compliance officer se le llama oficial de cumplimiento, quien tiene a su cargo el control del cumplimiento del programa respectivo (prevención) y la denuncia de las irregularidades que se cometan en la empresa (represión). Puede tener acotado su responsabilidad a determinados sectores, como el de las contravenciones y delitos

(criminal Compliance Officer). Puede tratarse también de un departamento del cumplimiento integrado por varias personas bajo la dirección de un "chief compliance officer" (Reyna, 2018:25-26).

2.2.1.5. VENTAJAS DEL COMPLIANCE EN LAS ORGANIZACIONES

Dentro de las ventajas financieras de una estructura de cumplimiento imbuida en la organización. La primera y más evidente se manifiesta en el ahorro económico que supone la evitación de las sanciones que se pueden imponer a las organizaciones por incumplimientos normativos.

Así, son muchas y muy diversas las normas que tipifican infracciones como graves y muy graves para luego establecer un régimen sancionador que recoge importes monetarios muy relevantes.

A modo meramente ejemplificativo, la Ley 30424, modificada por el D. Leg. 1352, exige la implementación de un programa de cumplimiento (Compliance) por parte de todas las personas jurídicas del país a fin de reducir o evitar la comisión de los delitos de cohecho activo genérico y específico, cohecho activo transnacional, lavado de activos, minería ilegal o terrorismo por parte de los miembros de la empresa, siguiendo el marco legal encontramos dos aspectos sustanciales: **(i)** Las sanciones que pueden ir desde la imposición de una multa hasta el cierre de la entidad y, **(ii)** El modelo de prevención que, si se implementa y aplica correctamente, puede salvar a la compañía.

Por si la ventaja anterior no fuera suficiente beneficio para una organización, parece claro que disponer de una función de cumplimiento normativo y desempeñar la actividad de forma ética y cumpliendo con la normativa vigente tiene ventajas estratégicas para los negocios, pues pueden suponer una mayor creación de valor, tanto para los accionistas, como para el resto de grupos de interés.

En muchos casos, esta ventaja estratégica no bien derivada directamente del solo cumplimiento de la normativa que resulta aplicable a una entidad, sino que es la consecuencia de una actitud proactiva de las empresas que han decidido hacer de la necesidad virtud.

Finalmente, otro efecto positivo que una cultura de comportamiento empresarial social tiene para las compañías es la atracción de talento, acercando a los profesionales más prometedores y preparados y animándolos a unirse a un proyecto rentable y respetable. Así, existen estudios que concluyen que la política de una compañía en materias como el tratamiento del medio ambiente, las relaciones con la comunidad, la diversidad de género el tratamiento de los empleados puede ser críticas a la hora de elegir o no a una empresa para trabajar (Sáiz, 2016:60-63).

2.2.2. EL IT COMPLIANCE, PRIVACIDAD Y PROTECCIÓN DE DATOS

2.2.2.1. ASPECTOS GENERALES

En Europa, en particular en los 28 estados que conforman la Unión Europea (UE), se ha establecido un marco común que regula el mercado de instrumentos financieros cuyo objetivo es fijar un régimen homogéneo en el sector de los servicios financieros, protegiendo a los inversores y consumidores.

En efecto, en el marco de la privacidad y protección de datos, la (UE) mediante el Reglamento (UE) 2016/679 relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales, obliga a las empresas y profesionales a adecuar sus procesos y operaciones de tratamiento de datos personales, así como a realizar revisiones periódicas para garantizar su cumplimiento, cuyas directrices son de aplicación directa e inmediata en los estados miembros de la (UE).

Sin embargo, ¿Por qué es necesario referirnos a la normativa de la Unión Europea para tratar el It Compliance, Privacidad y Protección de Datos?, pues bien, nos encontramos que, con el nuevo marco legal de protección de datos, es decir en el Reglamento (UE) 2016/679 se han introducido mecanismos de control muy similares a los del Compliance, denotándose una tendencia hacia la autorregulación de las compañías, sean públicas o privadas.

Acorde a lo señalado, encontramos los mecanismos de control más resaltantes que posteriormente serán analizados:

- **Análisis de riesgos y evaluación del impacto,** cuya finalidad es controlar la incertidumbre relativa a las amenazas en la información a fin de mitigar los riesgos en el tratamiento de datos.

- **Data Protection Officer,** el Reglamento introduce esta figura a modo de supervisor de cumplimiento de las obligaciones impuestas en la normativa de protección de datos.

- **Principio de Responsabilidad Proactiva,** del cual el responsable del tratamiento será responsable del cumplimiento de los principios relativos a la seguridad y debe estar en la capacidad de demostrarlo.

- **Régimen sancionador,** se prevé que las sanciones para a establecerse entre 100 y 1,000.00 euros de multa o, en su caso, si son empresas hasta un 5% de la facturación anual a nivel mundial.

Las figuras señaladas fueron introducidas en el marco legal de la (UE) y serán tratadas en el capítulo IV de la presente investigación. No obstante, es muy importante resaltar que diferentes especialistas en el manejo de la información y tratamiento de soft law (leyes blandas). Sáiz (2016) ha categorizado estas disposiciones como una materia del compliance, definiéndolo como It Compliance, Privacidad y Protección de Datos, siendo aquel programa

de cumplimiento normativo que las empresas deben adoptar para asegurar y garantizar la seguridad en el tratamiento de la información.

Pues bien, encontrándonos en ese contexto, corresponde ver algunos ejemplos de aplicación del It Compliance, Privacidad y Protección de Datos, resultando los siguientes:

En América Latina, contamos con Ecopetrol S.A., perteneciente a la industria petrolera establecida en Colombia, esta entidad ha implementado un programa de protección de datos, con la finalidad de establecer responsabilidad corporativa mediante la implementación de mecanismos de control en el tratamiento de datos.

En Norteamérica, se tiene a LinkedIn Coporation, que tiene sus filiales en Estados Unidos y cumple con los sistemas de seguridad de la información, establecidos por la Unión Europea y Suiza, asimismo, adoptó programas de cumplimiento en el manejo de la información, haciéndola una comunidad social confiable.

En Europa, uno de los casos más emblemáticos es del grupo Bayer AG, empresa químico farmacéutica, fundada en Alemania. Esta entidad dio importancia al creciente Buen Gobierno Empresarial y adoptó políticas de cumplimiento legal y responsabilidad corporativa, implementado políticas de It Compliance, Privacidad y Protección de Datos, para proteger y asegurar los datos compilados en sus registros.

Por último, las empresas antes descritas están en constante movimiento económico por lo que, al cumplir con estas garantías pueden comercializar o transferir los datos entre diferentes estados, por ejemplo, si una empresa de América Latina realiza un flujo transfronterizo de datos en alguno de los países miembros de la (UE), digamos Francia, esta entidad debe cumplir con los estándares mínimos señalados en la (UE), es decir la adopción de políticas de cumplimiento normativo en el manejo de datos.

2.2.2.2. DEL TRATAMIENTO DE DATOS EN LAS EMPRESAS PÚBLICAS

El progreso tecnológico social demanda que el ordenamiento jurídico no sólo proteja la más estricta intimidad del individuo, sino también garantías para asegurar el tratamiento y circulación de los datos personales en sus relaciones con terceros dentro de una organización, ya sea pública o privada, por ejemplo, la Unión Europea obliga a las empresas públicas la implementación de medidas de prevención en la regulación de datos.

Esto viene del reconocimiento de los derechos humanos que abrió la incorporación de nuevos valores que han sido reconocidos por la doctrina, tal es el caso del derecho a la protección de datos, cuyo origen se remonta a la célebre sentencia del Tribunal Constitucional Alemán de 1983, que por primera vez hace referencia al principio de **"autodeterminación informativa"**, -definido como la capacidad de control que tiene la persona sobre toda la información personal-, este tribunal establece que el derecho de protección de datos debe ser enmarcado en el derecho general de protección de la persona, por considerar que garantiza la facultad del titular a determinar por sí mismo la divulgación y utilización de sus datos personales.

Asimismo, el Tribunal Alemán sostiene que lo decisivo en la protección de datos no es la esfera íntima de la persona; sino, la utilización, la finalidad del tratamiento o la posible interconexión de los datos personales tratados. Es por ello, que de acuerdo a Herrán (2003), la protección de datos constituye una respuesta jurídica frente al fenómeno de la sociedad de la información, para frenar la potencial amenaza que el desarrollo tecnológico representa para los derechos y libertades de las personas.

En ese sentido, diferentes instituciones se esfuerzan por implementar medidas organizativas en el tratamiento de datos, a fin de garantizar un adecuado cumplimiento del

marco legal y evitar ser multadas en caso se presente alguna brecha en la seguridad de la información.

2.2.2.3. EL COMPLIANCE EN EL TRATAMIENTO DE DATOS

Los programas de cumplimiento enfocados al manejo de la información, constituyen una expresión de soft law (leyes blandas) que las compañías vienen adoptando, como forma de demostrar su responsabilidad con la sociedad y de garantizar protección frente a eventuales responsabilidades por infracciones en las brechas de seguridad de la información. Estos programas son un fenómeno relativamente novedoso, que hace referencia a unos protocolos de actuación que las empresas crean para supervisar sus propias acciones y evitar ser sancionadas.

Pues bien, se trata de procedimientos y reglas que, no siempre están dotados de fuerza jurídicamente vinculante, es decir que la normativa del estado lo prescriba de forma obligatoria. Estos principios se establecen para encausar efectos prácticos, toda vez que se prevén consecuencias jurídicas en caso de inobservancia de tales procedimientos, por ejemplo, la inobservancia de las disposiciones referidas al tratamiento de la privacidad y protección de datos en la Unión Europea son sancionadas con multas 20,000,000 EUR o 4% del volumen de negocio global del último año.

El plan, bien que se trate de una ordenación **intra-empresarial,** reviste, por tanto, caracteres de valor **cuasi-normativo.** Los programas institucionalizan la responsabilidad social de la compañía para la protección, fundamentalmente, de intereses financieros; es decir, despliegan su ámbito de influencia preferentemente en el área económica y, más en concreto en el de la contabilidad y auditoría, pero no exclusivamente, porque tienen a asegurar también otros intereses generales.

Para finalizar, la aparición de estos programas en nuestro país está inicialmente vinculada con la legislación del mercado de valores. Su implantación obedece, fundamentalmente, a los requerimientos de la ley 24/1998, de 28 de julio de Mercado de Valores, que obliga a las empresas de servicios de inversión e instituciones a establecer procedimientos de control interno del cumplimiento normativo, otro sector importante corresponde a las obligaciones de la Ley N° 29733 "Ley de Protección de Datos Personales", donde obliga al titular del banco de datos y encargado del tratamiento a adoptar medidas técnicas, organizativas y legales para garantizar la protección de los datos personales de los usuarios.

2.2.2.4. DESCRIPCIÓN DEL IT COMPLIANCE, PRIVACIDAD Y PROTECCIÓN DE DATOS

El cumplimiento en materia de protección de datos es una de las mayores preocupaciones de la empresa. La normativa europea nos permite observar importantes similitudes entre la regulación en esta materia y otros sistemas de Compliance, pues en este sector es donde hubo un avance muy significativo y homogenizado en relación al tratamiento de la privacidad y protección de datos personales.

Como lo hemos descrito anteriormente, si bien es cierto el Compliance está asociado a la prevención de los delitos de cohecho, lavado de activos, peculado entre otros, diversas instituciones públicas o privadas principalmente de origen anglosajón incluyen dentro de su programa de cumplimiento a la protección de datos y seguridad de la información, protección del derecho al medio ambiente, derecho de la competencia, entre otros.

En ese sentido, definimos al It Compliance de Privacidad y Protección de Datos, como el conjunto de acciones que las organizaciones deben desarrollar para cumplir con las obligaciones legales o contractuales obligatorias o aquellas libremente asumidas y con los

requisitos de seguridad derivados de las mismas, en los procesos corporativos de gestión de los sistemas de información, también el *"Cumplimiento TI"* hace referencia a todas aquellas medidas relacionadas con la protección de los datos y de las propias infraestructuras de las Tecnologías de la Información y la Comunicación (TIC) que los almacenan, procesan y transmiten, como puedan ser las políticas de accesos a datos confidenciales o los sistemas de alerta temprano frente a ciberataques.

Acorde a ello, se deriva el derecho fundamental a la protección de datos, pues bien, abarcando ello, el cumplimiento de las medidas organizativas constituye uno de los principales cometidos de las áreas dirigidas a asegurar el cumplimiento normativo de cualquier organización, llámese It Compliance, asesoría jurídica, control interno, etc. Por cuanto que es habitual que el desarrollo de cualquier actividad empresarial conlleve la necesidad de recabar y tratar datos personales relativos a empleados, candidatos o clientes, entre otros.

En síntesis, el It Compliance de Privacidad y Protección de Datos exige una actitud consciente, diligente y proactiva por parte de las organizaciones frente a todos los tratamientos de datos personales que se lleven a cabo; para describir este programa de cumplimiento normativo se hará un análisis comparativo entre la Unión Europea, España, Argentina, Uruguay con nuestro ordenamiento jurídico.

2.2.2.5. IMPORTANCIA DEL IT COMPLIANCE DE PRIVACIDAD Y PROTECCIÓN DE DATOS

El cumplimiento de TI describe, entre otras cosas, el cumplimiento de las leyes y normas legales aplicables que regulan, por ejemplo, el manejo de los datos del titular. El nuevo Reglamento General de Protección de Datos de la UE (GDPR) de la Unión Europea es un ejemplo prominente y muy discutido.

Las empresas deben establecer procesos que garanticen el cumplimiento de estas leyes, por ejemplo, restringiendo el acceso a datos confidenciales, nombrando a un supervisor del tratamiento, cumplimiento de deberes, implementación o sistemas de alerta temprana para ataques de piratas informáticos. La administración de cumplimiento también debe cumplir con ciertos estándares de la industria.

Es tal la importancia de esta materia que en diversas legislaciones reviste la categoría de derecho fundamental, es decir, la protección de datos personales garantiza a su titular la facultad de controlar el uso que los terceros hacen de su información y la capacidad de disponer y decidir sobre dicho uso, además:

- Se trata de una norma auditable.
- Las consecuencias de su incumplimiento, en ocasiones, se tangibilizan en sanciones económicas elevadas, y en otras, se manifiesta en impacto reputacional, lo que provoca, en muchas ocasiones, deterioro de la imagen corporativa y/o pérdida de competitividad.
- Por otro lado, el cumplimiento de esta norma tiene un impacto positivo en la percepción de la marca por parte de clientes y potenciales consumidores por cuanto que la garantía de privacidad transmite seguridad y confianza.

2.2.2.6. OBJETIVOS DEL PROGRAMA IT

Entre los principales objetivos de que la empresa sea pública o privada establezca un programa de cumplimiento enfocado al tratamiento de la privacidad y protección de datos, son los siguientes:

- **Minimizar riesgos:** Se puede describir en la reducción de las sanciones por infracciones al tratamiento de datos personales, en el Perú reduciría el monto de la multa ya que en nuestro ordenamiento jurídico la persona jurídica sólo puede ser sancionada

administrativamente, asimismo, reduciría sustancialmente la pérdida de la imagen corporativa, cuyo valor intangible es demasiado importante para una entidad corporativa.

Para cumplir con este objetivo, se debe incorporar un auditor interno, en este caso la nominación de un delegado de protección de datos, cuyas funciones son: (i) Elaborar un programa de cumplimiento normativo identificado, analizando y valorando los riesgos que se puedan dar (mapa de riesgos); (ii) Facilitar al personal el acceso al programa de cumplimiento; (iii) Supervisar el cumplimiento de las disposiciones del programa de cumplimiento, códigos de conducta, entre otros; (iv) e Informar al Órgano de Control, las ilicitudes en el tratamiento.

- **Beneficios:** una vez identificada las principales zonas de riesgo, el It Compliance ayudará al cumplimiento de los estándares técnicos, organizativos y legales del tratamiento de los datos personales, también contribuirá a la organización de los directivos frente a los trabajadores, impulsando el principio de confianza, muy practicada en las empresas. Por último, está demostrado que una gran parte de incidencias se produce por la actividad irresponsable de los empleados, en gran medida por desconocimiento de prácticas adecuadas en el manejo de los datos personales, por ello, resulta de vital importancia dedicar recursos a su formación y concienciación.
- **Consultoría:** Integración de estrategias de responsabilidad social, para ello, se hará difusión de códigos éticos, códigos de buena conducta, gestión del Buen Gobierno Corporativo, elementos que ayuden a difundir la cultura de la organización bajo supervisión. Estas gestiones se realizarán en torno al tratamiento de datos.

2.2.3. IMPLEMENTACIÓN DE LOS PROGRAMAS DE CUMPLIMIENTO EN EL PERÚ

El programa de cumplimiento normativo es el documento interno que las empresas implementan para cumplir con la normativa vigente, así como para prevenir y detectar las infracciones legales que puedan producirse dentro de las mismas o como parte de las actividades que éstas realizan.

El programa se concentra en protocolos de actuación diseñados a fin y efecto de mitigar o expulsar las conductas delictivas por parte de los trabajadores de la empresa. Gómez, citado por Reyna (2018).

La idea es que las empresas internalicen o implementen un conjunto de normas o medidas que traten de asegurar la prevención de infracciones que se podrían generar como consecuencia de las actividades que realizan o debido al nivel de complejidad de su estructura organizacional (Reyna, 2018:19-20).

Pues bien, de acuerdo con Castells, citado por Astudillo (2016), la crisis económico financiera comprendida en el período 2007 a 2015 ha traído repercusiones respecto a la manera en que los juristas y economistas entendían la protección de los mercados financieros y el sistema económico mundial. En efecto, el hundimiento de los mercados bursátiles y la investigación penal de corporaciones importantes parecen haber puesto en evidencia las debilidades del sistema, abriendo el debate en el campo de las ideas sobre la conveniencia de incrementar la supervisión legal del modelo económico adoptado por los Estados occidentales, cuya regulación ha sido insuficiente para evitar las malas prácticas corporativas de muchas empresas.

Para combatir este fenómeno diversos organismos internacionales han venido recomendando al sector empresarial adoptar una serie de medidas con el objetivo de mejorar

la gestión de las empresas. Entre los conceptos más usados para referirse a estas medidas se encuentran nombres como "risk manegement", "programas de cumplimiento", "compliance", "códigos de ética", "normas de buen gobierno corporativo", "código de buena conducta", "programa de prevención de delitos".

Aunque muchos de estos conceptos surgieron a fines de los años noventa vinculados al concepto de responsabilidad social corporativa, todos ellos describen una serie de medidas orientadas a lograr una gestión empresarial que evite la comisión de ilícitos y promueva valores éticos en la empresa (Bacigalupo, 2012).

De esta manera, las personas jurídicas deben asumir la función de prevención de ilícitos mediante la adopción de medidas de **"autorregulación regulada"** que se conocen comúnmente como programas de cumplimiento. Estos persiguen fomentar y concretar una cultura empresarial de "cumplimiento de la legalidad" el interior de la organización.

Para hacer más efectivo el cumplimiento, en algunos ámbitos regulados, los Estados han recurrido el derecho penal siguiendo las recomendaciones de organismos internacionales para incorporar en su derecho interno la responsabilidad penal de las personas jurídicas, fundamentada en el modelo por **"defecto de organización".**

El modelo de atribución por defecto de organización, tiene en cuenta la propia "conducta" de la persona jurídica, analizándose su estructura, organización y su incidencia en la comisión del entuerto penal (Reyna, 2018:13-14). Es decir, en este esquema, la culpabilidad de la persona jurídica queda configurada si los hechos ilícitos de las personas físicas (hechos de conexión) se consideran delitos de la persona jurídica porque ésta a través de sus órganos o representantes ha omitido tomar las medidas de seguridad necesarias para asegurar un funcionamiento acorde a ley; esto es organizándose defectuosamente.

Por el contrario, cuando se comprueba que la persona jurídica ha desplegado todos los controles exigibles, de modo que se haya dirigido a evitar la aparición de un hecho delictivo, aunque un empleado o directivo lo realice, puede decirse "que no es cosa suya" y de este modo no ser sancionada (Nieto, 2015). Por cuanto, si la entidad ha implementado mecanismos de control y prevención, y pese a ello, un directivo o trabajador ha realizado un hecho ilícito, la empresa está exenta de responsabilidad.

Dicho de esta manera, la trascendencia que tienen actualmente los programas de cumplimiento es muy significante. Por una parte, la responsabilidad de la persona jurídica se fundamenta en que esta no ha tomado todas las medidas de precaución y seguridad jurídicamente exigibles para evitar o prevenir la comisión de ilícitos. Mientras que, por otro, los programas de cumplimiento suponen que su implementación efectiva en la empresa si está en condiciones de evitar la comisión de ilícitos a través de las medidas de prevención y del cumplimiento estricto de sus códigos de ética o cualquier otro mecanismo de control y supervisión.

En consecuencia, la no adopción de un programa de cumplimiento eficiente viene a justificar la sanción impuesta a la persona jurídica. Al punto de establecerse en diversos ordenamientos como una causa de exoneración de responsabilidad penal si la persona jurídica ha implementado un programa de cumplimiento antes de que se hubiere cometido el hecho criminal.

El legislador será incluso quien establezca que un programa de cumplimiento se aplique como una circunstancia atenuante. Lo resultante que dicho programa adquiere relevancia, pues se convierte en el único argumento de defensa que deberá probar la empresa para exonerar o mitigar su responsabilidad, en el caso de que exista evidencia de que uno de

sus representantes o empleados cometió o participó en un hecho criminal en su favor o beneficio.

Nuestro país no es ajeno a esta tendencia. En enero de 2015, la Comisión de Justicia y de Derecho Humanos del Congreso de la República aprobó el pre dictamen del proyecto de ley del nuevo Código Penal, en cuyo texto el legislador propuso la responsabilidad de las personas jurídicas en el caso de que la empresa incurra en el delito de cohecho activo internacional (Art. 130 y Art. 584).

Sin embargo, después de largos debates en el Congreso de la República, el 17 de marzo de 2016, el pleno del congreso aprobó el proyecto de ley 4054-2014/PE, introduciendo un texto sustitutorio denominado ahora **"ley que regula la responsabilidad administrativa de las personas jurídicas por el delito de cohecho transnacional".** Si bien este proyecto recoge la idea inicial de hacer responsable a la empresa en aquellos casos en los que se detecte que uno de sus representantes se encuentre incurso en un acto de corrupción, lo cierto es que la esencia y justificación de una verdadera responsabilidad penal autónoma de la persona jurídica ha sido reemplazada por un sistema de **"responsabilidad administrativa"** que constituye un retroceso con relación al proyecto primigenio que presentó el Poder Ejecutivo.

2.2.3.1. CUESTIONES A INCORPORAR EN UN PROGRAMA DE CUMPLIMIENTO EMPRESARIAL

En nuestra legislación específicamente no se han contemplado las características que deberían tener los programas de cumplimiento. Dado que ello podría generar inseguridad jurídica, resulta recomendable que el legislador establezca los elementos esenciales que deberían tener los mismos, pues a partir de dichas condiciones la empresa podrá autorregularse con ayuda especializada y adoptar el programa más adecuado y compatible con sus actividades.

Al respecto, **es necesario señalar que el fenómeno de la autorregulación de las empresas no es nuevo, pues ya existen normas en el ámbito de la prevención de riesgos laborales (**El artículo 1 de la ley 29738 "Ley de seguridad y salud en el trabajo", prevé el sistema de prevención de riesgos laborales, tiene por objeto "promover una cultura de prevención de riesgos laborales en el país. Para ello, cuenta con el deber de prevención de los empleados, el rol de fiscalización y control del Estado y la participación de los trabajadores y sus organizaciones sindicales, quienes, a través del diálogo social, velan por la promoción, difusión y cumplimiento de la normativa sobre la materia), **de prevención de lavado de activos y en la protección de datos personales**. De acuerdo con esta normativa, se exige a las empresas que implementen ciertas medidas y capaciten a sus empleados en todo aquello que tenga que ver con el cumplimiento de dicha normativa. Lo que se pretende es aprovechar la mayor proximidad que tiene la empresa con sus órganos y empleados para capacitarlos y evitar conductas ilícitas.

De acuerdo a Jara citado por Astudillo (2016:250), considera que un programa de cumplimiento común debería contener los siguientes elementos:

- Código de conducta escrito. (contemplado en la ley 29733 "Ley de Protección de Datos Personales").
- Supervisión de esfuerzos de cumplimiento por personal cualificado. (a cargo del Delegado de Protección de Datos).
- Reforzamiento mediante sistemas efectivos de control y auditoria (medidas técnicas y organizativas).
- Reforzamiento mediante procedimientos disciplinarios.
- Adopción de medidas cautelares tras detección de una infracción.
- Seguimiento de una formación continuada a directivos y empleados. (supervisión)

- Comunicación efectiva de los estándares y procedimientos de los códigos de conducta. (comunicación directa al Registro Nacional de Protección de Datos Personales).

En el caso peruano, el proyecto de ley 4054-2014 prevé, en el artículo 17, que "la persona jurídica está exenta de responsabilidad administrativa por la comisión de delito de cohecho activo transnacional, si adopta e implementa en su organización. Con anterioridad a la comisión del delito, un modelo de prevención adecuado a su naturaleza, riesgos, necesidades y características, consistente en medidas de vigilancia y control idóneas para prevenir el delito de cohecho activo trasnacional o para reducir significativamente el riesgo de su comisión". Si bien la responsabilidad de la persona jurídica solo se ha previsto para dicho ilícito, el legislador de reforma ha previsto los elementos mínimos de lo que denomina **"modelo de prevención".**

a. Una persona u órgano, designado por el máximo órgano de administración de la persona jurídica, que ejerza la función de Auditoría Interna de Prevención y que cuente con el personal, medios y facultades necesarios para cumplirla adecuadamente. Esta función se ejerce con la debida autonomía respecto del órgano de administración, sus propietarios, accionistas o socios, salvo en el caso de la micro, pequeña y mediana empresa, donde puede ser asumida directamente por el órgano de administración.

b. Medidas preventivas referidas a:

- La **identificación** de las actividades o procesos de la persona jurídica que generen o incrementes **riesgos** de comisión del delito de cohecho activo transnacional.
- El establecimiento de procesos específicos que permitan a las personas que intervengan en éstos, programar y ejecutar sus tareas o labores de una manera que prevenga la comisión del delito de cohecho activo transnacional.

- La **identificación de los procesos de administración y auditoría** de los recursos financieros que permitan a la persona jurídica prevenir su utilización en la comisión de la conducta delictiva de cohecho activos transnacional; y,
- La existencia de **sistema de denuncia,** protección de denunciante, persecución e imposición de sanciones internas en contra de los trabajadores o directivos que incumplan el modelo de prevención.
- **Un mecanismo de difusión y supervisión** interna del modelo de prevención, el cual debe ser aprobada por un reglamento o similar emitido por la persona jurídica.

Es evidente que el objetivo del legislador peruano apunta a que las empresas peruanas implementen un sistema de gestión del cumplimiento con el objetivo de detectar y prevenir la comisión de infracciones realizados por sus trabajadores y representantes en el ámbito de su actividad y en beneficio de las personas jurídicas.

La existencia y aplicación práctica y efectiva de un programa de cumplimiento, de una empresa, va a determinar importantes consecuencias ante una eventual comisión de un delito y la apertura de un proceso penal. En principio, la implantación de un programa se constituye en un potente indicio de descargo, en el sentido que la empresa cumplió con sus deberes de control y de que, por ello, el eventual delito cometido en su nombre y beneficio no es atribuible a un "defecto de organización". Por tanto, debe ser atenuada su responsabilidad penal o eximida completamente Nieto citado por (Astudillo, 2016).

Si bien el proyecto de ley 4054-2014-PE, establece algunos parámetros que se pueden encontrar en la doctrina y en algunas normas internacionales sobre normalización, es evidente que no se han considerado todos estos elementos que permitan que el cumplimiento o Compliance se estandarice. Por ejemplo, el proyecto no indica ni señala cuáles serían los requisitos para asumir la función de responsable de auditoría interna de prevención de la

empresa (Compliance Officer). En principio, tanto la doctrina como las normas sobre cumplimiento hacen hincapié en la formación técnica que debe tener el oficial de cumplimiento de la empresa; sin embargo, esto no se refleja en el proyecto.

Si lo que se pretende es hacer eficiente un sistema de gestión de cumplimiento, resulta necesario establecer el contenido de un estándar común tal como ya prevén en normas internacionales. En ese sentido, en diciembre de 2014, la Organización Internacional de Normalización (ISO) publicó la Norma ISO 19600 sobre Compliance Management System (CMS) o "Sistemas de gestión de Compliance", que recoge recomendaciones y buenas prácticas para ayudar a las organizaciones a desarrollar un sistema de gestión que les permita identificar, controlar y cumplir con los requisitos legales que le aplican.

De esa manera, esta norma se ha convertido en el exponente más actual de normas dedicadas exclusivamente a la gestión de cumplimiento, dejando atrás otras normas que se utilizaban como referencia para gestionar este tipo de programas.

Para efectos de la presente investigación, conviene precisar que, para gestionar un programa de cumplimiento en el tratamiento de datos personales, en la **Directiva de Protección de Datos de la legislación peruana, se establece como criterio de seguridad el condicionamiento de las medidas de seguridad según los requisitos establecidos en el NTP-ISO/IEC 27001 o ISO/IEC 27001.**

Esta norma peruana ha sido condicionada para proporcionar los requisitos para establecer, implementar, mantener y mejorar un sistema de gestión de seguridad de la información, ya que el sistema de gestión de la seguridad de información preserva la confidencialidad, integridad y disponibilidad de la información aplicando un proceso de gestión de riesgos, sin embargo, esta disposición tiene carácter voluntario, es decir no exige que las empresas lo adopten.

2.2.4. EMPRESAS PÚBLICAS DEL SECTOR ENERGÉTICO

La LPDP, en su artículo 3 prescribe que los bancos de datos de las entidades de administración pública o privada están obligadas a implementar las disposiciones legales en su tratamiento de datos, por lo que, las empresas públicas del sector energético al ser entes de servicio público se encuentran obligadas a obedecer lo prescrito en la normativa sectorial.

Las empresas públicas son aquellas entidades que pertenecen total o parcialmente al gobierno de un Estado determinado y donde éste puede tener participación en la toma de decisiones de la empresa. El objetivo de ellas como cualquier otra empresa es obtener ganancias monetarias pero por sobre todo eso, el objetivo primordial es satisfacer las necesidades de la población a través de los servicios que ofrece (electricidad, agua, telefonía, entre otros).

Las empresas públicas son creadas para la realización de diversas actividades, estas son financiadas principalmente por el Estado y por las ganancias que las mismas obtienen de la explotación de algún servicio o producto. Los resultados obtenidos por éstas no se van a medir por el monto de dinero ganado, sino por la calidad del servicio que se está prestando.

Este tipo de empresas se encuentran bajos las leyes de función pública por lo tanto los empleados de dichas empresas se deben regir por lo dispuesto en la normativa vigente. Éstas son sometidas a controles fiscales realizados por los organismos competentes (auditorías, Contraloría, SBS, etc) creados para este fin, estos verifican que el dinero proveniente de los fondos públicos vaya destinado a los requerimientos más urgentes de la población, es decir que las contralorías velan por el buen desempeño de las empresas públicas.

El principal objetivo de la empresa pública es buscar el bien común de la colectividad en general es por ello que los costos de producción pasan a un segundo plano si el servicio a ofrecer es de alta calidad, a diferencia de la empresa privada cuyo objetivo primordial es el crecimiento de las ganancias y expansión en los diferentes mercados de la economía.

En ese sentido, se podría afirmar que una empresa pública del sector energético es aquella entidad financiada por el estado, constituida con el fin de realizar actividades destinadas a la producción, transportación, innovación, manejo y comercialización de energía eléctrica.

En relación a ello, es necesario precisar que este tipo de empresas se encuentran bajo el ámbito del Fondo Nacional de Financiamiento de la Actividad Empresarial del Estado – FONAFE, la cual es una empresa de Derecho Público adscrita al Sector Economía y Finanzas creada por la Ley No. 27170, que fue promulgada el día 08.09.99, se publicó el día 09.09.99 y entró en vigencia el día 10.09.99, por lo que recién nace FONAFE el día 10.09.99 como la Entidad encargada de normar y dirigir la actividad empresarial del Estado. Al momento de su creación, FONAFE asumió las funciones de la desaparecida Oficina de Instituciones y Organismos del Estado –OIOE.

De acuerdo a lo dispuesto por el artículo 9º del Reglamento de la Ley No. 27170, aprobado mediante Decreto Supremo No. 072-2000-EF, modificado mediante Decreto Supremo No. 115-2004-EF, FONAFE cuenta con un Directorio conformado por seis miembros, todos ellos Ministros de Estado de los siguientes sectores:

Economía y Finanzas; Transportes y Comunicaciones; Vivienda, Construcción y Saneamiento; Energía y Minas; el Ministro a cuyo sector esté adscrito PROINVERSIÓN; y, Presidencia del Consejo de Ministros. Sin embargo, dado que PROINVERSION se encuentra adscrita al Ministerio de Economía y Finanzas, en la práctica el Directorio de FONAFE está

compuesto por cinco Ministros de Estado, quienes tienen entre sus facultades principales, las siguientes:

(I) Ejercer la titularidad de las acciones representativas del capital social de todas las empresas (creadas o por crearse) en las que participa el Estado y administrar los recursos provenientes de dicha titularidad.

(II) Aprobar el presupuesto consolidado de las empresas en las que FONAFE tiene participación mayoritaria, en el marco de las normas presupuestales correspondientes.

(III) Aprobar las normas de gestión en dichas empresas.

(IV) Designar a los representantes ante la Junta General de Accionistas de las empresas en las que tiene participación mayoritaria.

Bajo el ámbito de FONAFE se encuentran únicamente las empresas que cuentan con participación mayoritaria del Estado.

2.2.5. DERECHO COMPARADO

El Derecho Comparado, es un aspecto importante en la investigación jurídica, porque constituye una ciencia cuyo objeto es el estudio de las semejanzas y diferencias entre los ordenamientos jurídicos de dos o más países. Una disciplina auxiliar muy efectiva en la construcción de cualquier Derecho nacional positivo, configurándose como una ciencia jurídica autónoma, con un contenido propio y un método ajustado al objeto perseguido.

De acuerdo con García, citado por Aranzamendi (2015:125), “el Derecho Comparado consiste en el estudio comparativo de instituciones o sistemas pertenecientes a diversos lugares o épocas, con el fin de determinar las notas comunes y las diferencias que entre ellos

existen, y derivar de tal examen, conclusiones sobre la evolución de tales instituciones o sistemas y criterios para su perfeccionamiento o reforma".

2.2.5.1. IMPORTANCIA DEL DERECHO COMPARADO

Desde otro aspecto, el Derecho comparado permite la construcción del Derecho nacional desde las experiencias del Derecho de otros países, como sucede en el nuestro de origen básicamente romano-germánico o la introducción del Common Law, respecto al nuevo modelo del Derecho Procesal Penal. Facilita también conocer esta disciplina con mayor amplitud que dé común poseen los distintos ordenamientos jurídicos positivos mediante la confrontación de los mismos.

Para el jurista investigador, la importancia del estudio del Derecho comparado es ineludible, pues, muchas veces es preciso estudiar el Derecho de todos los tiempos y pueblos de la Tierra, si se quiere tener una idea holística del derecho, admitiendo que cada derecho nacional no es sino una parte de toda la cultura creada por la humanidad (Aranzamendi, 2015:126).

2.3. MARCO TEÓRICO CONCEPTUAL

2.3.1. AUTORREGULACIÓN REGULADA

Es el mecanismo a través del cual los sujetos que forman parte de la sociedad se organizan y regulan, teniendo como objeto el establecimiento de normas de conducta o políticas que aplican a la actividad que realizan. Este fenómeno involucra la creación de organizaciones, procedimientos, mecanismos y fórmulas diversas que tienen por objeto el autocontrol y autodominio de unos medios que, por razones diversas no pueden ser dominados por el Estado. Esteve, citado por Carmona (2015).

2.3.2. COMPLIANCE

El término compliance significa "cumplimiento", "observancia", "conformidad con determinados mandatos", y hace alusión en este contexto a procedimientos para la "transposición de prescripciones legales" con la pretensión de evitar la criminalidad empresarial. En ese sentido, puede decirse que la finalidad de los programas es aplicar normas jurídicas u otras directivas dirigidas para la empresa y, a través de ello, evitar la reclamación de responsabilidad y otros perjuicios para la empresa, sus órganos y empleados (Kuhlen, 2013).

2.3.3. COMPLIANCE OFFICER

El oficial de cumplimiento es quien tiene a su cargo el control del cumplimiento del programa respectivo (prevención) y la denuncia de las irregularidades que se cometan en la empresa (represión). Puede tener acotado su responsabilidad a determinados sectores, como el de las contravenciones y delitos (Criminal Compliance Officer). Puede tratarse también de un departamento del cumplimiento integrado por varias personas bajo la dirección de un chief compliance officer (Reyna, 2018:25-26).

2.3.4. DISEÑO POR DEFECTO DE ORGANIZACIÓN

Estando de acuerdo con González (2012), "El defecto de organización es la creación de una actitud criminal del grupo o la omisión de medidas de cuidado para evitar, en la medida de lo posible, de que las personas físicas que trabajan para la persona jurídica, cometan delitos en nombre, por cuenta y en provecho de ella".

2.3.5. GOBIERNO CORPORATIVO

El gobierno corporativo se define como las normas y herramientas por las cuales se rige una empresa, hoy en día tener un buen gobierno corporativo, acorde a las características

inherentes de la empresa es vital para el buen desarrollo de la misma, es decir que las empresas que poseen buen gobierno corporativo son más confiables y atraen mayor inversión, que las empresas que no lo poseen (Indacochea, 2000).

2.3.6. IT COMPLIANCE, PRIVACIDAD Y PROTECCIÓN DE DATOS

Se entiende por It Compliance, Privacidad y Protección de Datos al conjunto de acciones que las organizaciones tiene que desarrollar para cumplir con las obligaciones legales o contractuales obligatorias o aquellas que libremente hayan asumido con los requisitos de seguridad derivados de las mismas, en los procesos corporativos de gestión de información (Cumbreras, 2016).

III. MATERIALES Y MÉTODOS

3.1. TIPO DE INVESTIGACIÓN

El presente estudio por su orientación es una investigación **JURÍDICA - DOGMÁTICA**, la cual concibe el problema jurídico desde una perspectiva estrictamente formalista, caracterizado por el análisis crítico de las leyes, doctrinas o modelos teóricos de procedimientos jurídicos. Para la Tesis planteada radica el desarrollo de un análisis cualitativo y sistemático de normas y doctrina que permite describir el It Compliance, Privacidad y Protección de Datos para empresas públicas en el Perú.

3.2. DISEÑO DE LA INVESTIGACIÓN

La presente investigación tiene un enfoque **CUALITATIVO**, porque versa sobre un problema específico y exclusivamente relacionados a una **investigación DOGMÁTICO – JURÍDICA**, la misma que concluirá con la obtención de resultados a los cuales no es posible llegar a un sondeo estadístico u otro tipo de cuantificación, porque para el desarrollo de la investigación se requerirá una actividad sistemática, orientada a la comprensión en profundidad de los temas tratados.

3.3. ÁMBITO Y OBJETO DE INVESTIGACIÓN

El ámbito de investigación se circunscribe a las normas de carácter nacional e internacional, a través de las cuales se comprende el It Compliance, Privacidad de Protección Datos, así como los dispositivos legales que sirven para la base de su implementación y que se encuentren vinculadas con el objeto de investigación.

El objeto de investigación se encuentra delimitado en describir la normativa del It Compliance de privacidad y protección de datos convenidos en la legislación nacional y extranjera, comprendiendo a este último, la Unión Europea, España, Argentina y Uruguay.

3.4. MÉTODOS, TÉCNICAS E INSTRUMENTOS DE INVESTIGACIÓN

3.4.1. MÉTODOS TÉCNICAS E INSTRUMENTOS UTILIZADOS PARA LA RECOLECCIÓN DE DATOS

a Método de Observación. Es el procedimiento de percepción atenta, racional, planificada y sistemática de los fenómenos relacionados con el problema objeto de la investigación, a fin de poder describir y obtener los resultados, recurriéndose a la técnica de "Análisis de Contenido", consistente en la investigación de teorías, doctrinas, leyes y jurisprudencia, en función de los objetivos de investigación.

Instrumento Utilizado: Ficha de observación.

b. Método comparativo. Se somete a estudio las instituciones jurídicas que pertenecen al mismo género, pero que difieren en especie. En estos casos, se trata de identificar las similitudes o diferencias normativas y teóricas de dos o más sistemas en ámbito del Derecho nacional o internacional (Aranzamendi, 2015:79). La técnica a usarse es la observación documental, siendo aquella en la que el objeto de la observación está constituido por los documentos.

Instrumento Utilizado: Ficha de registro.

Se usará este método respecto al segundo objetivo específico a fin de analizar e identificar las diferencias existentes en cuanto al tratamiento legislativo del It Compliance, Privacidad y Protección de datos con la Unión Europea, España, Argentina y Uruguay, con nuestro ordenamiento jurídico.

c. Método propositivo. La singularidad de esta tipología es indagar la falta o deficiencia de un enfoque teórico para resolver un problema jurídico. En otros casos, evidencia el vacío o lagunas de una o varias normas jurídicas o se cuestiona las existentes.

3.4.2. MÉTODOS UTILIZADOS PARA EL ESTUDIO DE LA INFORMACIÓN OBTENIDA

a. Método Deductivo. Con el cual los planteamientos generales se aplican al caso particular, esto es, investigar las disposiciones legales vigentes a fin que las empresas públicas viabilicen la implementación del It Compliance, privacidad y protección de datos a través de la introducción de un sistema de responsabilidad de las personas jurídicas en el Perú.

b. Método Analítico. Es el procedimiento por el cual se examinará los conceptos pertinentes y los elementos esenciales que debe contener el It Compliance de Privacidad y Protección de Datos para asegurar su funcionamiento eficaz en un sistema de responsabilidad de las empresas públicas del Perú.

3.5. UNIDAD DE ESTUDIO. - Tratándose de un estudio cualitativo comparativo, la unidad de estudio está comprendida por el IT Compliance, Privacidad y Protección de datos y el tratamiento legal que este recibe en la Unión Europea, España, Argentina y Uruguay.

3.6. PROCEDIMIENTO DE INVESTIGACIÓN

En las investigaciones de carácter cualitativo, el análisis y recolección de datos concurren prácticamente en forma concatenada, asimismo, el análisis no es uniforme, ya que cada estudio requiere de un esquema propio de análisis, por tratarse de estudios teóricos, sin embargo se desarrolló un proceso de análisis e interpretación de datos a efectos de estructurar el proceso de investigación, sirviendo de directriz para un fácil entendimiento del proceso de investigación, los mismos que se realizaron de la siguiente forma:

a. Estructuración de datos. Para la estructuración de los datos, se organizó las unidades, ejes, sub ejes, sus categorías y los patrones, a efecto de contar con una debida estructuración que sirviera de guía a fin de realizar los subsecuentes pasos de la investigación.

b. Orientación. En esta parte del proceso se orientó a encontrar el sentido a los datos recolectados en el marco del planteamiento del problema, contrastándose sistemáticamente y objetivamente los parámetros planteados al inicio de la investigación.

c. Búsqueda de la relación de resultados. Finalmente se efectuó la relación de los resultados con los objetivos propuestos.

IV. RESULTADOS Y DISCUSIÓN

RESPECTO AL OBJETIVO ESPECÍFICO N° 01

4.1. DEL ESTADO ACTUAL DEL IT COMPLIANCE, PRIVACIDAD Y PROTECCIÓN DE DATOS EN EL PERÚ

El Cumplimiento IT se relaciona con aquellas medidas vinculadas a la protección de los datos y dispositivos que lo almacenan, ya sean sistematizados o no, también abarcan políticas de accesos a datos confidenciales y sistemas de alerta frente a posibles infracciones legales, sin duda el It Compliance, Privacidad y Protección de Datos constituye en actualidad una de los mejores sistemas para evitar que la actividad empresarial conlleve la realización de infracciones en el tratamiento de la información.

Ello se debe a que las entidades corporativas se encuentran en mejor posición que el Estado para controlar y supervisar que el comportamiento del titular del banco de datos y responsable del tratamiento se ajuste a la normativa sectorial de la protección de datos. En nuestro ordenamiento jurídico, específicamente en el inciso 6° del artículo 2° de la Constitución Política del Perú, se reconoce al instituto de protección de datos como el derecho fundamental que tiene toda persona a que los servicios informáticos, computarizados o no, públicos o privados, no suministren informaciones que afecten la intimidad personal.

Sin embargo, esta regulación resultó siendo deficiente debido a que menciona como único fundamento la protección de la intimidad personal o familiar, omitiendo otros derechos tales como el resguardo, control y manejo de información personal o tratamiento de datos sensibles.

Por ello, al apreciar estas deficiencias en el texto constitucional, se introdujo en el Código Procesal Constitucional, alcances del proceso de hábeas data, cuyo desarrollo tuvo

mayor precisión del contenido del derecho a la protección de los datos personales como una forma de suplir muchas de las carencias u omisiones antes señaladas.

Así, en el artículo 61, numeral 2, del Código Procesal Constitucional se establece: Artículo 61.- "El hábeas data procede en defensa de los derechos constitucionales reconocidos por los incisos 5) y 6) del Artículo 2 de la Constitución. En consecuencia, toda persona puede acudir a dicho proceso para: […]. Eguiguren (2015).

En respuesta a la problemática social por parte de las instituciones sobre el manejo, transferencias y control de los datos personales, y siendo necesaria establecer garantías que tutelen la vida privada de las personas frente a la agresión informática, el Congreso de la República aprobó, el 07 de junio de 2010, el Proyecto de Ley N° 4079/2009-PE que propuso la implementación de la "Ley de Protección de Datos Personales", con la finalidad de dar cumplimiento a los compromisos adquiridos por el Estado para homologar la legislación interna sobre la protección de datos personales dispuesta en los Tratados internacionales en los cuales Perú es parte.

Es así que, el 03 de julio de 2011 se promulgó la Ley 29733 del "Ley de Protección de Datos Personales" (en adelante, LPDP) y modificada por el Decreto Legislativo 1353" del 06 de enero de 2017, siendo reglamentada desde el 22 de marzo de 2013, mediante el DS 003-2013-JUS, (en adelante, el Reglamento); y 11 de octubre de 2013 la Autoridad Nacional de Protección de Datos Personales mediante la Resolución Directoral N° 060-2014-JUS/DGPDP, publicó la "Directiva sobre Protección de Datos Personales y Programas Sociales" (en adelante, la Directiva), con la finalidad de orientar las medidas técnicas, organizativas y legales del tratamiento de protección de datos, **cuyo cumplimiento es voluntario.**

Realizando un análisis a La LPDP y su Reglamento, se puede deducir que tienen como objeto garantizar el derecho fundamental a la protección de datos previstos en la Constitución, ello a través de un adecuado tratamiento, estos son de aplicación a los datos personales contenidos en los bancos de datos personales ya sea de administración pública y de administración privada. Asimismo, estas normas han establecido obligaciones para los titulares y encargados del tratamiento de datos personales, cuya actuación debe ajustarse al contenido de la normativa ya descrita y a los principios rectores que guían todo tratamiento de la información personal.

Para finalizar, el titular de los bancos de datos personales y el encargado del tratamiento está obligado a implementar medidas de seguridad adecuadas que les permitan un tratamiento seguro de los datos que suministran, preservando su confidencialidad, disponibilidad e integridad de aquellos, de acuerdo al marco normativo procedo a describir los principios y obligaciones relativos a la seguridad en el tratamiento de datos personales realizados en el territorio nacional, siendo los siguientes:

4.1.1. PRINCIPIOS Y OBLIGACIONES EN GENERAL

4.1.1.1. PRINCIPIOS EN EL TRATAMIENTO DE DATOS

Dentro de los principios rectores consignados en la LPDP, tenemos al **Principio de Finalidad,** el cual establece que los datos personales deben ser recopilados para una finalidad lícita, es decir que no sean desviados maliciosamente de la finalidad establecida al momento de su recopilación.

El siguiente principio es el que marca un hito importante en el tratamiento de los datos personales, ya que impulsa a las entidades públicas o privadas a la implementación de programas de cumplimiento a fin de evitar futuras sanciones, pues bien tenemos al **Principio**

de Seguridad, prescrito en el artículo 9 de la LPDP, **el cual consiste en que el titular del banco de datos personales y el encargado de su tratamiento adopten medidas técnicas, organizativas y legales para garantizar la seguridad de los datos personales**. En ese sentido las medidas de seguridad deben ser apropiadas y acordes con el tratamiento que se vaya a efectuar y con la categoría de datos personales de que se maneje.

Asimismo, el artículo 10 del Reglamento recoge el principio ya referido, el cual exige al titular y encargado del tratamiento de los datos personales, la adopción de medidas de seguridad que resulten necesarias a fin de evitar cualquier tratamiento contrario a la norma y evitar sanciones, incluyéndose en ellos la adulteración, la pérdida, las desviaciones de información, intencionales o no, ya sea que los riesgos provengan de la acción humana o del medio técnico utilizado.

También, la LPDP prevé en su artículo 11 al **Principio de nivel de protección adecuado**, el cual consiste en garantizar un nivel suficiente de protección de los datos personales para el flujo transfronterizo equiparable a los estándares internacionales, es decir que el país receptor de los datos debe mantener niveles adecuados de protección o que el emisor del flujo transfronterizo de datos personales garantice que el tratamiento de los datos personales en el país destinatario se efectúe acorde a lo dispuesto por la LPDP y su Reglamento.

En cuanto a las transferencias dentro de un sector o grupo empresarial, dice el artículo 21 del reglamento que, la implementación de un código de conducta garantiza el tratamiento de datos personales por lo que es apto para el flujo de datos.

Por último, de acuerdo a la tercera disposición complementaria del Decreto Legislativo 1353 “Decreto Legislativo que crea la Autoridad Nacional de Transparencia y Acceso a la Información Pública, Fortalece el Régimen de Protección de Datos Personales y

la Regulación de la Gestión de Intereses", se ha modificado diversos artículos y se ha incluido nuevas figuras legales, tal es el caso del encargado del tratamiento de datos personales, antes de su modificación se le consideraba como encargado del banco de datos personales, cuya diferencia resalta en la relación jurídica, obligaciones y ámbito de actuación. No obstante, tanto la actuación del titular y encargado del tratamiento de datos personales está sujeta al cumplimiento fiel de los principios ya mencionados, ello lo vemos en el artículo 12 de la LPDP.

Para ejemplificar, en el artículo 32 del Reglamento se establece que, los operadores de comunicaciones o telecomunicaciones, deberán velar por la confidencialidad, seguridad y uso adecuado de cualquier dato personal obtenido como consecuencia de su actividad, y adoptarán las medidas técnicas, legales y organizativas, conforme a lo establecido en la LPDP, sin perjuicio de las medidas establecidas en las normas del sector de comunicaciones y telecomunicaciones que no se opongan a lo establecido por ambas normas.

De lo descrito, podemos constatar que implícitamente el principio de seguridad y el principio de nivel adecuado de protección, rige en la obligación legal que tienen los titulares de bancos de datos personales, ya sean personas naturales, instituciones públicas o privadas a implementar medidas destinadas al tratamiento y protección de los datos personales.

4.1.1.2. OBLIGACIONES EN EL TRATAMIENTO DE DATOS

DEL TITULAR DEL BANCO DE DATOS Y RESPONSABLE DEL TRATAMIENTO

El artículo 16 de la LPDP establece que, para la seguridad del tratamiento de datos personales, el titular del banco de datos personales debe adoptar medidas técnicas, organizativas y legales que garanticen su seguridad y eviten su alteración, pérdida, tratamiento o acceso no autorizado y, los requisitos y condiciones que deberán reunir los bancos de datos personales en materia de seguridad son establecidos por la Autoridad

Nacional de Protección de Datos Personales, dice la LPDP que el tratamiento de datos personales que no reúna las condiciones de seguridad antes descritos quedarán prohibidos.

Otras obligaciones del titular del banco de datos y encargado del tratamiento de protección de datos personales, es proporcionar a la Autoridad Nacional de Protección de Datos Personales, la información relativa al tratamiento de datos personales que esta le requiera y permitirle el acceso a los bancos de datos personales que administra, otra exigencia de la LPDP y Reglamento es la prohibición a recopilar datos por medios fraudulentos, desleales o ilícitos. Accesoriamente el artículo 14 del Reglamento incluye la figura del responsable del tratamiento, siendo aquél que decide sobre el tratamiento de los datos personales y en la Directiva se incluye a un responsable de seguridad, siendo definido como una persona que coordina y controla la implementación de las medidas de seguridad en un banco de datos personales.

Además, las entidades representadas por el titular o encargado del tratamiento de datos personales podrán elaborar códigos de conducta que establezcan normas para el tratamiento de datos personales que tiendan a asegurar o mejorar las condiciones de operación de los sistemas de información en función a los principios rectores ya referidos.

Es decir, la LPDP impone exigencias al titular y encargado del tratamiento de datos personales vinculadas al cumplimiento del registro, almacenamiento y reporte de la información contenida en los bancos de datos a la Autoridad Nacional de Protección de Datos Personales y otorga facultades para que redacten voluntariamente un código de conducta, el mismo que contendrá los valores y estándares éticos de la empresa, todo esto acorde a lo establecido en la LPDP y Reglamento.

DE LA AUTORIDAD NACIONAL DE PROTECCIÓN DE DATOS PERSONALES

La Autoridad Nacional de Protección de Datos Personales, (en adelante, la ANPDP) nace con la dación de la LPDP, la cual establece los términos en que se garantiza el derecho fundamental a la protección de los datos personales a través de un adecuado tratamiento. La Autoridad debe cumplir y hacer cumplir la normatividad en materia de protección de datos personales, tiene **funciones administrativas, orientadoras, normativas, resolutivas, fiscalizadoras y sancionadoras.**

Concerniente a la presente investigación me enfocaré en las **funciones normativas**, las cuales son: **(i)** emitir opinión técnica respecto de los proyectos de normas que se refieran total o parcialmente a los datos personales, **(ii)** emitir las directivas que correspondan para la mejor aplicación de lo previsto en la LPDP y en su reglamento, así como supervisar su cumplimiento y **(iii) promover el uso de mecanismos de autorregulación como instrumento complementario de protección de datos personales.** Es decir que el Estado promueve la implementación de mecanismos que aseguren la seguridad de los datos, los mismos que deben ser adoptados supletoriamente al tratamiento.

En efecto, dentro de sus **funciones fiscalizadoras** encontramos las siguientes: **(i)** supervisar el cumplimiento de las exigencias previstas en la LPDP, **(ii) supervisar** la sujeción del tratamiento de los datos personales que efectúen el titular y el encargado del tratamiento de datos personales a las disposiciones técnicas que se emita y, en caso de contravención iniciar procedimientos administrativos sancionadores, **(iii)** iniciar fiscalizaciones de oficio o por denuncia de parte por presuntos actos contrarios a lo establecido en la LPDP y en su reglamento.

Pues bien, de acuerdo a lo detallado en los parágrafos precedentes, se puede comprender que la ANPDP es un órgano de control que ejerce diferentes funciones, tales

como la supervisión, fiscalización, orientación y sanción. Por último, la LPDP creó el Registro Nacional de Protección de Datos Personales a cargo de la Autoridad con carácter administrativo; como principales funciones de este órgano comprenden las siguientes:

(i) el registro de los bancos de datos personales de administración pública o privada, este registro no posibilita el conocimiento del contenido de los bancos de datos personales por parte de la Autoridad, salvo procedimiento administrativo en curso; **(ii)** la inscripción de los Códigos de Conducta; las sanciones, medidas cautelares o correctivas impuestas por la Dirección General de Protección de Datos Personales; y **(iii)** las comunicaciones referidas al flujo transfronterizo de datos personales.

4.1.2. DE LOS SISTEMAS DE SEGURIDAD Y PROTECCIÓN EN EL TRATAMIENTO DE DATOS

En la LPDP y su Reglamento se establece las medidas de seguridad que el titular del banco de datos y responsable del tratamiento deberán adoptar, para ello, en la Directiva se expone los criterios que tienen que ser considerados voluntariamente, tales como el volumen de registros, número de datos, periodo de tiempo para la finalidad del tratamiento de datos personales, la titularidad del banco de datos personales, finalidad del tratamiento de datos personales, multiplicidad de localizaciones y tratamiento de datos sensibles (son aquellos datos 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).

Por lo que, las entidades o personas privadas deben conocer la probabilidad de infracción de la normativa de protección de datos personales que pueda generar su actividad, y acorde a ello implementar las medidas de seguridad más eficientes. En la Directiva de Seguridad de la ANPDP, se ha categorizado el tratamiento de seguridad que se les debe dar a los bancos de datos personales, siendo los siguientes: i) básico, ii) simple, iii) intermedio,

iv) complejo y v) crítico. Entonces, según la categoría de que se trate (de menos a más), se exigirá un mayor nivel de protección y seguridad en el tratamiento de datos personales.

Por lo tanto, las disposiciones de nuestra legislación respecto a los sistemas de seguridad y tratamiento de datos personales han modificado su estrategia reguladora, dejando así la hetero regulación, de acuerdo con (Reyna, 2018), este modelo consistía en que el Estado era el único competente y exclusivo por la regulación. Es así que opta por la autorregulación regulada, mediante el cual impone a la entidad la obligación de implementar un sistema de seguridad y protección de datos personales, estableciendo que dicho sistema deberá cumplir la normativa competente caso contrario será sancionado.

4.1.3. DE LA IMPLEMENTACIÓN DE MEDIDAS DE SEGURIDAD

En materia de protección de datos personales, nuestra legislación ha establecido requisitos y medidas de seguridad que deberán cumplir de forma obligatoria los titulares de los bancos de datos personales y/o encargado de su tratamiento y los responsables del tratamiento, bajo sanción por incumplimiento, ello dependerá de la clasificación en la que se encuentren (básico, simple, intermedio, complejo y crítico) para implementar las medidas de seguridad y protección.

DE LOS REQUISITOS DE SEGURIDAD

En relación a los requisitos de seguridad de obligatorio cumplimiento, en la Directiva de la LPDP menciona los siguientes: **(i)** Determinar y dar a conocer una política de protección de datos personales; **(ii)** Mantener gobernabilidad completa de los procedimientos involucrados en el tratamiento (es decir que el titular o encargado tengan pleno conocimiento de las decisiones y procedimientos en el tratamiento de datos); **(iii)** Implementar y mantener los procedimientos documentados (publicación de los principios rectores en un lugar visible e implementar un cuaderno simple de registro); (iv) Adoptar un enfoque de riesgos (método

usado para medir la necesidad de atención en las medidas técnicas y organizativas a adoptar); **(v) Alineamiento a los requisitos según NTP-ISO/IEC 27001 o ISO/IEC 27001 (sistemas de gestión de seguridad), (con carácter voluntario)** y **(vi)** Desarrollar y mantener un documento maestro de seguridad de la información del banco de datos personales (Es aquel documento requerido por la ANPDP a las personas jurídicas que tratan dichos datos, por ejemplo, personal, contratistas, clientes a fin de demostrar que aplican las medidas de seguridad recomendadas por aquella en su Directiva de Seguridad).

Estos criterios son requisitos que las empresas deben implementar como políticas de protección, asumiendo un compromiso a adoptar los lineamientos organizacionales en la implantación de condiciones, requisitos y medidas de seguridad. En caso del ítem 1.3.1.3. De la Directiva, la implementación de las medidas de seguridad según las disposiciones específicas del numeral 2, debo describir las siguientes:

(i) Para los tratamientos determinados como complejos o críticos, se deben implementar los controles adecuados de un sistema de gestión de seguridad de la información bajo los requisitos y controles de la NTP-ISO/IEC 27001 EDI en su edición vigente, incorporando a los bancos de datos personales dentro del alcance del SGSI, asegurando como mínimo el cumplimiento de las medidas indicadas y que los riesgos asociados al banco de datos personales sean adecuadamente gestionados.

(ii) El titular del banco de datos personales debe designar un responsable de seguridad del banco de datos personales, quien coordinará en la institución la aplicación de la directiva. El rol de responsable de seguridad del banco de datos personales debe asignarse a una persona que tenga las capacidades y autoridad necesaria para el desarrollo de sus funciones. Cuando dicha designación no exista, se entiende que el rol de responsable de seguridad del banco de datos personales recae en el titular del banco de datos personales.

(iii) Las referencias a documentos o registros pueden estar en cualquier formato o tipo de medio (Hoja impresa, cuaderno, página web, afiche, registro de video, entre otros).

(iv) Limitar los bancos de datos personales a los datos estrictamente necesarios para cumplir la finalidad para la cual fueron acopiados.

(v) Evaluar la posibilidad de implementar mecanismos de anonimización o disociaciones aplicables.

Por último, en caso del ítem 1.3.1.4. Acerca de los procedimientos documentados, son de importancia los siguientes: Del numeral 1.4.2 Se debe lograr la implementación y el mantenimiento de los siguientes procedimientos documentados**: a)** Control de documentos y registros. **b)** Registros de personal con acceso autorizado**.** c) Registro de incidentes y medidas adoptadas. Del 1.4.3 se debe lograr la implementación y mantener los siguientes procedimientos documentados **a)** Control de documentos y registros. **b)** Registros de acceso. **c)** Registro de auditorías. **d)** Registro de incidentes y problemas.

DE LAS MEDIDAS DE SEGURIDAD ORGANIZATIVAS

Se exige implementar Medidas de Seguridad Organizativas relacionadas con la estructura y el personal que maneja los datos personales, dentro de las cuales está que los titulares de los bancos de datos personales adopten una serie de criterios o directivas de acuerdo con la categoría en la que se encuentren, por ejemplo, en el ítem 2.1.1. debe desarrollar una estructura organizacional con roles y responsabilidades de acuerdo con la proporcionalidad de los datos por proteger; resulta importante determinar las responsabilidades y roles organizacionales apropiados con la suficiente autoridad y recursos para liderar y hacer cumplir la política de seguridad para la protección de datos personales.

En relación a ello el titular de banco de datos deberá designar un responsable de seguridad del banco de datos personales, quien coordinará en la institución la aplicación de

la Directiva, siendo su rol de asignar una persona que tenga las capacidades y autoridad necesaria para el desarrollo de sus funciones. Cuando dicha designación no exista, se entiende que el rol de responsable de seguridad del banco de datos personales recae en el titular del banco de datos personales.

Otra medida de seguridad signada en el ítem 2.1.3. es que el titular del banco de datos lleve un **control y registro** de los operadores con acceso al banco de datos personales, con el objetivo de identificar al personal con acceso en determinado momento, sobre todo en aquellas situaciones en las que se detecta una infracción a la normativa del sector. La LPDP y su reglamento, exigen una revisión periódica de la efectividad de las medidas de seguridad adoptadas, y registrar dicha verificación en un documento adjunto al banco de datos personales; además, exigen desarrollar un procedimiento de auditoría respecto de las medidas de seguridad implementadas, teniendo como mínimo una auditoría anual.

Finalmente, en el ítem 2.1.10 de la Directiva se exige desarrollar un procedimiento de **Gestión de Incidentes** para la protección de datos personales; de esta manera se busca determinar las falencias del sistema y reaccionar ante ellas implementando las medidas correctivas necesarias.

En segundo lugar, se deberá adoptar **MEDIDAS DE SEGURIDAD JURÍDICA**, incluyen mantener los formatos de consentimiento para el tratamiento de datos personales, adecuados y de conformidad con la finalidad para la cual son acopiados; asimismo, se requiere la adecuación de los contratos del personal relacionado con el tratamiento de datos personales, así como la adecuación de los contratos con terceros.

En último lugar, se exige implementar **MEDIDAS DE SEGURIDAD TÉCNICAS**, relacionadas con los medios utilizados y con la forma de manejar y utilizar la información y los datos personales. Por ejemplo, en el Capítulo V “Medidas de Seguridad”, artículo 39 del

Reglamento se señala que los sistemas informáticos que manejen bancos de datos personales deberán incluir en su funcionamiento:

(i) El control de acceso a la información de datos personales, incluyendo la gestión de accesos desde el registro de un usuario, la gestión de los privilegios de dicho usuario, la identificación del usuario ante el sistema, entre los que se encuentran usuario-contraseña, uso de certificados digitales, toquen, entre otros, y realizar una verificación periódica de los privilegios asignados, los cuales deben estar definidos mediante un procedimiento documentado a fin de garantizar su idoneidad.

(ii) Generar y mantener registros que provean evidencia sobre las interacciones con los datos lógicos, incluyendo, para los fines de la trazabilidad, la información de cuentas de usuario con acceso al sistema, horas de inicio y cierre de sesión y acciones relevantes. Estos registros deben ser legibles, oportunos y tener un procedimiento de disposición y su destino, una vez que ya no sean útiles, su destrucción, transferencia o almacenamiento, entre otros.

(iii) Establecer las medidas de seguridad relacionadas con los accesos autorizados a los datos mediante procedimientos de identificación y autenticación que garanticen la seguridad del tratamiento de los datos personales.

Asimismo, en la Directiva se prescribe que se debe **revisar periódicamente el acceso a los datos personales** que correspondan al personal autorizado, para detectar y prevenir ingresos de personas no autorizadas, también se exige que la revisión genere un registro que evidencie su realización, es decir, que se deje constancia, el periodo de revisión dependerá de las políticas organizacionales y del tipo de datos personales que maneje el banco de datos personales, debiendo realizarse por lo menos semestralmente. En lo dicho anteriormente se requiere que el acceso sea limitado solo a los involucrados en el tratamiento de los datos personales y que estén debidamente autorizados, y, en tal sentido, se deberá proteger el banco

de datos personales contra el acceso no autorizado mediante algún mecanismo de bloqueo físico o informático.

El nivel de protección dependerá de **la categorización** del banco de datos y del medio que se utilice para su tratamiento; se podrá guardarlo físicamente en un gabinete, caja o gaveta que tenga cerradura hasta crear un sistema en el que los usuarios cuenten con un identificador único de acceso y una contraseña, que podría ser autenticada con mecanismos de alta seguridad como el toquen, dispositivos biométricos, firmas digitales, tarjetas inteligentes y tarjetas de coordenadas, entre otros, debiendo tener un registro de los accesos realizados a los datos personales para su tratamiento.

La normativa del sector requiere que el titular del banco de datos personales, o quien este designe, sea quien autorice a los usuarios a acceder al tratamiento de datos personales; dicha autorización debe ser registrada a fin de tener un control respecto del personal que tiene acceso al banco de datos, en el momento del traslado de datos personales, los datos en soporte físico deben estar contenidos en un contenedor que evite su acceso y legibilidad, los datos contenidos en soporte informático deben transportarse previa encriptación y un mecanismo de verificación de la integridad (checksum MD5, firma digital o similar).

Las **medidas de seguridad técnicas** también deberán estar dirigidas a prevenir y reaccionar frente a la pérdida, alteración o tratamiento no autorizado de los datos personales. Una medida para prevenir la pérdida de datos es realizar copias de respaldo que permitan su recuperación inmediata. La normativa exige realizar pruebas de recuperación a fin de verificar que las copias de respaldo funcionan de manera adecuada y pueden ser utilizadas en caso de ser requerido.

Desde una perspectiva más específica, se requiere que los equipos utilizados para el tratamiento de los datos personales cuenten con software de protección contra software

malicioso (virus, troyanos, spyware, etc), para proteger la integridad de los datos personales. El software de protección deberá ser actualizado frecuentemente de acuerdo con las recomendaciones y especificaciones del proveedor.

Es importante resaltar que se impone la obligación de que todo evento identificado que afecte la confidencialidad, integridad y disponibilidad de los datos personales, o que indique un posible incumplimiento de las medidas de seguridad establecidas, **debe ser reportado inmediatamente al encargado del banco de datos personales; esta exigencia responde a acciones correctivas y a generar una mejora continua del sistema de seguridad de datos personales.**

Por último, siendo una medida optativa, el artículo 31 de la LPDP otorga a las entidades representativas de los titulares o encargados de bancos de datos, la posibilidad de elaborar **códigos de conducta** que establezcan normas internas para el tratamiento de datos personales; códigos que tiendan a asegurar y mejorar las condiciones de operación de los sistemas de información en función de los principios rectores establecidos. El artículo 90 del Reglamento consigna los requisitos esenciales que deberá contener el código de conducta.

Mediante estos Códigos, se pretende establecer un **sistema de autorregulación** que incluya garantías adicionales a las exigidas por la normativa de protección de datos, pero con el matiz de establecer en ellos un plus o un esmero adicional a la hora de establecer dichas prácticas. Los códigos persiguen adecuar la normativa a las peculiaridades de sectores o empresas concretas, conteniendo reglas o estándares específicos con el objetivo de armonizar los tratamientos de datos efectuados por los adheridos; facilitar el ejercicio de los derechos de los afectados y, en definitiva, favorecer el cumplimiento de lo dispuesto en la normativa de protección de datos.

Por lo tanto, el nivel de seguridad del sistema de protección de datos personales dependerá del análisis de riesgo que se realice y de la categoría que se le dé al tratamiento del banco de datos. A mayor riesgo de infracción de la normativa sectorial, se deberán implementar mayores medidas. Como se ha visto, las medidas que se deben implementar deben estar destinadas a detectar y prevenir el acceso no autorizado a los datos personales, pérdida, destrucción, contaminación, uso fraudulento, copia, modificación, adulteración, revelación, comunicación o difusión no autorizada. Asimismo, el sistema requiere constante evaluación y revisión, a fin de determinar las falencias, que serán superadas mediante las medidas correctivas correspondientes (Clavijo, 2016:72).

4.1.4. DE LAS INFRACCIONES Y SANCIONES ADMINISTRATIVAS

Finalmente, es necesario señalar que el incumplimiento de las obligaciones establecidas por la LPDP y su Reglamento puede originar responsabilidad administrativa, civil e, incluso, penal. En primer lugar, el procedimiento administrativo sancionador lo inicia de oficio la Autoridad Nacional de Protección de Datos Personales, siendo la que determinará si el administrado incurrió en una infracción leve, grave o muy grave, ello de acuerdo a lo prescrito en el artículo 38 de la LPDP y regida de acuerdo a lo dispuesto por el numeral 4) del artículo 230 de la Ley Nº 27444, Ley del Procedimiento Administrativo General, siendo el Director de la Dirección de Sanciones el que instruye y resuelve en primera instancia y, el Director General de Protección de Datos Personales resuelve en segunda y última instancia el procedimiento sancionador, con ello se agota la vía administrativa.

Una vez determinada la infracción, procede establecer el monto de las multas por las infracciones cometidas, en el numeral 3 del artículo 39 de la LPDP podemos ver las siguientes: **(i)** Infracciones leves de desde cero coma cinco de una unidad impositiva tributaria (UIT) hasta cinco unidades impositivas tributarias (UIT); **(ii)** Infracciones graves

desde cinco unidades impositivas tributarias (UIT) hasta cincuenta unidades impositivas tributarias (UIT); **(iii)** Infracciones muy graves desde cincuenta unidades impositivas tributarias (UIT) **hasta cien unidades impositivas tributarias (UIT).**

Pues bien, habiéndose determinado los montos, llegado a este punto corresponde mencionar que infracciones son consideradas leves, graves o muy graves y si la ejecución de éstas constituye un cumplimiento o atenuación de la responsabilidad, en relación a la investigación determinaré los siguientes:

De acuerdo al reglamento, se considera **INFRACCIÓN LEVE** cuando, **(i)** el titular del banco de datos de la entidad ha realizado el tratamiento de datos personales incumpliendo las medidas de seguridad establecidas en la LPDP (adoptar medidas técnicas y organizativas), **(ii)** cuando se recopile datos personales que no sean necesarios, adecuados ni pertinentes y **(iii)** no inscribir ni actualizar en el Registro Nacional los actos establecidos en el artículo 34 de la LOPD (por ejemplo, la inscripción y actualización de los códigos de conducta).

Se consideran **INFRACCIONES GRAVES, (i)** realizar el tratamiento de datos personales sensibles incumpliendo las medidas de seguridad establecidas en la normativa de protección de datos y **(ii)** incumplir la obligación de confidencialidad**.** Por último, SON **INFRACCIONES MUY GRAVES**, **(i)** dar tratamiento a los datos personales contraviniendo las obligaciones contenidas en la LPDP y su Reglamento, **(ii)** Recopilar datos personales mediante medios fraudulentos, desleales o ilícitos y **(iii)** no cumplir con las medidas correctivas establecidas por la Autoridad como resultado de un procedimiento trilateral.

Conforme al artículo 126 de la LPDP, se considerará atenuantes cuando la entidad ha colaborado con las acciones de la Autoridad Nacional de Datos Personales y el

reconocimiento espontáneo de las infracciones, ello permitirá la reducción motivada de la sanción por debajo del rango previsto en las disposiciones legales.

La imposición de la multa se efectúa sin perjuicio de las sanciones disciplinarias sobre el personal de las entidades públicas en los casos de bancos de datos personales de administración pública, asimismo se configurará una responsabilidad civil del titular del banco de datos personales por la pérdida, alteración o un uso de los datos personales contrario a la a las disposiciones vigentes, estando obligado a indemnizar por los daños y perjuicios al titular de los datos personales, además la Autoridad de Protección de Datos podrá imponer multas coercitivas frente al incumplimiento de las obligaciones accesorias de la sanción.

De acuerdo con Clavijo (2016), respecto a la responsabilidad penal es necesario analizar dos disposiciones legales, las cuales son: En primer lugar, el Capítulo II del Título IV del Código Penal tipifica los delitos relativos a la violación de la intimidad y el honor: i) artículo 154 (violación de la intimidad), ii) artículo 154-A (tráfico ilegal de datos personales), iii) artículo 156 (revelación de la intimidad personal y familiar) y iv) artículo 157 (uso indebido de archivos computarizados).

El artículo 154-A, que tipifica el delito de Tráfico Ilegal de Datos Personales tiene especial relevancia, ya que se vincula directamente con la protección de datos personales; este tipo penal sanciona con pena privativa de libertad no menor de dos ni mayor de cinco años a quien ilegítimamente comercializa o vende información no pública relativa a cualquier ámbito de la esfera personal, familiar, patrimonial, laboral, financiera u otro de naturaleza análoga sobre una persona natural.

Es necesario resaltar que los delitos tipificados en el mencionado Capítulo son perseguibles por acción privada, salvo en el caso del delito previsto en el artículo 154-A, lo cual demuestra un interés mayor del Estado por sancionar ese tipo de conducta. En segundo

lugar, debemos referirnos a la Ley 30096 –Ley de Delitos Informáticos, modificada por la Ley 30171 "Ley que modifica la Ley de Delitos Informáticos"; esta norma ha criminalizado una serie de conductas que afectan los sistemas y datos informáticos y otros bienes jurídicos de relevancia penal, cometidas mediante la utilización de tecnologías de la información o de la comunicación.

Se trata de una lucha frontal contra la llamada ciberdelincuencia, también describe el delito de Acceso Ilícito, tipificado en el artículo 2 de la Ley de Delitos Informáticos, que sanciona al que deliberada o ilegítimamente accede a todo o en parte de un sistema informático, siempre que se realice con vulneración de las medidas de seguridad establecidas para impedirlo; asimismo, sanciona a quien accede a un sistema informático excediendo lo autorizado.

Otro delito que se podría configurar es el de Atentado a la Integridad de Datos Informáticos, tipificado en el artículo 3 de la Ley, que sanciona a quien deliberada o ilegítimamente daña, introduce, borra, deteriora, altera, suprime o hace inaccesibles datos informáticos. Asimismo, se podría configurar el delito de Atentado a la Integridad de Sistemas Informáticos, tipificado en el artículo 4, que sanciona a quien deliberada o ilegítimamente inutiliza total o parcialmente un sistema informático, impide el acceso a este, entorpece o imposibilita su funcionamiento o la prestación de su servicio. (Clavijo, 2016).

RESPECTO AL OBJETIVO ESPECÍFICO N° 02

4.2. DEL ANÁLISIS COMPARATIVO DEL IT COMPLIANCE, PRIVACIDAD Y PROTECCIÓN DE DATOS EN LOS SISTEMAS JURÍDICOS DEL PERÚ CON LA UNIÓN EUROPEA, ESPAÑA, ARGENTINA Y URUGUAY

DERECHO CONTINENTAL

En Europa son diversos los países que han implementado y regulado un sistema de responsabilidad penal, administrativa y autónoma de las personas jurídicas en relación al tratamiento de los datos personales, dejando a entrever que han adoptado un sistema de **autorregulación regulada**.

A continuación, describiré los sistemas jurídicos relacionados al manejo de la información de la Unión Europea y España, los mismos que actualmente cuenta con disposiciones legales que incluyen la protección de datos en las empresas.

4.2.1. DEL TRATAMIENTO DE DATOS EN LA UNIÓN EUROPEA

En cuanto a la regulación jurídica de la protección de datos en Europa, cabe señalar que las normas más relevantes en este ámbito han tenido una influencia indudable en las normativas nacionales de los Estados miembros de la Unión Europea, implicando un aumento del nivel de protección y un efecto homogenizante.

La Unión Europea destaca por su compromiso por la adecuada protección de derechos, poniendo especial atención al tratamiento de la privacidad y protección de datos, realizada mediante los instrumentos jurídicos que dispone. El primer texto normativo, en el ámbito estrictamente europeo, que garantiza como derecho fundamental el respeto a la vida privada está representada por el artículo 8 del Convenio Europeo de Derechos Humanos, aprobado en Roma en 1950. Luego, la primera iniciativa formal que podemos encontrar, es el denominado Convenio 108 del año 1981, que veremos a continuación.

4.2.1.1. CONVENIO N° 108 DEL CONSEJO DE EUROPA

El 28 de enero de 1981, los estados miembros del Consejo de Europa aprobaron el "Convenio N. 108 del consejo de Europa para la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal", (en adelante, el Convenio), siendo el instrumento más relevante en materia de protección de las personas físicas en cuanto al tratamiento automatizado de datos personales, además, fue la primera norma europea que marcó las pautas del modelo común de Protección de Datos.

El Convenio tenía por objeto que, en el territorio de cada nación parte le sea respetado a las **personas** su derecho a la salvaguarda de su información, de esta forma contribuyó a la protección de los derechos y las libertades fundamentales, ello teniendo en cuenta la intensificación de la circulación a través de las fronteras de los datos de carácter personal que son objeto de tratamientos informatizados.

Asimismo, el Convenio recogía principios básicos, tales como, **a) principio de lealtad**, b) principio de exactitud, c) principio finalista, c) principio de pertinencia, d) principio de utilización no abusiva, e) principio del derecho al olvido, f) principio de publicidad, y d) **principio de seguridad**; por último es necesario señalar que mediante el inciso 2, del art. 4 del convenio se obligaba a los estados miembros, tales como España a dotarse de una ley interna de protección de datos dentro del plazo que el propio Convenio establecía en su artículo 22:

"El presente Convenio entrará en vigor el día primero del mes siguiente a la expiración de un período de tres meses después de la fecha en que cinco Estados miembros del Consejo de Europa hayan expresado su consentimiento para quedar vinculados por el Convenio, con arreglo a las disposiciones del párrafo anterior (…)".

4.2.1.2. DIRECTIVA 95/46/CE DEL PARLAMENTO EUROPEO

A mediados de octubre de 1995, las autoridades legislativas y ejecutivas de la Unión Europea, conscientes de la importancia que tiene la protección de los derechos y libertades fundamentales, en particular el Derecho a la Intimidad, como de la necesidad de viabilizar todo procesamiento, tratamiento, circulación y teletransmisión de los datos personales con miras al mejoramiento de la sociedad y las economías de los Estados Miembros, publican, respectivamente, la Directiva 95/46/CE (Da Cunha Lopes, 2010).

Es así, que en fecha 24 de octubre de 1995, entró en vigencia la Directiva 95/46/CE del Parlamento Europeo y del Consejo, (en adelante, la Directiva). La base de la Directiva son los principios aportados por el Convenio anteriormente descrito. Se trata del **primer instrumento** que obliga a los Estados miembros a garantizar la protección, a las personas físicas, de derechos como la intimidad y protección de datos, así como la libre circulación de tales datos, además sintetizó los principios aportados por el Convenio N° 108.

A fin de garantizar las disposiciones legales emitidas, se adoptó medidas legales que limitarían el alcance de las obligaciones, tales limitaciones eran medidas necesarias para salvaguardar: a) la seguridad del Estado; b) la defensa; c) la seguridad pública; d) la prevención, la investigación, la detección y la represión de infracciones penales o de las infracciones de la deontología en las profesiones reglamentadas; e) un interés económico y financiero importante de un Estado miembro o de la Unión Europea, incluidos los asuntos monetarios, presupuestarios y fiscales; **f) función de control, de inspección o reglamentaria relacionada, aunque sólo sea ocasionalmente, con el ejercicio de la autoridad pública en los casos a que hacen referencia las letras c), d) y e); g) la protección del interesado o de los derechos y libertades de otras personas.**

Otro punto importante lo encontramos en el capítulo V de la Directiva, donde se establecía que los estados miembros del parlamento debían impulsar la elaboración de códigos de conducta, los mismos que estaban destinados alinear la correcta aplicación de las disposiciones nacionales adoptadas por los estados miembros, éstos debían establecer que las asociaciones profesionales y demás organizaciones representantes de otras categorías de responsables de tratamientos, que hayan elaborado códigos nacionales existentes puedan someterlos a exámenes nacionales.

Por último, una de las prerrogativas que no debemos soslayar es la adopción de una **Autoridad de Control**, en la Directiva se establecía que cada Estado miembro dispondrá de una o más autoridades públicas, quienes se encargarían de la vigilancia de sus disposiciones sobre materia de protección de datos. La autoridad de protección de datos estaba obligada a presentar periódicamente un informe sobre sus actividades, siendo publicadas.

4.2.1.3. REGLAMENTO (UE) 2016/679 DEL PARLAMENTO EUROPEO Y DEL CONSEJO

El Reglamento UE 2016/679, (en adelante, el RGPD), publicada el 27 de abril de 2016, entró en vigencia para ser aplicada a **partir del 25 de mayo de 2018,** constituida por 173 considerandos previos, y 99 artículos divididos en 11 capítulos, la misma que derogó expresamente la Directiva 95/46/CE con efecto a partir del 25 de mayo de 2018, indicando que cualquier referencia que se contenga a la citada Directiva que se deroga, se entenderá hecha a dicho RGPD.

El RGPD, tiene por objeto regular las normas relativas a la protección de las personas físicas en lo que respecta al tratamiento de los datos personales y las normas relativas a la libre circulación de tales datos, así como la protección de los derechos y libertades

fundamentales de las personas físicas y, en particular, **su derecho a la protección de los datos personales.**

El RPGD supone una profunda modificación del régimen vigente en materia de protección de datos personales, no sólo desde el punto de vista sustantivo y de cumplimiento por los sujetos obligados, sino particularmente en lo que afecta a la **actividad de supervisión** por parte de las autoridades de control que el mismo regula. Los principios aplicables al tratamiento de datos en el RGPD están regulados en su artículo 5, y son:

- Licitud, lealtad y transparencia; recogidos con fines determinados, explícitos y legítimos (limitación de la finalidad)

- Limitados a lo necesario en relación con los fines para los que son tratados (minimización de datos)

- Exactos y, si fuera necesario, actualizados («exactitud»)

- Mantenidos de forma que se permita la identificación de los interesados durante no más tiempo del necesario para los fines del tratamiento de los datos personales («limitación del plazo de conservación»)

- Tratados de tal manera que se garantice una seguridad adecuada de los datos personales («integridad y confidencialidad»)

- El responsable del tratamiento será responsable del cumplimiento de lo establecido en las disposiciones del RGPD («responsabilidad proactiva»).

4.2.1.3.1. DEL RESPONSABLE DEL TRATAMIENTO DE PROTECCIÓN DE DATOS PERSONALES

El responsable del tratamiento es la persona física o jurídica o autoridad pública, que decide sobre el tratamiento de los datos personales, determinando los fines y los medios de dicho tratamiento. En virtud del principio de **responsabilidad proactiva** el responsable del

tratamiento tiene que aplicar **medidas técnicas y organizativas** para, en atención al riesgo que implica el tratamiento de los datos personales, cumplir y ser capaz de **demostrar el cumplimiento.**

El RGPD atribuye, en determinadas condiciones, al responsable del tratamiento la aplicación de medidas técnicas y organizativas apropiadas, que se revisarán y actualizarán cuando sea necesario, a fin de garantizar y poder demostrar que el tratamiento es conforme a esta normativa (por ejemplo, la aplicación, por parte del responsable del tratamiento, de políticas de protección de datos).

Para demostrar el cumplimiento de las obligaciones por parte del responsable del tratamiento se mencionan expresamente la **adhesión a códigos de conducta o a un mecanismo de certificación**. Asimismo, el responsable del tratamiento de protección de datos puede elegir a un **encargado que ofrezca garantías suficientes para aplicar medidas técnicas y organizativas apropiadas**, de manera que el tratamiento sea conforme al RGPD y garantice la protección del tráfico de datos, asimismo, cada responsable, representante o encargado llevará un registro de las actividades de tratamiento efectuadas, bajo sanción en caso de incumplimiento.

Se prevé que el responsable del tratamiento en determinadas condiciones (cuando sea probable que un tipo de tratamiento entrañe un alto riesgo para los derechos y libertades de las personas físicas), realice una **evaluación del impacto** de las operaciones de tratamiento en la protección de datos personales junto con el asesoramiento del **delegado de protección de datos**, si ha sido nombrado.

Se regula una consulta previa a la autoridad de control, por parte del responsable del tratamiento que deberá facilitar una concreta información que se detalla, antes de proceder al tratamiento en aquellos supuestos en los que una **evaluación de impacto** relativa a la

protección de los datos muestre que el tratamiento entrañaría un alto riesgo si es que el responsable no toma medidas para para mitigarlo.

Si la **Autoridad de Control** considera que el tratamiento puede infringir la normativa prevista en el RGPD, en particular cuando el responsable no haya identificado o mitigado suficientemente el riesgo, la autoridad de control tiene que asesorar por escrito al responsable, y en su caso al encargado, en un plazo de ocho semanas desde la solicitud de la consulta, aunque este plazo podrá prorrogarse seis semanas, en función de la complejidad del tratamiento previsto, y suspenderse hasta que la autoridad de control haya obtenido la información solicitada a los fines de la consulta.

4.2.1.3.2. DEL DELEGADO DE PROTECCION DE DATOS

El Reglamento Europeo ha introducido la figura del **Delegado de Protección de Datos (en adelante, DPD)**, imponiendo su designación al **responsable y al encargado** del tratamiento, exigiendo la obligatoriedad de su nombramiento a todos los organismos públicos, con la excepción de tribunales que actúen en el ejercicio de la función judicial, y a las entidades privadas, sean éstas consideradas responsables o encargados del tratamiento, cuyas actividades principales conlleven la "observación habitual y sistemática de interesados a gran escala" o el "tratamiento a gran escala de categorías especiales de datos personales" y "de datos relativos a condenas e infracciones penales".

En cuanto a las funciones que tendrá el DPD, destacan el asesoramiento general dentro de la compañía en todo lo relativo a protección de datos personales, **la supervisión del cumplimiento de la legislación y políticas de privacidad con especial atención a los riesgos asociados a las actividades que llevara a cabo la empresa**, la elaboración de informes de **evaluación de impacto** de ciertos tratamientos de datos personales y la cooperación con las autoridades de control nacionales. Cada responsable o encargado del

tratamiento de datos (o su representante) realizará un registro que deberá contener toda la información indicada, disposición contenida en el art. 30 del RGPD, bajo sanción en caso de incumplimiento.

4.2.1.3.3. DE LAS MEDIDAS DE SEGURIDAD

El RGPD atribuye, en determinadas condiciones, al responsable y encargado del tratamiento la aplicación de medidas técnicas y organizativas apropiadas, que se revisarán y actualizarán cuando sea necesario, a fin de garantizar y poder demostrar que el tratamiento es conforme a derecho, por ejemplo, la aplicación por parte del responsable del tratamiento, de políticas de protección de datos, entre otros. Para demostrar el cumplimiento de las obligaciones se menciona en la RGPD expresamente la adhesión a códigos de conducta o algún mecanismo de certificación que acredite las buenas prácticas corporativas, en mérito a lo dispuesto en el artículo 41 del RGPD, el cumplimento de los códigos de conducta será supervisado por la Autoridad de Control.

Asimismo, la RGPD prescribe deberes obligatorios para el responsable y encargado del tratamiento bajo sanción en caso de incumplimiento, los cuales veremos a continuación:

- **Deber de protección de datos desde el diseño,** tiene como objetivo cumplir los requisitos definidos en el RGPD y, por tanto, los derechos de los interesados y busca que la protección de datos se encuentre presente en las primeras fases de concepción de un proyecto.

- **Deber de protección de datos por defecto**, se refiere a que sólo sean objeto de tratamiento los datos personales que sean estrictamente necesarios para cada uno de los fines de tratamiento.

- **Deber de cooperación con la autoridad de control**, los responsables y encargados están obligados a facilitar la información para investigaciones o cuando sean requeridos por la autoridad competente.

- Deber de registro de las actividades del tratamiento, los responsables deben documentar todas las operaciones del tratamiento, es decir debe existir un registro respecto de cada actividad del tratamiento realzado, por ejemplo, los fines, categoría de los datos, trasferencias internacionales, las medidas técnicas y organizativas adoptadas, entre otros). Este deber no se encuentra establecido en nuestra legislación, de acuerdo a la Directiva de protección de datos del Perú, no obliga al titular del banco de datos o encargado del tratamiento a registrar las medidas de seguridad implementadas o transferencias internacionales realizadas, siendo hitos importantes de garantía en la protección de datos.

- Deber de información y de transparencia, establece que se debe facilitar a los interesados la información sobre el tratamiento de sus datos personales en el momento en que se obtengan de ellos.

- Deber de seguridad en el tratamiento, en caso se advierta una brecha en la seguridad del tratamiento, el responsable o encargado del manejo de los datos, deberá comunicar inmediatamente la Autoridad de Control y al afectado, bajo sanción. En la legislación peruana se impone la obligación de que todo evento que afecte al tratamiento **sea reportado al encargado del tratamiento o titular del banco de datos**, sin embargo, no adopta como medida de seguridad, el deber de informar posibles infracciones en el tratamiento al afectado y a la Autoridad Nacional de Protección de Datos.

- Deber de evaluación del impacto, cuando exista probabilidad que un tipo de tratamiento alcance un alto riesgo para los derechos y libertades de las personas físicas, el responsable y encargado del tratamiento deberá realizar una evaluación del impacto de las operaciones de tratamiento en la protección de datos personales.

La evaluación deberá contener como mínimo: **(i)** una descripción sistemática de las operaciones del tratamiento, **(ii)** una evaluación de interés y la proporcionalidad de las

operaciones del tratamiento con respecto a su finalidad, **(iii) evaluación de los riesgos** y **(iv)** medidas de seguridad y mecanismos que garanticen la protección de datos personales, por último el cumplimiento de los códigos de conducta se tendrá en cuenta para evaluar las operaciones de tratamiento realizada por los responsables o encargados, en particular para la evaluación del impacto.

En este mismo sentido, debe señalarse que las medidas de seguridad establecidas en el RGPD se configuran como mínimos exigibles, de ahí muchas organizaciones (por iniciativa propia) personalizan y amplían dichas medidas de seguridad en función de los riesgos específicos de sus procesos de negocio y de la propia estructura y funcionamiento interno de la organización

4.2.1.3.4. DE LA AUTORIDAD DE CONTROL Y REGULACIÓN DE TRANSFERENCIAS

Los estados miembros establecerán que es responsabilidad de una o varias autoridades públicas independientes, supervisar la aplicación del RGPD, con el fin de proteger los derechos y libertades fundamentales de las personas físicas en lo que respecta al tratamiento y de facilitar la libre circulación de datos personales dentro de la Unión Europea.

En la RGPD, una transferencia internacional de datos es un tratamiento de datos que supone una transmisión de los mismos fuera del territorio del Espacio Económico Europeo (EEE), bien constituya una cesión o comunicación de datos o tenga por objeto la realización de un tratamiento de datos por cuenta del responsable del soporte de datos establecido en territorio español.

Así, si los datos personales se transfieren de la Unión Europea a responsables, encargados u otros destinatarios en terceros países o a organizaciones internacionales, esto no debe menoscabar el nivel de protección de las personas físicas garantizado en la Unión

Europea por el nuevo reglamento de protección de datos, ni siquiera en las transferencias ulteriores de datos personales desde el tercer país u organización internacional a responsables y encargados en el mismo u otro tercer país u organización internacional, en caso de incumplimiento se cometerá una infracción.

Con esta finalidad se encomienda a la Comisión la evaluación del nivel de protección que ofrece un territorio o un sector de tratamiento en un tercer país, y en el supuesto que la Comisión no haya adoptado una decisión, la transferencia de datos personales se puede seguir realizando en casos especiales o cuando existan garantías apropiadas (cláusulas tipo de protección de datos, normas corporativas vinculantes, cláusulas contractuales).

En definitiva, en ausencia de una decisión por la que se constate la adecuación de la protección de los datos, el responsable o el encargado del tratamiento deben tomar medidas para compensar la falta de protección de datos en un tercer país mediante garantías adecuadas para el interesado.

4.2.1.3.5. DE LAS INFRACCIONES Y SANCIONES

El RGPD contempla la posibilidad de que el interesado que considere vulnerados sus derechos, pueda conferir mandato a una entidad, organización o asociación sin ánimo de lucro para que presente en su nombre una reclamación ante la autoridad de control, ejerciendo el derecho a la tutela judicial en nombre de los interesados e incluso a ser indemnizado, si así lo establece el Derecho del Estado miembro.

El RGPD declara que el responsable o el encargado del tratamiento tiene que indemnizar los daños y perjuicios que pueda sufrir una persona como consecuencia de una infracción al Reglamento (artículo 82.1 RGPD), es decir cualquier responsable que participe en la operación de tratamiento de datos y que no haya **cumplido con las obligaciones que demanda el RGPD,** responderá por los daños causados. **Sin embargo, quedarán exento de**

responsabilidad si se demuestra que no es en modo alguno responsable de los hechos que hayan causado los daños. (artículo 82.3 RGPD). A este punto podemos inferir que si el encargado o responsable del tratamiento a cumplido con las medidas y obligaciones establecidas en el RGPDP para el manejo de los datos personales, quedará exento de responsabilidad en caso exista alguna infracción al interesado de los datos.

El régimen sancionador se agrava y se vuelve mucho más exigente, existiendo la posibilidad de que la Autoridad de Control imponga sanciones, multas administrativas, que pueden alcanzar los 20.000.000 EUR, o tratándose de una empresa, de una cuantía equivalente al 4 % como máximo del volumen de negocio total anual global del ejercicio financiero anterior, optándose por la de mayor cuantía. (artículo 83.5 RGPD).

Por último, para la imposición de multas administrativas se deberá considerar los criterios generales contenidos en el artículo 83 del RGPD, siendo los siguientes: por ejemplo: **(i)** la naturaleza, gravedad y duración de la infracción, **(ii)** intencionalidad o negligencia en la infracción, **(iii)** las medidas que optó el responsable o encargado del tratamiento para mitigar los daños y perjuicios, **(iv)** el grado de aplicabilidad de las medidas técnicas y organizativas (de diseño y por defecto, y medidas de protección) optadas por el responsable o encargado del tratamiento, **(v)** el grado de cooperación con la autoridad de control con el fin de poner remedio a la infracción, **(vi)** si el responsable o encargado notificaron a la autoridad de control y afectado cualquier brecha de seguridad al tratamiento de datos, **(vii)** la adhesión de códigos de conducta y **(viii)** cualquier otro factor agravante o atenuante aplicable a las circunstancias del caso, como los beneficios financieros obtenidos o las pérdidas evitadas, directa o indirectamente, a través de la infracción.

4.2.2. DEL TRATAMIENTO DE DATOS EN ESPAÑA

La Constitución Española en su artículo 10 reconoce el derecho a la dignidad de la persona. Por su parte, el artículo 18.4 dispone que la "ley limitará el uso de la informática para garantizar el honor y la intimidad personal y la familiar de los ciudadanos y el pleno ejercicio de sus derechos".

De ambos preceptos deriva el derecho fundamental a la protección de datos de carácter personal, que ha sido definido como autónomo e independiente por la Sentencia del Tribunal Constitucional 292/2000, de 30 de noviembre /RTC2000.292).

La citada sentencia, define el contenido del derecho fundamental a la protección de datos personales como la facultad que se le otorga al titular de los datos de poder disponer de su información personal sea quien sea el tercero que los trate. Reza la sentencia que, "el derecho fundamental a la protección de datos persigue garantizar a esa persona un poder de control sobre sus datos personales, sobre su uso y destino, con el propósito de impedir su tráfico ilícito y lesivo para la dignidad y derecho afectado".

4.2.2.1. LEY ORGANICA 5/1992, DE REGULACIÓN DEL TRATAMIENTO AUTOMATIZADO DE LOS DATOS DE CARÁCTER PERSONAL

La Ley Orgánica 5/1992, fue aprobada por el estado Español en fecha 29 de octubre de 1992, (en adelante, LORTA) culminó un proceso de elaboración doctrinal y normativa que se remonta al año 1976. Con esta ley, España cumplía el compromiso asumido con la ratificación del Convenio 108 del Consejo de Europa. El objeto de la LORTA fue regular el tratamiento automatizado de los datos de carácter personal, su alcance de la regulación no era tecnológico, sino pretendía limitar el uso de la informática y otras técnicas y medios de tratamiento automatizado de la información en aras de la salvaguarda de los derechos de la

personalidad, recogiendo lo establecido en el inciso 4 del artículo 18 de la Constitución Española, como el honor, la intimidad personal y familiar y el pleno ejercicio de los derechos.

La LORTA estableció un **sistema preventivo es decir cautelar, tendente a evitar que por efecto del uso incontrolado de los datos se produzcan perjuicios a las personas**, siendo el fin primordial ya no la protección de los datos de carácter personal, sino la libre circulación de los datos dentro del mercado interior. La protección de los datos es una limitación a la libre circulación, concebida como una norma protectora de alto nivel y como tal excluye toda limitación de la libre circulación de los datos que invoque la protección de los derechos y libertades.

A diferencia de las demás leyes de protección de datos, la LORTA no ha tipificado tipos penales. Ésta ha seguido la orientación de las leyes administrativas promulgadas desde mediados de la década de los ochenta, fundada en el principio de mínima intervención. En consecuencia, el dispositivo coercitivo de la ley no contiene unos tipos de delito, sino sólo de infracciones administrativas, constituyéndose en multas, considerándose como infracción grave, mantener los ficheros, locales, programas o equipos que contengan datos de carácter personal sin las debidas condiciones de segundad, esto contenido en el literal h del numeral 3 del artículo 43 de la Ley.

Por último gracias a esta ley se creó la **Agencia de Protección de Datos de Carácter Personal en España,** como un ente de derecho público con personalidad jurídica propia y plena capacidad pública y privada que actúa con independencia de la Administración pública en el ejercicio de sus funciones, siendo promulgada obedeciendo lo establecido por la Ley mediante el Real Decreto 428/1993 de 26 de marzo.

4.2.2.2. LEY ORGÁNICA 15/1999 DE PROTECCIÓN DE DATOS DE CARÁCTER PERSONAL

La ley orgánica 15/1999 de protección de datos de carácter personal, (en adelante, LOPDCP), entró en vigencia por el ordenamiento jurídico español el 13 de diciembre de 1999, a fin de dar cumplimiento a las disposiciones contenidas en la Directiva 95/46/CE del Parlamento Europeo.

Esta norma tenía como objeto garantizar y proteger el tratamiento de los datos personales, las libertades públicas y los derechos fundamentales de las personas físicas que se circunscribían en el territorio español, también, cuando el responsable del tratamiento no establecido en territorio español, le sea de aplicación la legislación española en aplicación de normas de Derecho Internacional Público, para ello veremos algunos de sus tópicos más importantes.

4.2.2.2.1. DE LOS PRINCIPIOS Y OBLIGACIONES

Los datos objeto de tratamiento deben ser recogidos de forma lícita, adecuarse a la finalidad para la que fueron recabados, ser exactos y no mantenerse indefinidamente sin justificación. A continuación, se explica brevemente en qué consisten cada una de las vertientes del principio de calidad de datos:

- **Finalidad.** Los datos sólo se podrán recoger para su tratamiento, así como someterlos a dicho tratamiento, cuando sean adecuados, pertinentes y no excesivos en relación con el ámbito y las finalidades determinadas, explícitas y legítimas para las que se hayan obtenido y, respecto de las cuales, se hubiera informado al afectado.

- **Utilización no abusiva.** La utilización no abusiva de los datos impide que los datos se usen para finalidades incompatibles con aquellas para las cuales hubieran sido recogidos, si bien

no se considera incompatible el tratamiento posterior de estos con fines históricos, estadísticos o científicos.

- Exactitud. Los datos serán exactos y puestos al día de forma que respondan con veracidad a la situación actual del afectado. Si los datos de carácter personal registrados resultaran inexactos, en todo o en parte, o incompletos, serán cancelados y sustituidos de oficio por los correspondientes datos debidamente rectificados o completados.

- Lealtad. Por último, la Ley impone la obligación de lealtad el Responsable del Fichero. Se prohíbe la recogida de datos por medios fraudulentos, desleales o ilícitos. La ilicitud en la recogía de los datos implica cumplir los mandatos señalados que, a modo de resumen serían los siguientes:

(i) los datos han de recabarse de forma legal, siendo necesario el consentimiento del afectado, Salvo que la Ley disponga ora cosa; (ii) los datos recabados deberán ser necesarios para la realización del contrato o la actividad que justifique su recogida y **(iii)** se utilizarán únicamente para la finalidad legítima para la que han sido recogidos.

4.2.2.2.2. DEBER DE INFORMACIÓN

El artículo 5 de la LOPDCP, establece que cuando se recaben datos de carácter personal será necesario informar al afectado de determinados extremos en relación con la recogida y tratamiento de sus datos personales.

De manera general, cuando los datos se recogen directamente de su titular, el Responsables del Fichero tiene la tarea de informarle previamente de modo expreso, preciso e inequívoco de los siguientes puntos:

- De la existencia de un fichero de datos de carácter personal, de la finalidad de la recogida de los datos y de sus destinatarios.

- Del carácter obligatorio o facultativo de sus respuestas a las preguntas que les fueran planteadas.
- De las consecuencias de la obtención de datos o de la negativa a suministrarlos.
- De la posibilidad del interesado de ejercitar los derechos de acceso, rectificación, cancelación y oposición.
- De la identidad y dirección del Responsable del Tratamiento o, en su caso, de su representante.

4.2.2.2.3. SEGURIDAD DE DATOS

De conformidad con lo establecido en el artículo 9 de la LOPDCP, el Responsable del Fichero y en su caso el Encargado del Tratamiento deberán adoptar las medidas de índole técnica y organizativas necesarias para que garanticen la seguridad de los datos de carácter personal y eviten su alteración, pérdida, tratamiento o acceso no autorizados, habida cuenta del estado de la tecnología, la naturaleza de los datos y los riesgos existentes.

Al respecto, conviene precisar que las medidas de seguridad aplicables a los ficheros automatizados (informáticos) y no automatizados (en soporte papel) que contengan datos de carácter personal se clasifican en tres niveles: básico, medio y alto en función de la tipología y sensibilidad de los datos personales contenidos en los mismos.

a) Niveles de Seguridad

Como se ha mencionado con anterioridad, las medidas de seguridad aplicables a los ficheros y tratamientos que contengan datos de carácter personal se clasifican en tres niveles; básico, medio y alto.

- **Nivel Básico.** Todos los ficheros que contengan datos de carácter personal deberán adoptar las medidas de seguridad de nivel básico.

- **Nivel Medio.** Deberán implementarse, además de las medidas de seguridad de nivel básico, las medidas de nivel medio, en los siguientes ficheros o tratamientos: Ficheros de solvencia patrimonial y crédito, los relativos a la comisión de infracciones administrativas o penales , aquellos de los que sean responsables las entidades financieras para finalidades relacionadas con la prestación de servicios financieros y aquellos de los que sean responsables las mutuas de accidentes de trabajo y enfermedades profesionales de la Seguridad Social, etc.
- **Nivel Alto.** Las medidas de nivel alto se aplicarán en los siguientes ficheros o tratamientos de datos de carácter personal: datos relativos a ideología, afiliación sindical, religión, creencias, origen racial, salud o vida sexual, datos recabados para fines policiales sin consentimiento de las personas afectadas y datos relativos a actos de violencia de género.
- **Supuestos Especiales.** Con respecto a los datos de tráfico y localización tratados por los operadores que presten servicios de comunicaciones electrónicas disponibles al público o exploten redes públicas de comunicaciones electrónicas.

b) Medidas de Seguridad

Las medidas de seguridad de índoles técnica y organizativa a implementar por parte del responsable del Fichero, se sintetizan en el siguiente cuadro:

4.2.2.2.4. MEDIDAS DE SEGURIDAD COMUNES A TODOS LOS FICHEROS

a) Documento de Seguridad. Se encuentra regulado en el artículo 88 del LOPDCP constituye un documento interno de la organización esencial a la hora de definir y aplicar de forma adecuada las medidas de seguridad en los sistemas de información, debiendo existir en cualquier organización que trate datos de carácter personal.

b) Delegación de Autorizaciones. Las autorizaciones atribuidas al Responsable del Fichero podrán ser delegadas en las personas designadas al efecto. Además, deberán constar en el documento de seguridad las personas habilidades para otorgar estas autorizaciones, así como aquellas sobre las que recae dicha delegación. Esta designación, en ningún caso, supone una delegación de responsabilidad que corresponde al Responsable del Fichero.

c) Acceso a Datos a través de Redes de Telecomunicaciones. El LOPDCP establece que las medidas de seguridad exigibles a los accesos a datos de carácter personal a través de redes de comunicaciones deberán garantizar un nivel de seguridad equivalente al acceso en modo local.

d) Régimen de Trabajo. El reglamento del LOPDCP señala que cuando los datos de carácter personal se almacenen en dispositivos portátiles o se traten fuera de los locales del Responsable del Fichero o del Encargado del Tratamiento será necesario que exista una autorización previa por parte del Responsable del Fichero y, en todo caso, que garantice el nivel de seguridad aplicable a los datos.

En tal caso la autorización deberá hacerse constar en el Documento de Seguridad de la organización y podrá establecerse para un usuario o para un perfil de usuario, por un periodo de validez determinado.

e) Ficheros temporales o copias de trabajo. - El artículo 87 del reglamento del LOPDCP establece que los ficheros temporales o copias de trabajo deberán cumplir el nivel que resulte aplicable a los datos y suprimirse cuando no resulte necesario.

4.2.2.2.5. CÓDIGOS TIPO

La regulación de los códigos tipo se establece en el artículo 32 de la LOPDCP y en los artículos 71, 72, 73, 74, 75, 76, 77 y 78 del RLOPD y éstos podrían definirse, como aquellos acuerdos o conjunto de normas deontológicas o de buena práctica que son adoptados por las

entidades, generalmente, pertenecientes a un mismo sector de actividad, para determinar las pautas a tener en cuenta en el desarrollo de sus actividades profesionales.

Los códigos tipo tendrán, por lo tanto, carácter de códigos deontológicos o de buena práctica profesional, debiendo ser depositados e inscrito en a Autoridad de Protección de Datos.

4.2.2.2.6. AUTORIDADES DE CONTROL Y RÉGIMEN SANCIONADOR

Con el objetivo de asegurar el cumplimiento de la legislación vigente en materia de protección de datos y con motivo de conceder mayor seguridad a los derechos fundamentales de las personas física, se crearon agencias con aun ámbito de aplicación limitada a los ficheros de titularidad pública declarados por las administraciones económicas y locales.

Dentro de la Agencia Española de Protección de Datos, encontramos un órgano que se denomina el Registro General de Protección de Datos, cuyas funciones principales se circunscribían en inscribir los ficheros tanto de titularidad privada como pública, además comprendía la inscripción de los códigos tipo.

4.2.2.3. LEY ORGÁNICA 3/2018, DE PROTECCIÓN DE DATOS PERSONALES Y GARANTÍA DE LOS DERECHOS DIGITALES

El 13 de diciembre de 2018, entró en vigor la Ley Orgánica 3/2018, de Protección de Datos Personales y Garantía de Derechos Digitales (en adelante, LOPDPGDG), teniendo como principal objetivo el de adaptar el ordenamiento jurídico español al Reglamento (UE) 2016/679 del Parlamento Europeo y el Consejo, (en adelante, el RGPD).

Asimismo, la LOPDPGDG derogó la Ley Orgánica 15/1999, el Real Decreto-ley 5/2018 y todas las disposiciones de igual o inferior rango que contradigan, se opongan o sean incompatibles con el Reglamento. Esta derogación permitió aclarar el panorama normativo

de protección de datos en España, ya que la normativa previa al Reglamento no se había derogado formalmente, ocasionando inseguridad jurídica en el tratamiento.

Como garantías en el procedimiento se establece que, las infracciones al tratamiento no serán imputables al responsable del tratamiento, siempre que este haya adoptado todas las medidas razonables para que se supriman o rectifiquen sin dilación, asimismo, tampoco será responsable por la inexactitud de los datos obtenidos directamente del afectado, cuando hubiera recibido los datos de otro responsable en virtud del ejercicio por el afectado del derecho a la portabilidad, o cuando el responsable los obtuviese del mediador o intermediario y cuando las normas aplicables al sector de actividad al que pertenezca el responsable del tratamiento establezcan la posibilidad de intervención de un intermediario o mediador o cuando los datos hubiesen sido obtenidos de un registro público.

También se recoge el **deber de confidencialidad** o deber de secreto, siendo que los responsables, encargados de protección están obligados a la **confidencialidad del tratamiento**; también el tratamiento de datos amparado por la ley, las categorías especiales de datos y el tratamiento de datos de naturaleza penal, se alude específicamente al consentimiento, que ha de proceder de una declaración o de una clara acción afirmativa del afectado, excluyendo lo que se conocía como **«consentimiento tácito»,** se indica que el consentimiento del afectado para una pluralidad de finalidades será preciso que conste de manera específica e inequívoca que se otorga para todas ellas, y se mantiene en catorce años la edad a partir de la cual el menor puede prestar su consentimiento.

Se podrán igualmente imponer condiciones especiales al tratamiento, tales como la adopción de **medidas adicionales de seguridad** u otras, cuando ello derive del ejercicio de potestades públicas o del cumplimiento de una obligación legal y solo podrá considerarse fundado en el cumplimiento de una misión realizada en interés público o en el ejercicio de

poderes públicos conferidos al responsable, en los términos previstos en el reglamento europeo, cuando derive de una competencia atribuida por la ley.

Como se ha desarrollado anteriormente, la legislación española adoptó las **figuras del responsable y encargado del tratamiento de protección de datos, establecidos en el título V,** los mismos que deben determinar las medidas técnicas y organizativas apropiadas a fin de garantizar y acreditar que el tratamiento es conforme al Reglamento de la Comisión Europea, conforme se denota en el reglamento. Acerca del **Delegado de Protección de Datos,** el ordenamiento jurídico español dice que, los responsables y encargados del tratamiento deberán designar a un Delegado de Protección de Datos, estando obligadas las empresas de servicio público, establecimientos de crédito, las entidades que exploten redes y presten servicios de comunicaciones electrónicas, empresas de servicios de inversión, reguladas por la legislación del Mercado de Valores, entre otras.

Es necesario tener en cuenta que la mayor novedad que homologa al Reglamento (UE) 2016/679 es la evolución de un modelo basado, fundamentalmente, en el control del cumplimiento a otro que descansa en el principio de **responsabilidad activa**, lo que exige una previa valoración por el responsable o por el encargado del tratamiento del riesgo que pudiera generar el tratamiento de los datos personales para, a partir de dicha valoración, adoptar las medidas que procedan.

4.2.2.3.1. DE LOS CÓDIGOS DE CONDUCTA Y CERTIFICACIONES

Como se ha definido acorde al reglamento europeo, un código de conducta es un documento redactado voluntariamente por una empresa en el que se exponen una serie de principios que se compromete unilateralmente a seguir. En el párrafo tercero del numeral 2 del artículo 38 de la LOPD expresa que, los responsables o encargados del tratamiento que se adhieran al

código de conducta se obligan a someter al organismo o entidad de supervisión las reclamaciones que les fueran formuladas por los afectados en relación con los tratamientos de dato, debiendo la autoridad de protección de datos de España verificar que los organismos o entidades que promuevan los códigos de conducta han dotado a estos códigos, estos códigos son aprobados por la Agencia Española de Protección de Datos .

4.2.2.3.2. AUTORIDADES DE PROTECCIÓN DE DATOS

El Título VII se dedica a las autoridades de protección de datos, que siguiendo el mandato del Reglamento (UE) 2016/679 se han de establecer por ley nacional. Manteniendo el esquema que se venía recogiendo en sus antecedentes normativos, la ley orgánica regula el régimen de la **Agencia Española de Protección de Datos (AEPD)** y refleja la existencia de las autoridades autonómicas de protección de datos y la necesaria cooperación entre las autoridades de control.

Según el artículo 44 de la LOPD, la Agencia Española de Protección de Datos es una autoridad administrativa independiente de ámbito estatal, con personalidad jurídica y plena capacidad pública y privada, que actúa con plena independencia, como función principal se estableció, supervisar la aplicación de la LOPD y el RGPD (Reglamento 2016/679); presidida por la Presidencia de la Agencia Española, quien la representa, asesorada por el Consejo Consultivo compuesto por un diputado, Senador, representantes del Poder Judicial, Comunidad Autónoma, entre otros.

Asimismo, las autoridades estatales, administraciones públicas, incluidas las tributarias y de la Seguridad Social, y los particulares están obligados a proporcionar a la Agencia Española de Protección de Datos los datos, informes, antecedentes y justificantes necesarios para llevar a cabo su actividad de investigación.

Por último, defiende la Agencia Española de Protección de Datos y la jurisprudencia existente en la materia desde las tres perspectivas implicadas y que podrían sintetizarse en el cumplimiento de los siguientes extremos:

- **Desde un punto de vista jurídico.** Principio de calidad, deber de información, obtención del consentimiento, deber de secreto, regulación de encargos del tratamiento/prestaciones de servicio sin acceso a datos/cesiones de datos, cumplimiento de requisitos ante transferencias internacionales y atención de derechos.
- **Desde un punto de vista técnico.** Acopio de medidas de seguridad en tratamiento de datos en sistemas automatizados y en soporte.
- **Desde un punto de vista organizativo**. Documentación e implantación de políticas, procedimientos, protocolos y directrices corporativas de actuación en relación al cumplimiento de los principios que establece la normativa de protección de datos personales.

4.2.2.3.3. DE LAS RESPONSABILIDAD Y SANCIONES

En el artículo 82 del RGPD se establece que el responsable o el encargado del tratamiento tiene que indemnizar los daños y perjuicios que pueda sufrir una persona como consecuencia de una infracción a las prerrogativas consignadas en el Reglamento (artículo 82.1 RGPD), es decir cualquier responsable que participe en la operación de tratamiento de datos y que no haya cumplido con las obligaciones que demanda el RGPD, responderá por los daños causados. Sin embargo, quedarán exento de responsabilidad si se demuestra que no es en modo alguno responsable de los hechos que hayan causado los daños. (artículo 82.3 RGPD). Por ende, si el encargado o responsable del tratamiento a cumplido con las medidas técnicas y organizativas establecidas en el RGPDP para el tratamiento de los datos personales, quedará exento de responsabilidad en caso exista alguna infracción.

El Título IX, que contempla el régimen sancionador, parte de que el Reglamento (UE) 2016/679 establece un sistema de sanciones o actuaciones correctivas que permite un amplio margen de apreciación. En este marco, la LOPDPGDD procede a describir las conductas típicas, estableciendo la distinción entre infracciones muy graves, graves y leves, tomando en consideración la diferenciación que el Reglamento general de protección de datos establece al fijar la cuantía de las sanciones hasta un máximo de 20.000.000 EUR según la infracción, y hasta un porcentaje (si se trata de una empresa) del 4% del negocio total anual global del ejercicio financiero anterior. Siendo sujetos al régimen sancionador, los responsables, encargados y representantes del tratamiento de los datos, entidades de certificación y supervisión de códigos de conducta. Concerniente a la investigación corresponde determinar que infracciones constituyen **infracciones muy graves, graves y leves.**

Para que se configure una infracción **grave**, deberá encontrarse una vulneración a los principios y garantías establecidas en el artículo 5 del reglamento, siendo los más importantes **la afectación a la licitud, transparencia y responsabilidad en el manejo de los datos,** también cuando afecte a los principios de integridad, confidencialidad; se debe recordar que el responsable del tratamiento será responsable del cumplimiento de lo dispuesto en la LOPD y reglamento, y ser capaz de demostrarlo.

Como infracciones **muy graves** se tiene las que sancionan a la entidad o responsable del tratamiento, cuando éstos no han adoptado medidas organizativas, diligentes y técnicas en la organización y en el mando de sus trabajadores, los mismos que están comprendidos en el artículo 73 de la LOPDPGDD, a continuación, a efectos de la investigación mencionaré los más concernientes:

- La falta de adopción de medidas técnicas y organizativas que resulten apropiadas para aplicar de forma efectiva los principios de protección de datos desde el diseño, así como la no integración de las garantías necesarias en el tratamiento, en los términos exigidos por el artículo 25 del Reglamento (UE) 2016/679.

- La falta de adopción de las medidas técnicas y organizativas apropiadas para garantizar que, por defecto, solo se tratarán los datos personales necesarios para cada uno de los fines específicos del tratamiento, conforme a lo exigido por el artículo 25.2 del Reglamento (UE) 2016/679.

- La falta de adopción de aquellas medidas técnicas y organizativas que resulten apropiadas para garantizar un nivel de seguridad adecuado al riesgo del tratamiento, en los términos exigidos por el artículo 32.1 del Reglamento (UE) 2016/679.

- El quebrantamiento, como consecuencia de la falta de la debida diligencia, de las medidas técnicas y organizativas que se hubiesen implantado conforme a lo exigido por el artículo 32.1 del Reglamento (UE) 2016/679.

- El incumplimiento de la obligación de designar un representante del responsable o encargado del tratamiento no establecido en el territorio de la Unión Europea, conforme a lo previsto en el artículo 27 del Reglamento (UE) 2016/679.

- La falta de atención por el representante en la Unión del responsable o del encargado del tratamiento de las solicitudes efectuadas por la autoridad de protección de datos o por los afectados.

- El incumplimiento de la obligación de designar un delegado de protección de datos cuando sea exigible su nombramiento de acuerdo con el artículo 37 del Reglamento (UE) 2016/679 y el artículo 34 de esta ley orgánica.

- **No posibilitar la efectiva participación del delegado de protección de datos en todas las cuestiones relativas a la protección de datos personales,** no respaldarlo o interferir en el desempeño de sus funciones y la falta de adopción por parte de los organismos acreditados de supervisión de un código de conducta de las medidas que resulten oportunas en caso que se hubiera producido una infracción del código.

Por último, constituyen **faltas leves:**

- Facilitar información inexacta a la Autoridad de protección de datos, en los supuestos en los que el responsable del tratamiento deba elevarle una consulta previa, conforme al artículo 36 del Reglamento (UE) 2016/679.

- No publicar los datos de contacto del delegado de protección de datos, o no comunicarlos a la autoridad de protección de datos, cuando su nombramiento sea exigible de acuerdo con el artículo 37 del Reglamento (UE) 2016/679 y el artículo 34 de esta ley orgánica.

- El incumplimiento por parte de los organismos acreditados de supervisión de un código de conducta de la obligación de informar a las autoridades de protección de datos acerca de las medidas que resulten oportunas en caso de infracción del código, conforme exige el artículo 41.4 del Reglamento (UE) 2016/679.

- La no adhesión de los códigos de conducta en virtud del artículo 40 o aplicar mecanismos de certificación aprobados con arreglo al artículo 42.

La categorización de las infracciones se introduce a los solos efectos de determinar los plazos de prescripción, teniendo la descripción de las conductas típicas como único objeto la enumeración de manera ejemplificativa de algunos de los actos sancionables que deben entenderse incluidos dentro de los tipos generales establecidos en la norma europea. La ley orgánica regula los supuestos de interrupción de la prescripción partiendo de la exigencia constitucional del conocimiento de los hechos que se imputan a la persona, pero teniendo en

cuenta la problemática derivada de los procedimientos establecidos en el Reglamento Europeo.

4.2.3. DEL TRATAMIENTO DE DATOS EN ARGENTINA

En REBOLLO & SALTOR (2013) se hace referencia que en la Ley 25.326 "Ley de Protección de Datos Personales", (en adelante, la LPDPA) se sigue la lógica de determinados principios, según los cuales los registros deben obtener los datos por medios lícitos y usarlos para fines determinados a priori, con el cuidado de mantener la fidelidad de los datos, respetando la prohibición de suministrar datos a terceros cuando no existiera conformidad del interesado o en casos que encuadren en excepciones especiales.

El artículo 1 de la LPDPA señala que la misma tiene por objeto la protección integral de los datos personales asentados en archivos, registros, bancos de datos, u otros medios técnicos de tratamiento de datos, sean estos públicos, o privados destinados a dar informes, para garantizar el derecho al honor y a la intimidad de las personas, así como también el acceso a la información que sobre las mismas se registre.

Cabe destacar que las disposiciones de la ley no sólo se aplican a los datos relativos a las personas físicas, sino también, en cuanto resulte pertinente, a los relativos a **las personas de existencia ideal.** En cuanto al ámbito de aplicación, la ley Argentina destina el tratamiento en los archivos, registros, bancos de datos, u otros medios técnicos de tratamiento de datos, sean éstos públicos, o privados destinados a dar informes sin mencionar la sede de su establecimiento ni el lugar en el que se lleva a cabo el tratamiento de datos como criterio para su aplicación territorial.

4.2.3.1. PRINCIPIOS FUNDAMENTALES DE LA PROTECCIÓN DE DATOS.

Los principios generales de la protección de datos son los que definen las pautas encaminadas a garantizar tanto la veracidad de la información contenida en los datos almacenados en los archivos, registros, bancos o bases de datos, cuanto la congruencia y la racionalidad de la utilización de los mismos.

Contenidos fundamentalmente en el Capítulo II de la LPDPA, pero rectores de todo su articulado, pueden reducirse a los siguientes:

- **Principio de pertinencia.** También conocido como principio de proporcionalidad y calidad de los datos, este principio exige que los datos que se recaben y almacenen en una base de datos sean pertinentes y adecuados, es decir, que estén relacionados con el fin perseguido en el momento de creación de la base de datos.

- **Principio de finalidad.** Este principio, engloba a los de pertinencia y utilización no abusiva, implica que los datos de carácter personal que sean recabados para incorporarse a una base de datos deben tratarse con un objetivo específico que debe conocerse antes de la creación de la base misma e informarse en el momento en el que la información personal es recolectada.

- **Principio de utilización no abusiva.** El artículo 4.3 incorpora este principio diciendo que los datos objeto de tratamiento no pueden ser utilizados para finalidades distintas o incompatibles con aquéllas que motivaron su obtención.

- **Principio de exactitud.** Los incisos 4 y 5 del artículo 4 establecen que los datos deben ser exactos y actualizarse en el caso de que ello fuere necesario y que los datos total o parcialmente inexactos, o que sean incompletos, deben ser suprimidos y sustituidos, o en su caso completados, por el responsable del archivo o base de datos cuando se tenga conocimiento de la inexactitud o carácter incompleto de la información de que se trate.

- Principio de derecho al olvido. Íntimamente relacionado con el principio de exactitud se encuentra este principio, también conocido como principio de limitación en el tiempo, implica que los datos deben desaparecer del archivo o base de datos una vez que se haya cumplido el fin para el que fueron recabados.

- Principio de legalidad. También conocido como principio de limitación de la recolección, establece que el procedimiento de recogida de datos no debe ser realizado en forma ilícita o desleal.

- Principio de publicidad. El artículo 21 establece que todo archivo, registro, base o banco de datos público, y privado destinado a proporcionar informes debe inscribirse en el Registro que al efecto habilite la Dirección Nacional de Protección de Datos Personales.

- Principio de control. Este principio, que la ley comentada incorpora en su artículo 29, se refiere a la existencia de un organismo de control responsable del cumplimiento efectivo de los principios contenidos en la legislación.

- Principio de seguridad. Una de las cuestiones que más preocupan en el tratamiento de datos en general, y de los datos personales en particular, es el de su seguridad, tanto en el momento de su recolección como en el de su tratamiento y cesión a terceros. Es por ello que el inciso 2 del artículo 9 prohíbe que se registren datos personales en archivos, registros o bancos que no reúnan condiciones técnicas de integridad y seguridad.

- Principio del consentimiento. Como regla general, el tratamiento de datos de carácter personal requiere el consentimiento libre, expreso e informado del titular de los datos. El propósito del consentimiento requerido es el de proporcionar a la persona el derecho a elegir qué datos referidos a su persona pueden ser sujetos a tratamiento.

4.2.3.2. MEDIDAS TÉCNICAS Y SEGURIDAD

Conforme al artículo 21 de la LPDPA, todo archivo, registro, base o banco de datos público o privado deberá ser inscrito en el Registro de la Autoridad de Control, debiendo considerar con carácter obligatorio los **medios utilizados para garantizar la seguridad de los datos**, y en caso de incumplimiento dará lugar a sanciones administrativas previstas en el capítulo VI de la LPDPA.

La LPDPA nombra a una Autoridad de Control (Agencia de Acceso a la Información Pública), que deberá realizar todas las acciones necesarias para el cumplimiento del tratamiento de datos, teniendo como principales funciones, la de controlar la observancia de las normas sobre integridad y seguridad de datos, para tal efecto podrá solicitar autorización judicial para acceder a locales, equipos o programas de tratamiento a fin de verificar posibles infracciones, otra es la **imposición de sanciones administrativas** y por último, la Agencia de Acceso a la Información Pública puede controlar el cumplimiento de los requisitos y garantías que deben reunir los archivos o banco de datos privados o públicos.

Otro punto muy importante, son los criterios que debe cumplir la legislación Argentina para implementar las medidas de seguridad para el Tratamiento de Datos Personales, es así que, mediante la Resolución 47/2018, regula las medidas técnicas de seguridad en medios informáticos y no informáticas, cuyo cumplimiento es voluntario.

Por último, la imposición de códigos de conducta, las asociaciones o entidades representativas de responsables o usuarios de bancos de datos de titularidad privada podrán elaborar códigos de conducta de práctica profesional, estos códigos deberán ser inscriptos en el registro que al efecto lleve el organismo de control.

4.2.3.3. DE LAS INFRACCIONES Y SANCIONES

La LPDPA sanciona a los responsables o usuarios de bancos públicos con responsabilidad por daños y perjuicios, el Organismo de Control podrá imponer como medidas sancionatorias, apercibimientos, suspensión y multas ascendentes hasta cien mil pesos, hasta la clausura o cancelación del registro o banco de datos.

4.2.4. DEL TRATAMIENTO DE DATOS EN URUGUAY

En la Constitución del país de Uruguay, encontramos en su artículo 72° lo que se puede denominar una cláusula abierta, es decir, se deja abierta la posibilidad de incorporar más derechos mediante este artículo. La carta fundamental señala que, La enumeración de derechos, deberes y garantías hecha por la Constitución, no excluye los otros que son inherentes a la personalidad humana o se derivan de la forma republicana de gobierno.

Por su parte, a mediados del año 2008 se promulgó la Ley Nº 18.331 sobre Protección de datos personales y acción de habeas data, la misma que, en su primer artículo indica que el derecho a la protección de datos es un derecho inherente a la persona humana, por tanto, se encuentra incorporado a la Constitución Uruguaya mediante el artículo 72 de dicha carta magna.

Algunas de las principales características de esta norma es su modernidad, es garantista e incorpora a las personas jurídicas como sujetos de protección, situación distinta a lo que ocurre en las legislaciones analizadas anteriormente y, en general, en el contexto internacional. Las características antes descritas le han valido ser considerado un Estado con un nivel adecuado de protección de datos, lo que trae consigo la ventaja de ser receptor de datos por parte de los países de la Unión Europea sin mayores contratiempos ni permisos especiales.

Esto le significa una ventaja en términos de competitividad económica, pues las empresas se valen de la calificación ya señalada para realizar los flujos transfronterizos de datos necesarios en la economía globalizada actual. Lo anterior le significó ser el primer país de Latinoamérica en ser invitado a adherir el denominado Convenio 108 del Consejo de Europa, el que fue ratificado por la Ley N°19.030 del 2013.

La ley de protección de datos añade algunos conceptos, además de los habituales en este tipo de regulaciones, entre los que se encuentra el de "Disociación de datos" en que la información obtenida del tratamiento de datos no puede ser vinculada a una persona. Respecto a los principios que contiene, se encuentra el de legalidad, veracidad, finalidad, consentimiento informado, seguridad de los datos, reserva y responsabilidad.

Establece derechos como el de información frente al tratamiento de datos, es decir, el deber de informar al titular que sus datos fueron recolectados para ser tratados. También contempla el derecho de acceso, rectificación, actualización, inclusión, supresión y el derecho de impugnación de valoraciones personales. Esta norma regula especialmente ciertos tipos de datos personales como los datos sensibles, los de la salud, de las telecomunicaciones, aquellos con fines publicitarios y con fines comerciales o crediticios.

En materia de datos transfronterizos establece una regla general que prohíbe la entrega de datos a estados que no ofrezcan un nivel adecuado de protección de datos, sin embargo, establece una serie de excepciones como la cooperación judicial internacional o el consentimiento del interesado, todos estos principios son homologados de acuerdo al Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo.

En cuanto a la regulación del tráfico de datos, se realiza de forma distinta, respecto a las bases de datos públicas y las privadas, dota a las primeras de excepciones al derecho de acceso, rectificación y cancelación. Mientras que para ambas existe un deber de ser

incorporadas a un registro que lleva el órgano de control. Igualmente crea un órgano o autoridad de control de datos personales, denominada Unidad Reguladora y de Control de Datos Personales. Se crea un consejo consultivo y se establecen las funciones que debe desempeñar este órgano, además de otros aspectos orgánicos. Señala que la infracción de la norma conlleva una sanción que puede fluctuar desde una observación, apercibimiento, multa de hasta 500.000 unidades indexadas, la suspensión de la base de datos respectiva por el plazo de cinco días, hasta la clausura de la misma.

Como característica de esta regulación es que incorpora el procedimiento llamado habeas data, el que procedería bajo la hipótesis de una situación de error, falsedad, prohibición de tratamiento, discriminación o desactualización. Y esta acción judicial puede conducir a exigir su rectificación, inclusión, supresión o lo que entienda corresponder, respecto a los datos en cuestión (ARRAYET, 2016).

4.2.5. ANÁLISIS COMPARATIVO

4.2.5.1. DEL IT COMPLIANCE, PRIVACIDAD Y PROTECCIÓN DE DATOS EN LA UNIÓN EUROPEA, ESPAÑA Y PERÚ

En Europa existe una alta tendencia a exigir legalmente a las empresas la **implementación de programas de cumplimiento normativo en el tratamiento de los datos**, esto se debe al trato diferenciado e irregular que se ha establecido en los países miembros de la Unión Europea, hasta la promulgación del Reglamento 2016/679. Por otro lado, el Perú no ha sido ajeno a la tendencia internacional antes señalada, ha desarrollado un sistema de responsabilidad administrativa y normas sectoriales relacionadas a la protección de los datos, las cuales pondremos en contraste a continuación:

4.2.5.1.1. DE LOS PRINCIPIOS Y OBLIGACIONES

Como se ha mencionado en la presente investigación, el principio de seguridad constituye uno de los principales lineamientos que la empresa debería adoptar en el manejo de protección de la privacidad y protección datos personales. La Unión Europea establece el principio de integridad y confidencialidad, cuya principal función es garantizar una seguridad adecuada a los datos personales, mediante la aplicación de medidas técnicas u organizativas; estas disposiciones son contenidas en el capítulo II del Reglamento (UE) 2016/679, (en adelante, RGPD), por tanto, obliga a los estados miembros de Europa a homologar sus prerrogativas legales.

En ese sentido la Legislación Española, en mérito a lo establecido en el artículo 99 del RGPD adopta sus disposiciones legales, dando origen a la Ley Orgánica 3/2018, (en adelante, LOPDPGD), si bien es cierto no lo expresa taxativamente como la RGPD, lo prescribe en el artículo 8 de la LOPDPGD, al imponer en su aplicación condiciones especiales al tratamiento de datos, es decir que el responsable del tratamiento adopte medidas técnicas y organizativas a fin de garantizar la seguridad en el tratamiento. Además, en cuanto al principio de confidencialidad (art. 5), establece que los responsables y encargados del tratamiento, así como todas las personas que intervengan, estarán obligadas a mantener en reserva la información tratada, por ejemplo, en el artículo 24.3 de la LOPDPGD, obliga la adopción de medidas necesarias para preservar la identidad y garantizar la confidencialidad de los datos correspondientes al tratamiento de los sistemas de información de denuncias internas.

En nuestra legislación, el principio de seguridad lo encontramos en el artículo 09 de la Ley General de Protección de Datos, “Ley N° 29733” (en adelante, LGPD) y el artículo 10 del Reglamento de la Ley de Protección de Datos Personales (en adelante, el Reglamento),

los cuales obligan al titular del banco de datos personales y al encargado del tratamiento, la adopción de medidas técnicas, organizativas y legales para garantizar la seguridad de los datos personales.

De lo descrito anteriormente, se puede apreciar que nuestra legislación aparentemente homologa la legislación Europea, al determinar las responsabilidades del titular del banco de datos y encargado del tratamiento, sin embargo, la Unión Europea establece el principio de **"responsabilidad proactiva",** el cual denomina al responsable del tratamiento como responsable del cumplimiento de la licitud, transparencia, lealtad, exactitud, integridad, confidencialidad y la adopción de medidas técnicas y organizativas **con la capacidad de demostrarlo.** En la RGPD se hace referencia a dos principios para la implementación efectiva de la **responsabilidad proactiva como son los de protección de datos desde el diseño y protección de datos por defecto, ambos lo veremos en el sub capítulo 4.5.1.2.**

4.2.5.1.2. DE LAS MEDIDAS DE SEGURIDAD

RESPECTO A LA LEGISLACIÓN EUROPEA

El RGPD atribuye, en determinadas condiciones, al responsable y encargado del tratamiento la aplicación de medidas técnicas y organizativas apropiadas, que se revisarán y actualizarán cuando sea necesario, a fin de garantizar y poder demostrar que el tratamiento es conforme a derecho, por ejemplo, la aplicación por parte del responsable del tratamiento, de políticas de protección de datos, entre otros. Para demostrar el cumplimiento de las obligaciones se menciona en la RGPD expresamente la adhesión a códigos de conducta o algún mecanismo de certificación que acredite las buenas prácticas corporativas, en mérito a lo dispuesto en el artículo 41 del RGPD, el cumplimento de los códigos de conducta será supervisado por la Autoridad de Control. (Esta obligación no se encuentra regulada en la legislación peruana).

Asimismo, la RGPD prescribe deberes obligatorios para el responsable y encargado del tratamiento bajo sanción en caso de incumplimiento, los cuales veremos a continuación:

- Deber de protección de datos desde el diseño, tiene como objetivo cumplir los requisitos definidos en el RGPD y, por tanto, los derechos de los interesados y busca que la protección de datos se encuentre presente en las primeras fases de concepción de un proyecto. (Éste deber no está contenido en nuestra legislación).

- Deber de protección de datos por defecto, se refiere a que sólo sean objeto de tratamiento los datos personales que sean estrictamente necesarios para cada uno de los fines de tratamiento. (Éste deber no está contenido en nuestra legislación).

- Deber de cooperación con la autoridad de control, los responsables y encargados están obligados a facilitar la información para investigaciones o cuando sean requeridos por la autoridad competente.

- Deber de registro de las actividades del tratamiento, los responsables deben documentar todas las operaciones del tratamiento, es decir debe existir un registro respecto de cada actividad del tratamiento realzado, por ejemplo, los fines, categoría de los datos, trasferencias internacionales, las medidas técnicas y organizativas adoptadas, entre otros). Este deber no se encuentra establecido en nuestra legislación, de acuerdo a la Directiva de protección de datos del Perú, no obliga al titular del banco de datos o encargado del tratamiento a registrar las medidas de seguridad implementadas o transferencias internacionales realizadas, siendo hitos importantes de garantía en la protección de datos.

- Deber de información y de transparencia, establece que se debe facilitar a los interesados la información sobre el tratamiento de sus datos personales en el momento en que se obtengan de ellos.

- **Deber de seguridad en el tratamiento**, en caso se advierta una brecha en la seguridad del tratamiento, el responsable o encargado del manejo de los datos, deberá comunicar inmediatamente la Autoridad de Control y al afectado, bajo sanción. En la legislación peruana se impone la obligación de que todo evento que afecte al tratamiento **sea reportado al encargado del tratamiento o titular del banco de datos**, sin embargo, no adopta como medida de seguridad, el deber de informar posibles infracciones en el tratamiento al afectado y a la Autoridad Nacional de Protección de Datos.

- **Deber de evaluación del impacto,** cuando exista probabilidad que un tipo de tratamiento alcance un alto riesgo para los derechos y libertades de las personas físicas, el responsable y encargado del tratamiento deberá realizar una evaluación del impacto de las operaciones de tratamiento en la protección de datos personales. La evaluación deberá contener como mínimo: **(i)** una descripción sistemática de las operaciones del tratamiento, **(ii)** una evaluación de interés y la proporcionalidad de las operaciones del tratamiento con respecto a su finalidad, **(iii) evaluación de los riesgos** y **(iv)** medidas de seguridad y mecanismos que garanticen la protección de datos personales.

El cumplimiento de los códigos de conducta se tendrá en cuenta para evaluar las operaciones de tratamiento realizado por los responsables o encargados, en particular para la evaluación del impacto. La LOPDPGD de España, lo introduce como una obligación propia del responsable y encargado del tratamiento que con fines de garantizar y acreditar su cumplimiento deben realizar la evaluación del impacto, para ello debe consultar a la Autoridad de Control su aplicabilidad (si es necesario o no).

La legislación peruana no ha implementado este deber en la LOPD y su Reglamento, si bien es cierto la Directiva de Protección de Datos Personales establece obligatoriamente la adopción de criterios de seguridad tales como adoptar un **enfoque de riesgos** para las

categorías de tratamiento intermedio, complejo y crítico; dicho criterio no está plenamente determinado ni es obligatorio, es decir no aclara ni especifica si las medidas están orientadas a determinar el impacto en la aplicación de las medias técnicas y organizativas, o si delimita los riesgos para los derechos y libertades de las personas, siendo sólo un apéndice del **deber de evaluación del impacto**, contenido en el RGPD.

- De la introducción del Delegado de Protección de Datos (en adelante, DPD), en el artículo 37 de la RGPD (Unión Europea) y artículo 34 de la LOPDPGD (España), se ha establecido la designación de una Delegado de Protección de Datos, que es una figura diferente al responsable y encargado del tratamiento, siendo un asesor legal de la entidad, intermediaria con la Autoridad de Control, desempeñará sus funciones prestando la debida atención a los riesgos asociados a las operaciones de tratamiento, teniendo en cuenta la naturaleza, el alcance, el contexto y fines del tratamiento.

Las funciones que se le encomiendan, son: **(i)** informar y asesorar al responsable o encargado del tratamiento, **(ii)** supervisar el cumplimiento de la legislación y políticas de privacidad con especial atención a los riesgos asociados a las actividades que llevará a cabo la entidad, **(iii)** ofrecer asesoramiento que se le solicite acerca de la evaluación del impacto, **(iv)** cooperar con la autoridad de control, **(v)** actuar como punto de contacto con la autoridad de control. La designación del DPD es obligatorio cuando **(a)** el tratamiento lo lleve a cabo una autoridad u organismo público, **(b)** cuando el tratamiento exija una observancia habitual y sistemática de los interesados a gran escala y **(c)** cuando el tratamiento se de en categorías especiales de tratamiento. **(Figura no contemplada en el Perú, cuyo análisis se verá en los siguientes párrafos).**

RESPECTO A LA LEGISLACIÓN PERUANA

En materia de protección de datos personales, se ha establecido requisitos y medidas de seguridad de cumplimiento obligatorio bajo sanción, dependiendo la categoría en la que se encuentren (de básico, simple, intermedio, complejo y crítico), para ello se considerará el volumen de registros, número de datos, periodo de tiempo para la finalidad del tratamiento de datos personales, la titularidad del banco de datos personales, finalidad del tratamiento de datos personales, multiplicidad de localizaciones y tratamiento de datos sensibles.

Dentro de la Directiva de Protección de Datos se exige la implementación de tres tipos de medidas de seguridad: **medidas organizativas** (estructura organizacional con roles y responsabilidades), **jurídicas** (mantener los formatos de consentimiento para el tratamiento de datos personales, adecuados y con la finalidad prevista en la norma) y **técnicas** (medios utilizados en la forma y utilización de la información y datos personales), éstas últimas deberán estar dirigidas a prevenir y reaccionar frente a pérdida, alteración o tratamiento no autorizado de datos personales.

Además, prescribe la Directiva al titular del banco de datos que designe un **responsable de seguridad** para la aplicación de las medidas y políticas antes descritas, algunos manifiestan que es similar a un **Delegado de Protección de Datos,** sin embargo en el **Perú no se ha implementado tal figura, si bien es cierto el responsable de seguridad, es la persona encargada de velar por el correcto cumplimiento de las medidas de seguridad, sin embargo, la diferencia más notoria entre el Responsable de Seguridad y el Delegado de Protección de Datos es la exclusividad de éste último en sus funciones, el (DPD) ya no será como hasta ahora la persona que se designaba como Responsable de Seguridad, ocurriendo que, sin apenas justificación, se elegía al informático o se autonombraba a cualquier administrativo a cumplir con la LPDP en la empresa, es por**

ello que esta nueva figura supone reforzar la cultura del compliance en materia de protección de datos (Lambert, 2016).

Por último, el artículo 31 de la LPDP establece que los titulares de los bancos de datos o encargados implementen elaboren códigos de conducta, el mismo que deberá estar inscrito en el Registro Nacional de Protección de Datos, bajo sanción en caso de incumplimiento.

4.2.5.1.3. DE LA RESPONSABILIDAD Y SANCIONES

LEGISLACIÓN EUROPEA

En el artículo 82 del RGPD se establece que el responsable o el encargado del tratamiento tiene que indemnizar los daños y perjuicios que pueda sufrir una persona como consecuencia de una infracción a las prerrogativas consignadas en el Reglamento (artículo 82.1 RGPD), es decir cualquier responsable que participe en la operación de tratamiento de datos y que no haya cumplido con las obligaciones que demanda el RGPD, responderá por los daños causados. Sin embargo, quedarán exento de responsabilidad si se demuestra que no es en modo alguno responsable de los hechos que hayan causado los daños. (artículo 82.3 RGPD). Por ende, si el encargado o responsable del tratamiento a cumplido con las medidas técnicas y organizativas establecidas en el RGPDP para el tratamiento de los datos personales, quedará exento de responsabilidad en caso exista alguna infracción.

Asimismo, prescribe que cada autoridad de control impondrá multas administrativas por la comisión de infracción del RGPD, además, en el artículo 83 del RGPD establece **condiciones generales** para la imposición de multas administrativas, estos criterios determinarán la cuantía de las multas, por ejemplo: **(i)** la naturaleza, gravedad y duración de la infracción, **(ii)** intencionalidad o negligencia en la infracción, **(iii) las medidas que optó el responsable o encargado del tratamiento para mitigar los daños y perjuicios, (iv) el**

grado de aplicabilidad de las medidas técnicas y organizativas (de diseño y por defecto, y medidas de protección) optadas por el responsable o encargado del tratamiento, (v) el grado de cooperación con la autoridad de control con el fin de poner remedio a la infracción, **(vi)** si el responsable o encargado notificaron a la autoridad de control y afectado cualquier brecha de seguridad al tratamiento de datos, **(vii)** la adhesión de códigos de conducta y **(viii)** cualquier otro factor agravante o atenuante aplicable a las circunstancias del caso, como los beneficios financieros obtenidos o las pérdidas evitadas, directa o indirectamente, a través de la infracción.

Las multas que impone el RGPD, no son clasificadas de leves a graves como lo hace la legislación española o peruana, diferenciándose de esta última en la cuantía, pues esta asciende hasta un máximo de 20 000 000 EUR como multas administrativas o, de una cuantía equivalente al 4% como máximo del volumen del negocio total anual global del ejercicio anterior, optándose por la de mayor cuantía; es necesario mencionar que la imposición de multas se hará evaluando cada caso individualmente, es decir si un banco de datos de 50 personas y otro de un millón cometen la misma infracción, no se les impondrán el mismo quantum.

A modo ejemplificativo, se impondrá hasta un máximo de 20 000 000 EUR si el encargado o responsable ha incumplido con implementar y adaptar en el tratamiento los principios básicos (licitud, transparencia, seguridad, entre otros), requeridos por la autoridad. La legislación española, mediante la LOPDPGD adoptó los criterios y condiciones generales para la imposición de multas, establecidas por Unión Europea. Para ello, estableció tres tipos de infracciones, (leves, graves y muy graves), describiré brevemente las más resaltantes para la presente investigación.

- Infracciones leves: éstas prescriben en un (01) año y las constituyen, **(i)** cuando el responsable o encargado no registra o documenta cualquier violación de seguridad al tratamiento de datos; **(ii)** el incumplimiento de los organismos acreditados de supervisión de un código de conducta de la obligación de informar a las autoridades de protección de datos acerca de las medidas que resulten oportunas en caso de infracción del código (art. 74 de la LOPDPGD).

- Infracciones graves: éstas prescriben en dos (02) años y las constituyen:

(i) la falta de adopción de medidas técnicas y organizativas que resulten apropiadas para aplicar en el tratamiento de protección de datos, así como no integrar garantías necesarias en el tratamiento (Protección de datos desde el diseño y por defecto); **(ii)** no adoptar medidas técnicas y organizativas necesarias para garantizar un nivel adecuado de seguridad en el tratamiento; **(iii)** el incumplimiento de la obligación de designar un representante del responsable o encargado del tratamiento no establecido en la Unión Europea; **(iv)** encargar el tratamiento de datos a un tercero sin la previa formalización de un contrato u otro acto jurídico escrito con el contenido exigido por el artículo 28.3 del RGPD; **(v)** no disponer del registro de actividades del tratamiento, **(vi)** el incumplimiento del deber del encargado del tratamiento de notificar al responsable del tratamiento las violaciones de seguridad; **(vii)** el incumplimiento del deber de notificación a la autoridad de protección de datos de una violación de seguridad de datos; **(viii)** el incumplimiento de comunicar al afectado cualquier incidencia o violación de seguridad de sus datos; **(ix)** realizar el tratamiento de datos personales sin haber llevado a cabo la evaluación del impacto de las operaciones de tratamiento, **(x)** el incumplimiento de designar un delegado de protección de datos cuando sea exigible (art. 34 LPPDPGD) y **(xi)** la falta de adopción por parte de los organismos

acreditados de supervisión de un código de conducta de las medidas que resulten oportunas en caso se hubiera producido una infracción al código.

- Infracciones muy graves: éstas prescriben a los tres (03) años y las constituyen, **(i)** la vulneración a los principios y garantías establecidas en el artículo 5 del RGPD (transparencia, licitud, seguridad, finalidad, responsabilidad proactiva, entre otros), **(ii)** el tratamiento de datos personales (sensibles, étnicos, opiniones políticas, datos genéticos) sin adoptar las medidas de seguridad apropiadas; **(iii)** el incumplimiento del deber de información al afectado del tratamiento de sus datos; **(iv)** la transferencia internacional de datos personales a un destinatario que se encuentre fuera del territorio español que no cumplan con las garantías, requisitos mínimos de seguridad establecidas en la LPPDPGD Y RGPDP.

LEGISLACIÓN PERUANA

La legislación peruana ha incorporado como órgano sancionador y fiscalizador a la Autoridad Nacional de Protección de Datos Personales, la misma que está facultada para imponer sanciones por infracciones leves, graves o muy graves con una multa hasta cien (100) unidades impositivas tributarias (UIT), diferenciándose sustancialmente del ordenamiento jurídico europeo al momento de establecer el quantum máximo de la multa, que es 20 000 000 EUR.

De acuerdo al reglamento, se considera **infracción leve** cuando, **(i)** el titular del banco de datos de la entidad ha realizado el tratamiento de datos personales incumpliendo las medidas de seguridad establecidas en la LPDP (adoptar medidas técnicas y organizativas), **(ii)** cuando se recopile datos personales que no sean necesarios, adecuados ni pertinentes y **(iii)** no inscribir ni actualizar en el Registro Nacional los actos establecidos en el artículo 34 de la LOPD (por ejemplo, la inscripción y actualización de los códigos de conducta).

Se consideran **infracciones graves, (i)** realizar el tratamiento de datos personales sensibles incumpliendo las medidas de seguridad establecidas en la normativa de protección de datos y **(ii)** incumplir la obligación de confidencialidad**.** Por último, son **infracciones muy graves**, **(i)** dar tratamiento a los datos personales contraviniendo las obligaciones contenidas en la LPDP y su Reglamento, **(ii)** Recopilar datos personales mediante medios fraudulentos, desleales o ilícitos y **(iii)** no cumplir con las medidas correctivas establecidas por la Autoridad como resultado de un procedimiento trilateral.

Conforme al artículo 126 de la LPDP, se considerará atenuantes cuando la entidad ha colaborado con las acciones de la Autoridad Nacional de Protección de Datos Personales y ha optado por el reconocimiento de las infracciones, ello permitirá la reducción motivada de la sanción por debajo del rango previsto en las disposiciones legales.

Asimismo, se configurará una responsabilidad civil del titular del banco de datos personales por la pérdida, alteración o un uso de los datos personales contrario a la a las disposiciones vigentes, estando obligado a indemnizar por los daños y perjuicios al titular de los datos personales, además la Autoridad de Protección de Datos podrá imponer multas coercitivas frente al incumplimiento de las obligaciones accesorias de la sanción.

4.2.5.2. DEL IT COMPLIANCE, PRIVACIDAD Y PROTECCIÓN DE DATOS EN URUGUAY Y PERÚ

4.2.5.2.1. DE LOS PRINCIPIOS Y OBLIGACIONES

LEGISLACIÓN URUGUAYA

Según la Ley N° 18.331 “Protección de Datos Personales y Acción de “Habeas Data”, (en adelante, PDPAHD), se aplica a las personas físicas, y por extensión a las personas jurídicas, en cuanto corresponda, a estas últimas no se les aplica la caducidad o prescripción de los datos. En la PDPAHD vemos diferentes principios muy similares a la legislación española y

peruana, tales como el de reserva, veracidad, finalidad, consentimiento, legalidad y seguridad de los datos, éste último principio merece ser tratado porque obliga al responsable o usuario de la base de datos a adoptar todas las medidas que resulten necesarias para garantizar la seguridad y confidencialidad de los datos personales, por ejemplo, evitar su adulteración, pérdida o tratamiento no autorizado.

El siguiente principio es el de responsabilidad (sustituyendo a la anterior disposición mediante la Ley N° 19670), consiste en que el responsable de la base de datos o tratamiento y el encargado, en su caso, serán responsables de la violación de las disposiciones de la PDPAHD, además, en ejercicio de una responsabilidad proactiva, deberán adoptar las medidas técnicas y organizativas apropiadas a fin de garantizar un tratamiento adecuado de los datos personales y **demostrar su efectiva implementación.** (con esta modificación el tratamiento de los datos personales en Uruguay homologa sistemáticamente a las disposiciones establecidas en el RGPD de la Unión Europea).

Al igual que la RGPD de la Unión Europea y la LOPDPGDD de España incorporan el principio de **responsabilidad proactiva**, **el deber de adoptar la privacidad desde el diseño, por defecto, análisis de riesgos a fin de ejercer y demostrar proactividad para la prevención de los incidentes de seguridad, elevando así su responsabilidad y la posibilidad de recibir sanciones.** El responsable por las infracciones a las disposiciones de la ley es la persona física o jurídica, pública o privada propietaria de la base de datos o que decida sobre la finalidad, contenido y uso del tratamiento según lo establecido en los artículos 4º lit. K) y 12 de la Ley Nº 18.331.

Por último, de acuerdo a lo dispuesto por la ley N° 19670 se incorpora la ampliación del ámbito de aplicación de la ley de protección de datos personales, quiere decir que la PDPAHD regirá también fuera de las fronteras del país en caso de que las actividades del

tratamiento están relacionadas con la oferta de bienes y servicios dirigidos a habitantes de Uruguay o que involucren el análisis de su comportamiento, o si así lo disponen normas de derecho internacional o un contrato (art. 37).

4.2.5.2.2. DE LAS MEDIDAS DE SEGURIDAD

Al igual que el ordenamiento jurídico peruano, Uruguay establece que los tratamientos de los datos relativos a las telecomunicaciones deberán adoptar las medidas técnicas y de gestiones adecuadas para preservar la seguridad a fin de garantizar sus niveles de protección.

Otro punto similar a nuestra legislación, es la transferencia internacional de datos, quiere decir que el flujo de datos podrá realizarse con otro país u organismo que esté fuera del territorio uruguayo siempre y cuando proporcione niveles adecuados de protección, de acuerdo a los estándares de protección internacional. (Artículo 23 de la PDPAHD).

De acuerdo a la PDPAHD, toda base de datos pública o privada deberá ser inscrita en el Registro habilitado por el órgano de control, debiendo registrar **(i)** los procedimientos de obtención y tratamiento de los datos, **(ii)** las medidas de seguridad y descripción técnica de la base de datos, entre otros. Estas disposiciones legales son distintas a la legislación peruana, en la Directiva de Protección de Datos, únicamente obliga el registro de, **(i)** control de documentos, **(ii)** Registro de personal con acceso autorizado y **(iii)** registro de auditorías y **(iv)** registro problemas, incidentes y medidas adoptadas para su mitigación; de modo que, no se obliga que se registre las medidas de seguridad (técnicas y organizativas) que se aplican al tratamiento de datos personales y así garantizar su protección.

El órgano de control es la Agencia para el Desarrollo del Gobierno de Gestión Electrónica y la Sociedad de la Información y del Conocimiento (AGESIC), ésta última tiene la obligación de controlar la observancia de las normas sobre la integridad, veracidad y seguridad de datos por parte de los responsables de las bases de datos.

Otra inclusión en mérito a lo dispuesto por la ley N° 19670, es el deber de información, figura idéntica a la establecida por la RGPD de la Unión Europea y LOPDPGDD de España, que consiste en la obligación de informar cualquier vulneración de seguridad de la información al afectado y a la Unidad Reguladora y de Control de Datos Personales. Esta figura no está implementada la legislación peruana, porque ante cualquier vulneración lo único que se exige es comunicar al titular del banco de datos.

Respecto a los códigos de conducta, los responsables o usuarios de bancos de datos de titularidad privada podrán elaborar códigos de conducta de práctica profesional, que establezcan normas para el tratamiento de datos personales que tiendan a asegurar y mejorar las condiciones de operación de los sistemas de información en función de los principios establecidos en la PDPAHD, al igual que la legislación peruana, estos códigos deberán ser inscritos en el registro del órgano competente.

Por último, en enero del 2019, Uruguay incorporó a su ordenamiento jurídico la figura del **Delegado de Protección de Datos**, siendo de obligatorio cumplimiento por parte de las entidades públicas, estatales o no estatales, privadas total o parcialmente de propiedad estatal, así como las entidades privadas que traten datos sensibles o manejen grandes volúmenes de datos, cuyas funciones principales son:

(i) Asesorar en la formulación, diseño y aplicación de políticas de protección de datos personales; **(ii)** Supervisar el cumplimiento de la normativa de protección de datos; **(iii)** Proponer todas las medidas que entienda pertinentes para adecuarse a la normativa y a los estándares internacionales en materia de protección de datos personales y **(iv)** Actuar como nexo entre su entidad y la Unidad Reguladora y de Control de Datos Personales. El delegado deberá poseer las condiciones necesarias para el correcto desempeño de sus funciones y actuará con autonomía técnica.

4.2.5.2.3. DE LA RESPONSABILIDAD Y SANCIONES

La Agencia para el Desarrollo del Gobierno de Gestión Electrónica y la Sociedad de la Información y del Conocimiento (AGESIC), puede sancionar a los responsables de las bases de datos o encargados del tratamiento en caso que violen las normas de la PDPAHD, imponiendo, apercibimientos, multas hasta quinientas mil unidades indexadas y la suspensión de la base de datos. El monto máximo establecido por el régimen uruguayo equivale a S/. 47, 661.20 (cuarenta y siete mil seiscientos sesenta y uno con 20/100 soles), **mientras que el monto máximo de las multas en la legislación peruana es 100 cien UIT, equivalente a s/. 42, 000.00 (cuarenta y dos mil con 00/100 soles).**

4.2.5.3. DEL IT COMPLIANCE, PRIVACIDAD Y PROTECCIÓN DE DATOS EN PERÚ Y ARGENTINA

4.2.5.3.1. DE LOS PRINCIPIOS Y OBLIGACIONES

La legislación Argentina, mediante la Ley N° 25326, "Ley de Protección de los Datos Personales" (en adelante, la LPDPA), establece mecanismos técnicos y organizativos para la protección de la privacidad y datos personales. Los principios establecidos en la LPDPA son muy similares al ordenamiento jurídico peruano y europeo, algunos de estos principios están comprendidos en los capítulos internos de nuestra legislación, tales como (transferencia internacional, cesión, datos relativos a la salud, categoría de datos), pues bien, en relación a la investigación me concentraré en **los principios de seguridad de los datos y principio de transferencia.**

El primero establece que el responsable o usuario del archivo de datos deberá adoptar medidas técnicas y organizativas que garanticen la seguridad y confidencialidad de los datos personales, y prohíbe el registro de los datos personales que no reúnan las condiciones

técnicas de integridad y seguridad, a diferencia de nuestra legislación, tal prohibición no es regulada como parámetro de disciplina sino como una infracción en caso de incumplimiento.

El segundo, acorde la legislación peruana, impone que las trasferencias internacionales de los datos a países u organismos internacionales deben proporcionar niveles adecuados de protección, es decir que el país receptor debe garantizar un nivel óptimo de seguridad en el tratamiento de datos.

En cuanto al ámbito de aplicación, muy similar a nuestro ordenamiento es aplicable para todo tipo de almacenamiento de datos, sin importar el soporte, ya sea en ficheros o que estén automatizados; quedando excluidos los datos concernientes a la seguridad nacional, por competencia, condenas o infracciones penales.

4.2.5.3.2. DE LAS MEDIDAS DE SEGURIDAD

Conforme al artículo 21 de la LPDPA, todo archivo, registro, base o banco de datos público o privado deberá ser inscrito en el Registro de la Autoridad de Control, debiendo considerar con carácter obligatorio los **medios utilizados para garantizar la seguridad de los datos**, y en caso de incumplimiento dará lugar a sanciones administrativas previstas en el capítulo VI de la LPDPA. La legislación peruana adolece de esta ausencia normativa, puesto que, en la LOPD, sólo establece como objeto de inscripción al **(i)** registro o documentación de los bancos de datos de administración pública y privada, **(ii)** inscripción de códigos de conducta y **(iii)** comunicaciones referidas al flujo transfronterizo de datos personales.

La LPDPA nombra a una Autoridad de Control (Agencia de Acceso a la Información Pública), que deberá realizar todas las acciones necesarias para el cumplimiento del tratamiento de datos, teniendo como principales funciones, la de controlar la observancia de las normas sobre integridad y seguridad de datos, para tal efecto podrá solicitar autorización

judicial para acceder a locales, equipos o programas de tratamiento a fin de verificar posibles infracciones, otra es la **imposición de sanciones administrativas** y por último, la Agencia de Acceso a la Información Pública puede controlar el cumplimiento de los requisitos y garantías que deben reunir los archivos o banco de datos privados o públicos.

En este punto, una clara diferencia con la legislación peruana es que la Autoridad Nacional de Protección de Datos Personales (Perú), cumple funciones **(i)** administrativas (representativas), **(ii)** orientadoras (promover la cultura de la protección de datos personales), **(iii) normativas (promover el uso de mecanismos de autorregulación como instrumento complementario de protección de datos), (iv)** resolutivas (resolver reclamaciones, fiscalizadoras (labores de supervisión al titular y encargado del tratamiento) y **(v)** sancionadoras (imposición de multas).

Otro punto muy importante, son los criterios que debe cumplir la legislación Argentina para implementar las medidas de seguridad para el Tratamiento de Datos Personales, es así que, mediante la Resolución 47/2018, regula las medidas técnicas de seguridad en medios informáticos y no informáticas, cuyo cumplimiento es voluntario. Sin embargo, en la legislación Europea y Peruana, el incumplimiento de éstas medidas constituyen infracciones a la materia normativa de protección de datos.

Por último, la imposición de códigos de conducta, las asociaciones o entidades representativas de responsables o usuarios de bancos de datos de titularidad privada podrán elaborar códigos de conducta de práctica profesional, estos códigos deberán ser inscriptos en el registro que al efecto lleve el organismo de control. Esta imposición es idéntica al ordenamiento jurídico de España, Uruguay y Perú.

4.2.5.3.3. DE LAS INFRACCIONES Y SANCIONES

La LPDPA sanciona a los responsables o usuarios de bancos públicos con responsabilidad por daños y perjuicios, el Organismo de Control podrá imponer como medidas sancionatorias, apercibimientos, suspensión y multas ascendentes hasta cien mil pesos, hasta la clausura o cancelación del registro o banco de datos.

Tabla 1

Análisis comparativo en los sistemas jurídicos de Argentina, España, Perú y Uruguay

País	Constitución	Norma General	Principios	Sujetos	Órgano de control	Medidas de seguridad	Responsabilidad y Sanciones
Argentina	Art. 43 de la Constitución	Ley nº 25.326, sancionada en el año 2000 y reglamentada en el año 2001.	- Principio de Licitud - Principio de calidad de datos - Principio de consentimiento - Principio de información - Principio de categoría de datos - Principio de datos relativos a la salud - Principio de Seguridad de los datos - Principio de Deber de confidencialidad - Principio de cesión - Principio de transferencia internacional	- Titular de los datos - Responsable de la base de datos - Usurario de los datos	Agencia de Acceso a la Información Pública	- Implementación de medidas técnicas y organizativas - Inscripción obligatoria de los registros	- Apercibimiento - Suspensión - Cancelación de base de datos - multas de (de $1.000 a $100.000)
España	Art. 18.4 de la constitución	Homologa al Reglamento 2016/679 de la UE Ley Orgánica 3/2018, de 05 de diciembre de 2018, de Protección de Datos Personales y garantía de los derechos digitales.	- Exactitud de los datos - Deber de confidencialidad Tratamiento basado en el consentimiento del afectado - Responsabilidad Proactiva	Responsable del tratamiento. Encargado del tratamiento Delegado de Protección de datos	Agencia Española de Protección de Datos	- Medidas Técnicas - Medidas Organizativas - Cumplimiento de deberes - Deber de protección de datos desde el diseño por defecto - Deber de cooperación con la autoridad de control - Deber de documentación del tratamiento, - Deber de información y de transparencia - Deber de seguridad en el tratamiento. - Deber de evaluación del impacto - Códigos de conducta	- Leves - Graves - Muy graves - Imposición de multas hasta un máximo de 20.000.000 EUR según la infracción, y hasta un porcentaje (si se trata de una empresa) del 4% del negocio total anual global del ejercicio financiero anterior.
Perú	**Art.2.6 de la Constitución**	Ley de Protección de Datos Personales "Ley N° 29733". Reglamento aprobado mediante el Decreto Supremo N° 003-2013-JUS	- Principio de legalidad - Principio de consentimiento - Principio de finalidad - Principio de proporcionalidad - Principio de nivel de protección adecuado	Titular del banco de datos Responsable del tratamiento Encargado del tratamiento	- Autoridad Nacional de Protección de Datos (ANPD)	- Organizativas - Técnicas - Jurídicas - Implementación de códigos de conducta (voluntario) - Deber de enfoque de riesgos	Hasta 100 UIT - Leve - Grave - Muy grave
Uruguay	**Art 7**	Ley N° 18331, "Ley de Protección de Datos Personales". Ley 19670 "Aprobación de rendición de cuentas y balance de ejecución presupuestal. ejercicio 2017"	- Principio de legalidad - Principio de veracidad - Finalidad - Previo consentimiento informado - Seguridad de los datos - Reserva - Responsabilidad proactiva	- Encargado del tratamiento - Tercero - Responsable de la base de datos o del tratamiento - **Delegado de Protección de Datos**	- La Agencia para el Desarrollo del Gobierno de Gestión Electrónica y la Sociedad de la Información y del Conocimiento (AGESIC),	- Medidas técnicas y gestiones adecuadas - Inscripción de la base de datos en el registro - Inscripción de las medidas de seguridad adoptadas en el registro - Implementación de códigos de conducta - Deber de información (afectado y a la Unidad Reguladora y Control de datos personales). - Deber de protección de datos desde el diseño por defecto	- Apercibimiento - Multa hasta multas hasta quinientas mil unidades indexadas - La suspensión de la base de datos.

FUENTE: Elaborado por el equipo de trabajo en base a la legislación obtenida de la Unión Europea, España, Argentina, Uruguay y Perú.

CONCLUSIONES

PRIMERA. El panorama expuesto en líneas anteriores, nos conduce a describir el It Compliance, Privacidad y Protección de Datos como una institución que exige a las entidades públicas y privadas, la implementación de mecanismos de prevención y control en el tratamiento de datos, esto a fin de garantizar la seguridad en el manejo de la información y eximir su responsabilidad en caso se presente alguna brecha en la seguridad de la información. En efecto, es imprescindible que las empresas del sector público incorporen en su gestión el It Compliance, Privacidad y Protección de Datos bajo la supervisión de un auditor interno, aplicado al presente estudio corresponde la nominación de un Delegado de Protección de Datos.

SEGUNDA. Actualmente, en nuestra legislación existe un avance sectorial pero insuficiente en cuanto a la regulación de la seguridad de la información por parte de las personas jurídicas, debido a la ausencia de dispositivos de prevención y mecanismos de control previstos en el Perú. Al respecto, en nuestro sistema jurídico se exige a las entidades la incorporación de medidas de seguridad en el tratamiento, sin embargo, tienen carácter genérico y las recomendaciones prescritas en la Directiva de Seguridad son voluntarias, es decir que las empresas públicas no están obligadas a demostrar su implementación. Por lo que, en ausencia de estos mecanismos no se crea estímulos para que las empresas se autorregulen y propicien una cultura de cumplimiento, mediante la implementación del It Compliance, Privacidad y Protección de Datos.

TERCERA. Como resultado del análisis comparativo, determinamos que la Unión Europea mediante un sistema de autoregulación regulada exige a las entidades la adopción de programas de cumplimiento normativo, a fin de garantizar la circulación de la información y

homogenizar sus disposiciones en los países miembros. España siguiendo estas prerrogativas homogenizó estos protocolos de actuación, creando condiciones para que las empresas se autoregulen mediante la implementación del It Compliance, Privacidad y Protección de Datos. América Latina recibió gran influencia de la Unión Europea, consideramos que Uruguay es el país con mejores garantías y condiciones en el tratamiento de datos, cuya distinción viene en mérito al cumplimiento de los controles que exige la Unión Europea. Por último, Argentina es pionero en el tratamiento de datos, sin embargo, actualmente no se ajusta a las condiciones establecidas en la Unión Europea, tampoco crea incentivos para que las empresas se autoregulen, al igual que Perú no fomenta una cultura de cumplimiento para la implementación del It Compliance, Privacidad y Protección de Datos, no obstante, a diferencia de nuestra legislación, Argentina se encuentra en un proceso de adaptación.

CUARTA. La adopción de los mecanismos de prevención y control en las empresas públicas relacionadas al tratamiento de datos han resultado ser idóneos y eficientes en el control de irregularidades en el manejo de la información, además de fomentar nuevos estándares éticos en el buen gobierno corporativo, sin embargo, en nuestro país su implementación en las empresas del sector público es muy reducido, generando un alto grado de debilidad institucional.

RECOMENDACIONES

PRIMERA. Se sugiere al legislador peruano modificar la Ley N° 29733 "Ley de Protección de Datos Personales", en los siguientes extremos:

(i) La incorporación del principio de responsabilidad proactiva, regulada por la Unión Europea, el cual exige a la entidad la adopción de medidas técnicas y organizativas apropiadas a fin de garantizar y demostrar su cumplimiento.

(ii) La adhesión de nuevas medidas técnicas y de seguridad, siendo las siguientes: registro de las actividades del tratamiento, privacidad por diseño y por defecto, notificación de una violación de seguridad, evaluación del impacto de protección de datos y la incorporación obligatoria de un Delegado de Protección de Datos en las empresas públicas.

SEGUNDA. Se sugiere al legislador peruano la modificación de la Ley N° 29733 "Ley de Protección de Datos Personales", en cuanto a la incorporación y registro de los códigos de conducta, debiendo tener carácter obligatorio, ya que constituye un mecanismo de autorregulación que contiene valores corporativos propios de la entidad.

TERCERA. Se sugiere a las empresas públicas la adopción del It Compliance de Privacidad y Protección de Datos debido , ya que manejan grandes volúmenes de información en su banco de datos, ello a fin de mejorar sus valores económicos, prevenir responsabilidades en caso ocurra alguna brecha en la seguridad de la información y fomentar una cultura de cumplimiento.

REFERENCIAS BIBLIOGRÁFICAS

1. Aranzamendi, L. (2015). *Del Diseño y redacción de la tesis en derecho.* Lima. GRIJLEY

Arrayet, R. (2016). *Evaluación de la Ley N° 19.628.* Recuperado de: www.evaluaciondelaley.cl/foro_ciudadano/site/artic/20151228/asocfile/2015_conportada.pdf

2. Astudillo, G., & Jiménez, S. (2015). *Programa de Cumplimiento como mecanismo de lucha contra la corrupción: especial referencia a la Autoregulación de las Empresas*. Recuperado de: http://revistas.pucp.edu.pe/index.php/derechoysociedad/article/view/15225/15693

3. Astudillo, G. (2017). *Hacia la implementación de los programas de cumplimiento (compliance) en el Perú.* Recuperado de: http://perso.unifr.ch/derechopenal/assets/files/anuario/an_2013_08.pdf

4. Bacigalupo, E. (2012). *"compliance" y derecho penal*. Buenos Aires. Editorial Aranzadi

Carmona, C. (2015). *Autorregulación: Análisis Normativo.* Recuperado de: http://repositorio.uchile.cl/bitstream/handle/2250/137601/Autorregulaci%C3%B3n-an%C3%A1lisis-normativo.pdf?sequence=1

5. Casanovas, A. (2012). Legal Compliance. *Principios de Cumplimiento Generalmente Aceptados*. Madrid. Economist & Jurist

6. Clavijo, C. A. (2016). *Criminal Compliance y Sistema Penal en el Perú*. Tesis sustentada en la Pontificia Universidad Católica del Perú, Facultad de Derecho, Lima

7. Cumbreras M. (2016). *It compliance: La importancia de la protección de datos de carácter personal.* Recuperado de: https://apryme.es/it-compliance-proteccion-de-datos

8. Eguiguren, J. (2015). *El derecho a la protección de datos personales. Algunos temas relevantes de su regulación en Perú.* Recuperado de: http://revistas.pucp.edu.pe/index.php/themis/article/view/14462

9. García, E. (2018). *La transparencia en el nuevo Reglamento General de Protección de Datos.* Recuperado de: https://www.radoctores.es/doc/2V3N1%20-GARCIACUEVAS%20-%20protecci%C3%B3n%20de%20datos.pdf

10. García, P. (2012). *Esbozo de un modelo de atribución de responsabilidad penal de las personas jurídicas. Lima.* Revista Estudios de la Justicia

11. Gonzales, P. (2012). *La responsabilidad penal de las personas jurídicas*. Tesis doctoral sustentada en la Universidad de Córdoba de España

12. Herrán A. (2003). *El derecho a la protección de datos personales en la sociedad de la información.* Recuperado de: http://www.deusto-publicaciones.es/deusto/pdfs/cuadernosdcho/cuadernosdcho26.pdf

13. Hurtado, J., & Mendoza, F. (2016). *Temas de derecho penal económico: empresa y compliance.* Lima. Fondo editorial PUCP

14. Indacochea A. (2010). *Una propuesta para mejorar las prácticas de Gobierno Corporativo.* Recuperado de: https://indacocheanoticias.files.wordpress.com/2013/01/gobierno-corporativo-cladea-03.pdf

15. Kuhlen, L., & Montiel, J., & Ortiz. (2013). *Compliance y teoría del Derecho Penal.* Madrid. Marcial Pons

16. Lambert, P. (2016). *The Data Protection Officer: Profession, Rules, and Role*. 1 Edition. Auerbach Publications

17. Mir, S., & Corcoy, M., & Gómez, V. (2014). Responsabilidad de la Empresa y Compliance. Argentina. Editorial Bdef

18. Montiel, J. (2018). *Ley 27.401 y criterios para determinar la idoneidad de los programas de integridad. En N. Durrieu y R. Saccani (Directores), Anticorrupción 133 y responsabilidad penal empresaria.* Buenos Aires. Editorial La Ley.

19. Navarro, F. (2008). Responsabilidad social corporativa: teoría y práctica. Madrid. ESIC Editorial

20. Nieto, M. (2015). *Manual de cumplimiento en la empresa.* Valencia. Editorial Tirant

Rallo, A. (2012). *Hacia un nuevo Sistema Europeo de Protección de Datos: Las claves de la reforma. Recuperado de:* http://revistas.uned.es/index.php/derechopolitico/article/view/10244

21. Rebollo, L., & SALTOR, C. (2013). *El Derecho a la Protección de Datos en España y Argentina, Orígenes y regulación vigente.* Argentina. Dykinson.

22. Reyna, L., & Coca, I., & Uribe. (2018). *Compliance y Responsabilidad Penal de las personas jurídicas.* Lima. Editorial Ideas

23. Sáiz, C. et. al. (2016). *Compliance, cómo gestionar los riesgos normativos en la empresa*. España. Thomson Reuters

24. Zaballos, E. (2013). *La protección de datos personales en España: evolución normativa y criterios de aplicación.* Recuperado de: https://eprints.ucm.es/22849/1/T34733.pdf

ANEXOS

RESPECTO AL OBJETIVO ESPECÍFICO N° 03

ANEXO 01: MANUAL DE GESTIÓN INTEGRAL DE RIESGOS

I.- OBJETIVO

Establecer un marco para la Gestión Integral de Riesgos, el cual facilite la integración de las actividades descentralizadas de administración de riesgos, implementadas en la **EMPRESA DEL SECTOR ELÉCTRICO**, proporcionando técnicas y metodologías, procurando consistencia y estandarización.

II.- ALCANCE

El presente Manual aplica a todas las unidades orgánicas de la **EMPRESA DEL SECTOR ELÉCTRICO**, Gerencia General, Gerencias y Sub Gerencias, unidades de producción, así como los procesos y proyectos; es decir, involucra a todos los actores, incluyendo clientes, inversionistas, miembros del Directorio, comités, contratistas, proveedores, entre otros; por tanto, es de competencia y obligatoria aplicación para todos los colaboradores de la **EMPRESA DEL SECTOR ELÉCTRICO.**

III.- DOCUMENTOS A CONSULTAR

- Normas de Control Interno, aprobado por Resolución de Contraloría General N° 320-2006-CG.
- Decreto Legislativo Nº 1031, Decreto Legislativo que Promueve la Eficiencia de la Actividad Empresarial del Estado y su reglamento Decreto Supremo N° 176-2010-EF y sus normas modificatorias.
- Código de Buen Gobierno Corporativo para las Empresas bajo el ámbito de FONAFE, aprobado por los Acuerdo de Directorio N° 002-2013/003-FONAFE.
- Lineamientos para la Gestión de la Continuidad Operativa de las Entidades Públicas en los tres niveles de Gobierno, aprobado con Resolución Ministerial N° 028-2015-PCM.

- Sistema Efectivo de Análisis de Riesgo (SEAR) - FONAFE
- Lineamiento Corporativo "Sistema de Control Interno para las Empresas bajo el ámbito de FONAFE", aprobado por Acuerdo de Directorio N° 015-2015/016-FONAFE
- Manual Corporativo "Guía para la Evaluación del Sistema de Control Interno", aprobado con Resolución de Dirección Ejecutiva Nº 123-2015/DE-FONAFE.
- Ley N° 30424, Ley que regula la responsabilidad administrativa de la persona jurídica
- Decreto Legislativo N° 1352, Decreto Legislativo que amplía la responsabilidad administrativa de las personas jurídicas.
- Ley N° 29733, Ley de Protección de Datos Personales
- Reglamento de la Ley N° 29733, aprobada mediante el Decreto Supremo N° 003-2013-JUS
- Directiva de seguridad de la Ley de Protección de Datos Personales
- Guía para la implementación y fortalecimiento del Sistema de Control Interno en las Entidades del Estado, aprobado por Resolución de Contraloría N° 004-2017-CG
- Plan Estratégico Institucional de la **EMPRESA DEL SECTOR ELÉCTRICO**
- Manual de Organización y Funciones (MOF) de la **EMPRESA DEL SECTOR ELÉCTRICO**
- Norma ISO 9001:2015 – Sistema de Gestión de Calidad. Norma ISO 31000:2009 – Gestión de Riesgos.
- Norma ISO/IEC 27001 – Sistema de Gestión de Seguridad de la Información.

IV.- DEFINICIONES

Activo: La información, el conocimiento sobre los procesos, el personal, hardware, software y cualquier otro recurso involucrado en el tratamiento de los datos personales, que tenga valor para la organización.

Alta Dirección: Toda referencia al Directorio y la Gerencia General.

Amenaza: Es cualquier factor de riesgo con potencial para provocar un impacto negativo en la **EMPRESA DEL SECTOR ELÉCTRICO** durante determinado periodo de tiempo.

Apetito de riesgo: es la cantidad de **riesgo** que una organización está dispuesta a asumir para alcanzar sus objetivos estratégicos.

Autorización: Consentimiento previo, expreso e informado del titular de los datos personales para llevar a cabo el tratamiento de datos personales

Aviso de privacidad: Es el documento físico, electrónico o en cualquier otro formato, generado por la **EMPRESA DEL SECTOR ELÉCTRICO**, dirigido al Titular para informarle que le serán aplicables las presentes Políticas de Tratamiento de Datos Personales, como puede conocer su contenido, y que finalidad se dará a sus Datos Personales.

Base de datos: Es el conjunto organizado de Datos Personales que sean objeto de Tratamiento, e incluye archivos físicos, electrónicos y automatizados.

Cambios Significativos: Todo aspecto relacionado con cambios en el entorno externo, en el Modelo de Negocio, así como en la Alta Dirección.

Capacidad al riesgo: Es el nivel máximo de riesgo que la **EMPRESA DEL SECTOR ELÉCTRICO** puede soportar en el logro de sus objetivos.

Control: Es una actividad que tiene como finalidad reducir la criticidad de un riesgo al cual se encuentra asociado.

COSO ERM: Marco para la Administración de Riesgos Corporativos publicado por la organización COSO

Datos personales: Cualquier información vinculada o que pueda asociarse a una o a varias personas naturales determinadas o determinables.

Delegado de protección de datos: Es aquel garante de la protección del tratamiento de los datos personales, cuya función comprende, supervisar, controlar, disponer políticas de prevención y actuación en el manejo de los datos personales de una organización.

Directorio: Toda referencia al Directorio, entiéndase realizada también a cualquier órgano equivalente.

Encargado de tratamiento de datos personales. Toda persona natural, persona jurídica de derecho privado o entidad pública que sola o actuando conjuntamente con otra realiza el tratamiento de los datos personales por encargo del titular del banco de datos personales en virtud de una relación jurídica que le vincula con el mismo y delimita el ámbito de su actuación. Incluye a quien realice el tratamiento sin la existencia de un banco de datos personales.

Gestión Integral de Riesgos: Proceso de identificación, medición, control, monitoreo, evaluación, retroalimentación y optimización de todas las situaciones que representan riesgos para la **EMPRESA DEL SECTOR ELÉCTRICO.**

Gobierno Corporativo: Es el conjunto de principios y normas que regulan el diseño, integración y funcionamiento de los órganos de gobierno de la **EMPRESA DEL SECTOR ELÉCTRICO**, procurando equilibrio entre el poder de los Accionistas, Directorio y la Gerencia General.

Impacto: La consecuencia o consecuencias de un evento, expresado ya sea en términos cualitativos o cuantitativos. Usualmente se expresará en términos monetarios, como pérdidas financieras. También es llamado severidad.

Mapa de Riesgos: Representación gráfica de la exposición al riesgo de los Macroprocesos y Procesos, en función al apetito, tolerancia y capacidad del riesgo definida por la **EMPRESA DEL SECTOR ELÉCTRICO.**

Nivel de Riesgo: Grado de exposición al riesgo, expresado en términos del producto de la probabilidad e impacto.

Manual de Gestión Integral de Riesgos: Documento que contiene las metodologías y procedimientos dispuestos para la identificación, evaluación, tratamiento, control, reporte y monitoreo de los riesgos de la **EMPRESA DEL SECTOR ELÉCTRICO.**

Probabilidad: La posibilidad de la ocurrencia de un evento que usualmente es aproximada mediante una distribución estadística. En ausencia de información suficiente, o donde no resulta posible obtenerla, se estimarán bajo métodos cualitativos, como se ha definido en la metodología de la **EMPRESA DEL SECTOR ELÉCTRICO.**

Proceso: Conjunto de actividades, tareas y procedimientos organizados y repetibles que producen un resultado esperado.

Proyecto: Un proyecto es un esfuerzo temporal que se lleva a cabo para crear un producto, servicio o resultado único.

Responsable del tratamiento: Es aquél que decide sobre el tratamiento de datos personales, aun cuando no se encuentren en un banco de datos personales.

Riesgo: La condición en que existe la posibilidad de que un evento ocurra e impacte negativamente sobre los objetivos de la empresa. De acuerdo al estado de tratamiento del riesgo es importante diferenciar los siguientes conceptos:

- Riesgo Inherente: Son los riesgos sin los efectos mitigadores de control.
- Riesgo Residual: Es el riesgo remanente después que los controles han sido implementados.

SEAR (Sistema Efectivo de Análisis de Riesgo): El Sistema Efectivo de Análisis de Riesgo es un enfoque estandarizado para la implementación de la Gestión de Riesgos en las empresas de la Corporación FONAFE el cual se basa en los principios del Marco COSO ERM.

Seguridad razonable: Se refiere al nivel de seguridad que la **EMPRESA DEL SECTOR ELÉCTRICO** puede tener en alcanzar sus objetivos, considerando que siempre es posible que se produzcan desviaciones o impactos financieros importantes que no sean prevenidos o detectados, dada la incertidumbre inherente al futuro.

Subcontratación: Modalidad de gestión mediante la cual la **EMPRESA DEL SECTOR ELÉCTRICO** contrata a un tercero para que éste desarrolle un proceso que podría ser realizada por esta.

Sistema de Control interno: Un proceso, realizado por el Directorio, la Gerencia y el personal, diseñado para proveer un aseguramiento razonable en el logro de objetivos referidos a la eficacia y eficiencia de las operaciones, confiabilidad de la información financiera, y cumplimiento de las leyes aplicables y regulaciones.

Tipos de Riesgo: Los riesgos pueden surgir por diversas fuentes, internas o externas, y pueden agruparse en diversas categorías o tipos, a continuación, se enumera una lista de los principales tipos de riesgos a que está expuesta una empresa:

- Riesgo de Reputación: La posibilidad de pérdidas por la disminución en la confianza en la integridad de la empresa, que surge cuando su buen nombre es afectado. El riesgo de reputación puede presentarse a partir de otros riesgos inherentes en las actividades de la empresa.

- Riesgo de Tecnología de la Información: La posibilidad de ocurrencia de un evento que comprometa el soporte tecnológico a los procesos de la **EMPRESA DEL SECTOR ELÉCTRICO.**

- Riesgo Operacional: La posibilidad de pérdidas debido a procesos inadecuados, fallas del personal, de la tecnología de información, o eventos externos. Esta definición incluye los riesgos que a continuación se definen, pero excluye el riesgo estratégico y de reputación.

- Riesgo de Seguridad y Salud Ocupacional: La posibilidad de ocurrencia de un evento en el ambiente de trabajo, de características negativas (produzca daño) el cual puede ser generado por una condición de trabajo directa o indirecta, capaz de desencadenar alguna perturbación en la salud o integridad física del trabajador.

- Riesgo Medioambiental: La posibilidad de ocurrencia de eventos que puedan causar un impacto en el medioambiente.

- Riesgo Operacional: La posibilidad de pérdidas debido a procesos inadecuados, fallas del personal, de la tecnología de información, o eventos externos. Esta definición incluye los riesgos que a continuación se definen, pero excluye el riesgo estratégico y de reputación.

- Riesgo de Desastre: Es la probabilidad de que la población y sus medios de vida sufran daños y pérdidas a consecuencia de su condición de vulnerabilidad y el impacto de un peligro.

Titular de datos personales. Persona natural a quien corresponde los datos personales.

Titular del banco de datos personales. Persona natural, persona jurídica de derecho privado o entidad pública que determina la finalidad y contenido del banco de datos personales, el tratamiento de estos y las medidas de seguridad.

Tratamiento: cualquier operación o conjunto de operaciones sobre datos personales dentro de las cuales se puede incluir su recolección, almacenamiento, uso, circulación o supresión.

Tolerancia al riesgo: El nivel de variación que la **EMPRESA DEL SECTOR ELÉCTRICO** está dispuesta a asumir en caso de desviación en relación a los objetivos empresariales trazados.

V.- MARCO PARA LA GESTIÓN INTEGRAL DE RIESGOS

La Gestión Integral de Riesgos es un proceso, efectuado por el Directorio, la Gerencia General, Gerencias, Sub Gerencias y los trabajadores en general, aplicado en toda la empresa y en la definición de su estrategia; está diseñado para identificar potenciales eventos que

pueden afectarla, gestionarlos de acuerdo a su Apetito, Tolerancia y Capacidad de riesgo y proveer una seguridad razonable en el logro de sus objetivos.

La aplicación de la Gestión Integral de Riesgos tiene como punto de partida la definición y conocimiento de los objetivos de la **EMPRESA DEL SECTOR ELÉCTRICO**, con lo cual se identifican los riesgos que pueden afectar el logro de los mismos; bajo este esquema se consideran las siguientes categorías de objetivos:

- **Estratégicos:** Son objetivos de alto nivel, vinculados a la visión y misión empresarial.
- **Operacionales:** Son objetivos vinculados al uso eficaz y eficiente de los recursos.
- **De Reporte:** Son objetivos vinculados a la confiabilidad de la información financiera y no financiera suministrada.
- **De Cumplimiento:** Son objetivos vinculados al cumplimiento de las leyes y regulaciones aplicables.

El objetivo primordial de toda organización es maximizar el valor empresarial, desarrollando un lenguaje común y estándares para la toma de decisiones, asegurando que todas las energías estén centradas en alcanzar este objetivo. Sin embargo, el éxito o fracaso para conseguir este objetivo depende de las decisiones gerenciales al más alto nivel (desde la estrategia), hasta las operaciones del día a día.

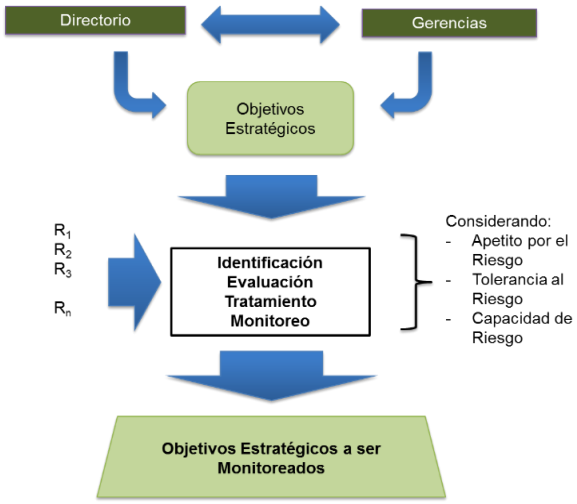
Para construir valor la Gerencia debe evaluar correctamente el riesgo inherente en sus decisiones, producto de estas decisiones gerenciales el valor es creado, destruido o preservado.

La Gestión Integral de Riesgos se inicia desde la concepción de los objetivos estratégicos, los cuales se definen considerando las probabilidades de la cantidad de riesgo que el Directorio y la Gerencia están dispuestos a aceptar en su búsqueda de valor, también

debe ser considerada la Tolerancia al riesgo, expresada por el nivel aceptable de la variación alrededor del logro de los objetivos estratégicos.

Una vez realizada la definición de objetivos, estos servirán de base para la definición y ejecución de las estrategias de negocios y posteriormente medir los resultados y evaluar el grado de cumplimiento de los objetivos trazados.

FIGURA 1: GESTIÓN INTEGRAL DE RIESGOS



FUENTE: Elaborado en base a la propuesta de implementación del Sistema de Prevención de Delitos D. Leg. 1352 de Electro Perú S.A.

Definidas las estrategias de negocios, se deberá identificar y evaluar los riesgos que puedan afectar la capacidad de lograr los objetivos y determinar a su vez estrategias de respuesta al riesgo y las actividades de control.

Objetivos de la Gestión Integral de Riesgos

Son objetivos y beneficios derivados de aplicar la Gestión Integral de Riesgos como parte de la estrategia empresarial:

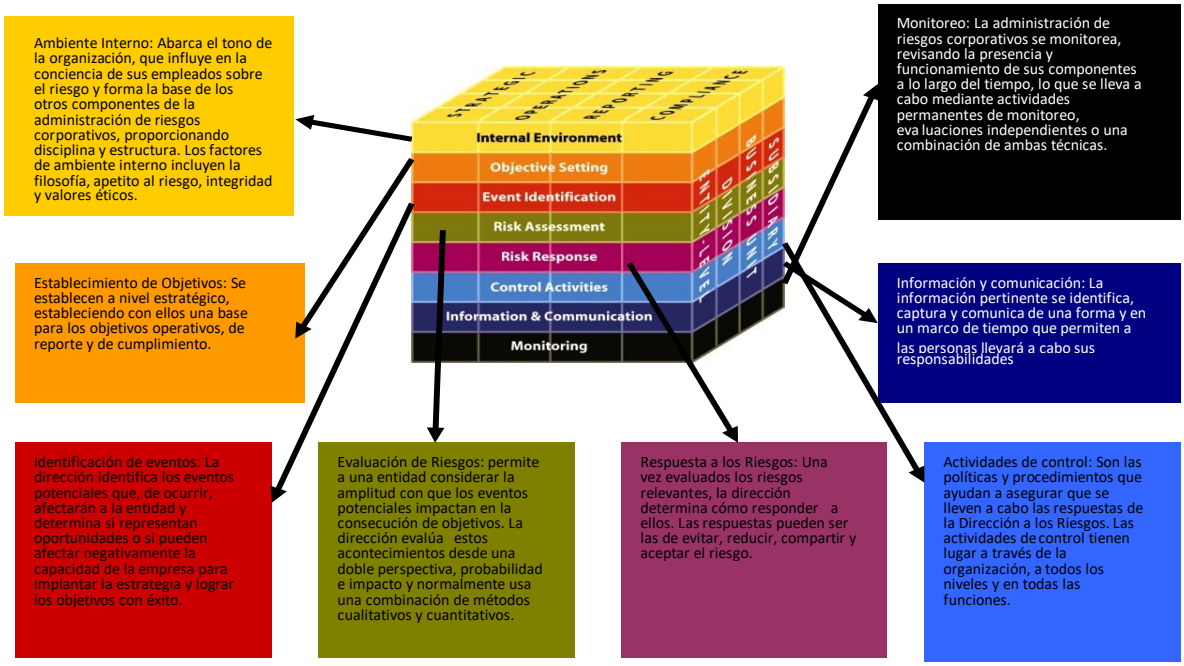
- Estandarizar las definiciones y de criterios para el proceso de administración de riesgos en el tratamiento de datos personales.

- Identificar las medidas de seguridad y realizar el análisis de brecha.
- Administrar los eventos futuros que crean incertidumbre.
- Transformar datos de riesgos en información y conocimiento para la toma de decisiones.

Enfoque Metodológico aplicado

El enfoque está basado en las recomendaciones del Informe COSO – ERM (*Committe of Sponsoring Organizations of the Treadway Commission*), que es un marco integrado para la administración de riesgos y ha sido la base para el diseño del SEAR por parte de FONAFE. Este marco consta de los siguientes componentes:

FIGURA 2: ENFOQUE METODOLÓGICO (COSO – ERM)

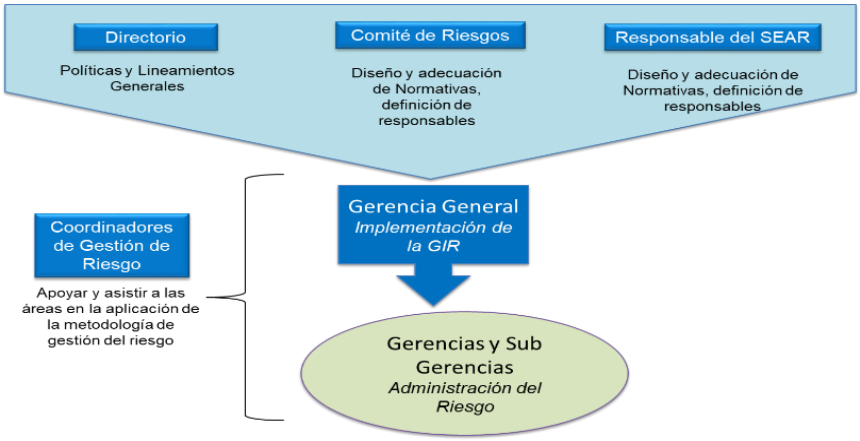


FUENTE: Elaborado en base a la propuesta de implementación del Sistema de Prevención de Delitos D. Leg. 1352 de Electro Perú S.A.

VI.- RESPONSABILIDADES

Representa la forma de asegurar el correcto funcionamiento de los componentes de la Gestión Integral de Riesgos a lo largo del tiempo, a través de la asignación de un esquema de responsabilidades consistentes con las características de la **EMPRESA DEL SECTOR ELÉCTRICO**, siendo fundamental establecer claramente el involucramiento y la responsabilidad de todos los trabajadores en la administración del riesgo.

FIGURA 3: ESTRUCTURA DE GOBIERNO Y RESPONSABILIDADES PARA LA GESTIÓN INTEGRAL DE RIESGOS



FUENTE: Elaborado en base a la propuesta de implementación del Sistema de Prevención de Delitos D. Leg. 1352 de Electro Perú S.A.

Directorio

El Directorio es responsable de establecer una gestión integral de riesgos y de propiciar un ambiente interno que facilite su desarrollo adecuado. Entre sus responsabilidades específicas están:

- Aprobar las políticas generales que guíen las actividades de **la EMPRESA DEL SECTOR ELÉCTRICO** en la gestión de los diversos riesgos que enfrenta en el tratamiento de datos personales.

- Aprobar el Apetito, nivel de Tolerancia y Capacidad de riesgo, es decir el grado de exposición al riesgo que la **EMPRESA DEL SECTOR ELÉCTRICO** está dispuesta a asumir en el desarrollo de sus operaciones.
- Seleccionar una plana gerencial con idoneidad técnica y moral, que actúe de forma prudente y apropiada en el desarrollo de sus operaciones, así como en el cumplimiento de sus responsabilidades.
- Aprobar los recursos necesarios para el adecuado desarrollo de la Gestión Integral de Riesgos, a fin de contar con la infraestructura, metodologías y personal apropiado.
- Establecer los objetivos empresariales, evaluar y aprobar sus planes de negocios con debida consideración a los riesgos asociados.
- Obtener aseguramiento razonable que **la EMPRESA DEL SECTOR ELÉCTRICO** cuenta con una efectiva gestión de los riesgos a que está expuesta, y que los principales riesgos se encuentran bajo control dentro de los límites que han establecido.
- Proveer gobierno, orientación y supervisión en relación a la implementación del marco de Administración de Riesgos en el tratamiento de protección de datos personales.
- Monitorear la medida en que la gerencia ha establecido una Gestión de Riesgos eficaz.

Comité de Auditoría y Riesgos

Se encuentra conformado por el Directorio la **EMPRESA DEL SECTOR ELÉCTRICO**, y será la instancia previa de discusión de los aspectos relevantes de la Gestión Integral de Riesgos, para posterior aprobación por parte del Directorio.

Gerencia General

La Gerencia General tiene la responsabilidad de implementar la Gestión Integral de Riesgos conforme a las disposiciones del Directorio, además de las responsabilidades dadas por otras normas internas, leyes o regulaciones. La Gerencia General puede constituir comités para el

cumplimiento de sus responsabilidades que son parte del Gobierno Corporativo de **la EMPRESA DEL SECTOR ELÉCTRICO**

Responsable de Proceso - Gerencias

Tienen la responsabilidad de implementar la Gestión Integral de Riesgos conforme a las disposiciones del Directorio. En cuanto al tratamiento de Protección de datos, puede realizarlo el titular o responsable del tratamiento de datos personales.

Además de las responsabilidades derivadas del entorno normativo y regulatorio que rige las actividades **la EMPRESA DEL SECTOR ELÉCTRICO**. Los Gerentes de las áreas, en sus respectivos ámbitos de acción, en su calidad de Responsables de Proceso, tienen la responsabilidad de administrar los riesgos relacionados al logro de sus objetivos. De acuerdo con lo anterior, entre sus responsabilidades específicas están:

- Asegurar la consistencia entre las operaciones y los niveles de Apetito, Tolerancia y Capacidad de riesgo definidos aplicables a su ámbito de acción.
- Asumir ante la Gerencia General, los resultados de la gestión de riesgos correspondiente a los procesos a su cargo, así como los compromisos de refuerzo que resulten necesarios en sus procesos.
- Implementar la cultura de Gestión de Riesgos en los procesos bajo su responsabilidad, por cuanto la cultura de riesgos es transversal a todos los procesos y responsable de cada Gerencia, bajo los lineamientos de cultura organizacional establecidos por la Ata Dirección.
- Participar en la definición del apetito, tolerancia y capacidad de los principales riesgos a los que se encuentran expuestos sus procesos en coordinación con el Responsable del SEAR y el Comité de Control Interno y Gestión de Riesgos.

- Validar los resultados de la identificación, análisis y evaluación de riesgos, así como las respuestas al riesgo realizados por los Coordinadores de Gestión de Riesgos.
- Designar responsables específicos para participar en la evaluación del riesgo en su proceso, complementando el rol del Coordinador de Gestión de Riesgos.
- Identificar oportunidades de mejora en los procesos bajo su responsabilidad, gestionar su implementación y monitorear el cumplimiento de los planes de acción.
- Comunicar los cambios en sus procesos y los riesgos asociados al Responsable del SEAR y el Comité de Control Interno y Gestión de Riesgos.
- Mantener vigente la documentación de sus procesos.
- Realizar seguimiento de los indicadores de riesgos.
- Implementar las acciones mitigantes definidas para cada uno de los riesgos identificados, de acuerdo a las prioridades establecidas.
- Conducir la evaluación regular del cumplimiento de las políticas de la **EMPRESA DEL SECTOR ELÉCTRICO,** los procedimientos y las prácticas relacionada con los riesgos.
- Reportar oportunamente la información de la gestión de riesgos al Responsable del SEAR.
- Asumir, ante el Gerente General, el Comité de Control Interno y Gestión de Riesgos, y el Directorio, los resultados de la gestión de riesgos correspondiente a su unidad.

Responsable del SEAR - Sub Gerencia de Planificación y Control

Responsable por coordinar los esfuerzos de la Gestión Integral de Riesgos, participando en el diseño y permanente adecuación de los manuales de gestión de riesgos y demás normas

internas que tengan por objeto definir las responsabilidades para la administración de riesgos la **EMPRESA DEL SECTOR ELÉCTRICO.** Asimismo, apoya y asiste a las demás áreas de la **EMPRESA DEL SECTOR ELÉCTRICO** para una adecuada gestión de riesgos en sus áreas de responsabilidad. Las principales funciones en relación a la Gestión Integral del Riesgo son las siguientes:

- Proponer las políticas, procedimientos y metodologías apropiadas para la Gestión Integral de Riesgos en la **EMPRESA DEL SECTOR ELÉCTRICO**, incluyendo los roles y responsabilidades.
- Velar por una Gestión Integral de Riesgos competente, promoviendo el alineamiento de las medidas de tratamiento de los riesgos de la **EMPRESA DEL SECTOR ELÉCTRICO** con los niveles de tolerancia al riesgo y el desarrollo de controles apropiados.
- Guiar la integración entre la gestión de riesgos, los planes del negocio y las actividades de gestión empresarial.
- Establecer un lenguaje común de gestión de riesgos basado en las definiciones del presente Manual y de los demás reglamentos aplicables.
- Informar a la Gerencia General y al Comité de Control Interno y Gestión de Riesgos los aspectos relevantes de la gestión de riesgos para una oportuna toma de decisiones.
- Monitorear el progreso y dar asistencia a otras áreas en trasmitir información importante sobre riesgos hacia arriba, abajo y horizontalmente.
- Asegurar que se desarrollen a cabalidad cada una de las etapas previstas para el diseño e implementación del marco de administración de riesgos.

- Hacer seguimiento a las actividades planeadas para el diseño e implementación del marco de Administración de Riesgos, aplicando correctivos donde se requiera.
- Someter a consideración del Comité de Control Interno y Gestión de Riesgos las propuestas de diseño e implementación del marco de Administración de Riesgos, para su aprobación.

Coordinadores de Gestión de Riesgos

- Mantener una permanente comunicación y coordinación con todos los colaboradores de su unidad, que son los encargados de reportar los riesgos y eventos de pérdida que pudieran presentarse.
- Participar conjuntamente con el Responsable del SEAR en el proceso de auto evaluación identificando los riesgos asociados a los procesos que se desarrollan en su respectiva área.
- Identificar y reportar al Responsable del SEAR sobre los eventos de pérdida que se presenten o se pudieran presentar en su gestión
- Participar en la capacitación del personal de su área, respecto a la Gestión Integral de Riesgos, en los programas de capacitación que promueva la **EMPRESA DEL SECTOR ELÉCTRICO**.
- Coordinar al interior de su área, todos los aspectos que le sean informados por el Responsable del SEAR respecto de la Gestión Integral de Riesgos.
- Tomar conciencia de los riesgos o amenazas que se presenten durante el desarrollo de sus actividades diarias.
- Identificar los eventos que pudieran significar un riesgo para la **EMPRESA DEL SECTOR ELÉCTRICO** dentro del desarrollo de sus funciones.

Responsable Designado de Auditoría Interna

El Comité de Auditoría y Riesgos debe designar un responsable por la vigilancia y supervisión de los procesos de Gestión Integral de Riesgos dentro de la **EMPRESA DEL SECTOR ELÉCTRICO**, pudiendo sub contratar para tal efecto, los servicios de especialistas en la materia. En relación al tratamiento de los datos personales, la empresa puede contar con los servicios de un **DELEGADO DE PROTECCIÓN DE DATOS**, quien supervisará los procesos de gestión en los soportes de información del banco de datos. La función de Auditoría Interna, desempeña un rol independiente a la gestión, que vigila la adecuación de la GIR, debiendo sujetarse a las disposiciones específicas que regulan su actividad. Asimismo, debe verificar la efectividad de los controles aplicados sobre los riesgos evaluados.

VII.- POLÍTICAS DE GESTIÓN INTEGRAL DE RIESGOS EN EL TRATAMIENTO DE DATOS PERSONALES

GENERALES:

- El Plan Estratégico deberá contemplar las categorías de objetivos estratégicos, de operaciones, de información y de cumplimiento, los cuales deberán estar alineados a la estrategia de la **EMPRESA DEL SECTOR ELÉCTRICO.**
- La Gestión Integral de Riesgos en la **EMPRESA DEL SECTOR ELÉCTRICO** forma parte integral del Sistema Efectivo de Análisis de Riesgo (SEAR), por lo cual el Directorio y la Gerencia de la empresa asumirán con liderazgo y compromiso su diseño e implementación, velando por su eficaz funcionamiento.
- La política la empresa se centra en identificar, analizar y responder apropiadamente a todos los riesgos. Las respuestas del riesgo seleccionadas son determinadas por el apetito, la tolerancia y capacidad de riesgo, establecidos por la empresa. Éstos variarán a través

del tiempo según los objetivos empresariales específicos **(Estratégicos, Operacionales, de Reporte y Cumplimiento).**

- La efectividad de las medidas de control que son resultado de la GIR, será reportada regularmente y ratificada por el Directorio. Además, se realizará la revisión periódica independiente. **La empresa debe establecer controles, procedimiento de vigilancia y supervisión en todas las etapas de los procesos, con la finalidad de identificar su criticidad, eventos y amenazas, facilitando el diseño de estrategias y controles adecuados para administrar los riesgos.**

ESPECÍFICAS:

A) AMBIENTE DE CONTROL

El Directorio y las Gerencias resaltan la importancia de la Gestión Integral de Riesgos, estableciendo y poniendo en práctica la filosofía empresarial y los estándares esperados de conducta ética de los colaboradores. Asimismo, refuerzan las expectativas sobre la administración de riesgos en los distintos niveles de **la empresa del sector eléctrico**, teniendo este componente, una influencia muy relevante sobre los demás:

- La conducta de los colaboradores se rige por el **Código de Ética, Reglamento Interno de Trabajo,** y otras complementarias respecto a posibles conflictos de interés o estándares esperados de comportamiento ético y moral, con lo que demuestra su compromiso con la integridad y valores éticos.
- El Directorio es explícito sobre el tono ético que debe conducir las acciones de los colaboradores, siendo tal expresión de alcance en toda la **EMPRESA DEL SECTOR ELÉCTRICO**, por tanto, las negociaciones con tales, con proveedores, clientes,

inversionistas, acreedores, aseguradores, entre otros vinculados, se basan en los principios de honestidad e imparcialidad.

- La **EMPRESA DEL SECTOR ELÉCTRICO** responde a las violaciones de las normas de conducta, en tanto que las acciones disciplinarias resultado de tales, son ampliamente comunicadas al interior, por lo que los colaboradores son conscientes que, ante eventual transgresión, serán objeto de sanciones de acuerdo a las citadas normas.

B) ESTABLECIMIENTO DE OBJETIVOS

El Directorio y las Gerencias conducen el proceso por el cual se determinan los objetivos empresariales, estos deben encontrarse alineados a la visión y misión de la **EMPRESA DEL SECTOR ELÉCTRICO**, y ser compatibles con el apetito por el riesgo, tolerancia al riesgo y capacidad de riesgo. El establecimiento de objetivos es una condición para Identificar eventos y, valorar y responder a los riesgos.

C) IDENTIFICACIÓN DE RIESGOS

Es el proceso por el que se identifican los riesgos originados por factores internos y externos, que pueden tener un impacto negativo sobre los objetivos de la **EMPRESA DEL SECTOR ELÉCTRICO**. Para tal fin se deben aplicar las medidas técnicas y organizativas contenidas en el manual de gestión de riesgos. Entre otros aspectos, se busca identificar factores influyentes que los determinan, como los cambios significativos o proyectos de envergadura.

- Se deben identificar los riesgos para cada objetivo definido, es importante considerar que uno o más riesgos podrían vincularse a un objetivo. La forma de identificar el riesgo inherente es independiente de la probabilidad de que este ocurra.

- Las Gerencias, las áreas de control y los colaboradores en general, identifican los riesgos que afectarían el logro de objetivos, aquellos que pueden tener impacto negativo y en casos sea posible los positivos.
- Los riesgos con una probabilidad relativamente baja de ocurrencia, como lo son aquellos que configuran escenarios de desastre, son objeto de monitoreo permanente dado su impacto potencial.
- Las fuentes de información utilizadas para la identificación de riesgos comprenden tanto aquella referida al pasado (información histórica) como al futuro (estimaciones), por tanto, al evaluar el riesgo, se consideran los riesgos que anteriormente se materializaron y aquellos que no.
- Se deben seleccionar técnicas que se ajustan a la filosofía de gestión de riesgos, asegurando el desarrollo de capacidades de identificación de riesgos necesarias.

D) EVALUACIÓN DE RIESGOS

La evaluación de riesgos comprende un proceso dinámico e iterativo que tiene como propósito identificar, analizar y gestionar la exposición a los riesgos relacionados al logro de los objetivos a nivel estratégico, operativo, de reporte y de cumplimiento.

- Se han establecido mecanismos para evaluar los riesgos a nivel empresa, a nivel del Mapa de Procesos, a nivel de Cambios Significativos y de Proyectos, tanto aquellos derivados de factores internos como externos que podrían condicionar sus respectivos objetivos.
- Los riesgos se evalúan desde dos perspectivas que son Probabilidad e Impacto / Severidad, en tal sentido, cada sistema de gestión de riesgos guardará consistencia con el presente enfoque. Sin perjuicio de lo anterior, cada sistema de gestión de riesgos podrá utilizar el enfoque metodológico que más se ajuste a sus necesidades y expectativas.

- El horizonte de tiempo utilizado para evaluar los riesgos es coherente con el horizonte de tiempo de implementación de la estrategia y los objetivos relacionados.
- Cuando el riesgo presenta más de un impacto, se aplicará preferentemente aquel que corresponda al Tipo de Riesgo por su naturaleza, en tanto que se utilizarán las escalas cuantitativas en caso se disponga de información del impacto económico del riesgo.

E) RESPUESTA A RIESGOS

Las respuestas al riesgo son las acciones a través de las cuales se opta por aceptar el riesgo, reducir (disminuir la probabilidad de ocurrencia o disminuir el impacto), transferirlo total o parcialmente, evitarlo, o una combinación de las medidas anteriores, de acuerdo al nivel de apetito, tolerancia y capacidad de riesgo definido. En este proceso se aplican conceptos de costo - beneficio para definir la ejecución de las acciones de mitigación de riesgos.

F) ACTIVIDADES DE CONTROL

Las actividades de control pueden ser preventivas o detectivas y comprenden una serie de actividades manuales o automáticas, como autorizaciones, aprobaciones, verificaciones, reconciliaciones, controles físicos, de supervisión y de productividad. Estas contribuyen a asegurar que se tomen acciones para minimizar los riesgos y así lograr los objetivos de la **EMPRESA DEL SECTOR ELÉCTRICO** en todos los niveles y en todas las funciones. Asimismo, la segregación de funciones por lo general se encuentra inmersas en el diseño de las actividades de control antes referidas, cabe precisar que ello incluye controles generales y de aplicación de tecnología.

G) SUPERVISIÓN

Es el proceso para verificar la calidad de desempeño de la Administración de Riesgos a través del tiempo. Se realiza a través de actividades de monitoreo continuo, es decir, actividades de

dirección y supervisión. También bajo la forma de evaluaciones específicas para monitoreo de riesgos y eficacia de los procedimientos para su administración.

- Se realizan evaluaciones permanentes a fin de asegurar que los componentes de la administración de riesgos están presentes y funcionando como se tiene previsto.
- Se han desarrollado mecanismos de autoevaluación para captar y reportar las deficiencias identificadas en la administración de riesgos, tanto de fuentes internas y externas (por ejemplo, clientes, proveedores, auditores, reguladores).
- Los reguladores comunican a la **EMPRESA DEL SECTOR ELÉCTRICO**, información sobre cumplimiento u otros asuntos que reflejen el funcionamiento del sistema de control interno y administración de riesgos, y esta realiza las acciones requeridas ante la identificación de eventuales brechas o deficiencias.
- Se da respuesta e implementan las recomendaciones de los auditores externos sobre los medios para fortalecer las medidas de administración de riesgos y se siguen las acciones deseadas para verificar la implementación.

VIII.- METODOLOGÍA DE ADMINISTRACIÓN DE RIESGOS

La metodología está basada en el marco del COSO ERM (Comittee of Sponsoring Organizations Enterprise Risk Management), la cual ha sido complementada y adecuada a las características propias de la **EMPRESA DEL SECTOR ELÉCTRICO**, presentando cinco fases claramente definidas:

1. Planificación de la Gestión de Riesgos
2. Identificación y Clasificación del Riesgo
3. Evaluación de Riesgos
4. Identificación y Clasificación de Controles

5. Supervisión y seguimiento

Cabe recordar que la calificación de los riesgos asociados a un proceso / sub proceso que se desarrolla de formas similares en distintas sedes de la **EMPRESA DEL SECTOR ELÉCTRICO**, se evaluarán estos individualmente y se promediarán los resultados a fin de obtener un nivel de riesgo del proceso / sub proceso.

FASE 1 – PLANIFICACIÓN DE LA GESTIÓN DE RIESGOS

La planificación es la fase inicial en el desarrollo de la gestión de riesgos de la **EMPRESA DEL SECTOR ELÉCTRICO** y es fundamental para que las actividades sean implementadas de manera eficiente, oportuna y alineadas a sus necesidades.

FASE 2 – IDENTIFICACIÒN Y CLASIFICACIÒN DE RIESGOS

- Previamente al desarrollo de esta fase se requiere establecer un entorno que estimule e influencie las actividades del personal con respecto a la administración de los riesgos, basándose en la integridad y valores éticos, competencia del personal y cultura organizacional.
- El proceso de identificación, análisis, evaluación y respuesta al riesgo, se documentará en Matrices de Riesgos.
- La identificación y clasificación de riesgos es fundamental para hacer frente a los eventos que afecten el cumplimiento de los objetivos de la entidad y los procesos.

FASE 3 – IDENTIFICACIÓN Y CLASIFICACIÓN DE CONTROLES

La identificación y clasificación de controles consiste en la identificación de los esfuerzos realizados por la **EMPRESA DEL SECTOR ELÉCTRICO** para procurar que los riesgos se encuentren dentro del nivel de apetito de riesgo.

a. Etapa 1 - Criterios para la identificación y documentación de controles

Un control es una actividad que tiene como finalidad reducir la criticidad de un riesgo al cual se encuentra asociado. Para tal efecto en el **ANEXO - Matriz de Riesgos y Controles**, se identificarán los siguientes aspectos:

b. Etapa 2 – Clasificación de controles

Los controles se clasifican según sus atributos, los cuales determinan su fortaleza, estos son:

a. La oportunidad en la que se ejecutan
b. El grado de automatización.
c. Objetivo del control
d. Definición del control
e. Operatividad y Autoevaluación del control

FASE 4 – EVALUACIÓN DEL RIESGO

La evaluación de riesgos tiene como objetivo determinar la criticidad de los riesgos a los la **EMPRESA DEL SECTOR ELÉCTRICO** está expuesta y, así, definir un tratamiento de riesgos adecuado, priorizando los esfuerzos hacia los riesgos más críticos.

a. Etapa 1 - Definición de la criticidad por probabilidad e impacto

Es la determinación de la criticidad de un riesgo evaluando el grado de posibilidad de que este ocurra y el nivel del daño que causaría. Los riesgos son evaluados en función de dos variables:

- Probabilidad

- Impacto

Como parte del despliegue de la metodología, se aplicarán para la evaluación de riesgos, las variables cualitativas de probabilidad señaladas anteriormente para todos los sistemas de gestión de riesgos, sin perjuicio de ello, en cada uno de estos se podrá analizar la información histórica con el propósito de definir escalas de cuantitativas de frecuencia que complementen las cualitativas definidas.

TABLA 2: PROBABILIDAD DE RIESGO

NIVEL	PROBABILIDAD
Bajo	Probabilidad de ocurrencia baja, casi nula (raro) No existe recuerdo de haber ocurrido
Medio	Probabilidad moderada, ocurrencia periódica
Alto	Es muy probable ocurre con frecuencia
Extremo	Probabilidad elevada, ocurre muchas veces

FUENTE: Elaborado en base a la propuesta de implementación del Sistema de Prevención de Delitos D. Leg. 1352 de Electro Perú S.A.

b. Etapa 2 - Evaluación del riesgo inherente

- Un riesgo inherente es aquel riesgo en su forma natural sin el efecto mitigante de los controles.

- Reflejan la exposición de la **EMPRESA DEL SECTOR ELÉCTRICO** a la ocurrencia de un evento de impacto negativo.
- Si bien estos riesgos no pueden eliminarse por completo, es posible implementar controles que mitiguen la probabilidad de ocurrencia y/o el impacto del riesgo en la **EMPRESA DEL SECTOR ELÉCTRICO.**

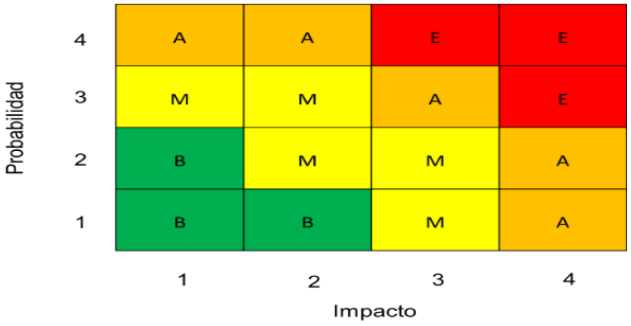
c. Etapa 3 - Evaluación del riesgo residual

- Un riesgo residual es el riesgo restante luego de haber aplicado los controles.

o El nivel de riesgo al que está sometido la **EMPRESA DEL SECTOR ELÉCTRICO** nunca puede erradicarse totalmente, es importante alinear el mismo a la tolerancia al riesgo definida por la empresa.

Finalmente, los resultados de las evaluaciones de riesgo a nivel inherente y residual se representan en un Mapa de Riesgos, el cual permite visualizar gráficamente el grado de exposición:

FIGURA 4: MAPA GENERAL DE RIESGOS



FUENTE: Elaborado en base a la propuesta de implementación del Sistema de Prevención de Delitos D. Leg. 1352 de Electro Perú S.A.

FASE 5 – TRATAMIENTO DEL RIESGO

El tratamiento que se le brinda a un riesgo tiene como propósito mantener la criticidad del riesgo dentro de los niveles de apetito al riesgo definidos por **la empresa de servicio eléctrico**

a. Etapa 1 - Elaboración de estrategias de tratamiento al riesgo

- En esta etapa se definirán las estrategias de tratamiento a los riesgos identificados para mantenerlos dentro de los niveles establecidos en el apetito,

tolerancia y capacidad de riesgo. así como la reevaluación de las respuestas en caso, el nivel de riesgo exceda estos umbrales.

- Existen diversas alternativas para administrar los riesgos de acuerdo a sus características, estas se aplican una vez realizada la evaluación del riesgo residual y de acuerdo al apetito
- Las estrategias y respuestas al riesgo a aplicar varían en función al riesgo administrar y el apetito de riesgo.

TABLA 3: ESTRATEGIAS PARA EL TRATAMIENTO DE RIESGO

ESTRATEGIA	¿QUÉ HACER?	¿CUÁNDO?
Evitar	Dejar de realizar la actividad ligada al riesgo.	El beneficio de implementar un control es menor al costo de la materialización del riesgo inherente
Reducir o Mitigar	Disminuir la probabilidad de ocurrencia e impacto.	El beneficio de implementar un control es mayor al costo del riesgo inherente y la empresa se encuentra en capacidad de realizar el tratamiento del riesgo.
Transferir	Transferir a un tercero la administración del riesgo o enfrentar las pérdidas originadas.	El beneficio de implementar un control es mayor al costo del riesgo inherente y un tercero tiene mayor capacidad para realizar el tratamiento del riesgo.
Aceptar	Conservar el riesgo en su presente nivel.	El riesgo inherente al negocio se encuentra dentro del apetito por riesgo, sin embargo, debe permanecer monitoreado pues podría cambiar la exposición.

FUENTE: Elaborado en base a la propuesta de implementación del Sistema de Prevención de Delitos D. Leg. 1352 de Electro Perú S.A.

b. Etapa 2 - Elaboración de planes de acción

- Corresponde a la propuesta de medidas a implementarse con el fin de abordar una estrategia de tratamiento definida sobre el riesgo identificado.
- Criterios para su presentación:

  Es necesario definir planes de acción cuando:

  - El control que mitiga al riesgo se encuentra mal diseñado.
  - El riesgo no cuenta con un control.

- El riesgo residual se encuentra por encima de los niveles de tolerancia al riesgo.

FASE 6 – SEGUIMIENTO Y MONITOREO CONTINUO

- Las acciones e indicadores producto de las fases previas deben estar en constante seguimiento y monitoreo continuo, de modo que la gestión de los riesgos se desarrolle de acuerdo a lo establecido.
- Esta fase implica hacer la supervisión, seguimiento o monitoreo de las acciones y/o controles acordados, de los diferentes procesos críticos, sean estos controles ya establecidos e implantados como controles propuestos o acordados implantar a futuro, de acuerdo al presupuesto de **la empresa de servicio eléctrico**, plan de crecimiento y situación financiera.
- Cada funcionario a cargo del proceso es responsable de remitir al Responsable del SEAR el informe sobre el estado situacional de los riesgos de sus respectivos procesos.
- Responsable del SEAR consolidará la información del reporte de seguimiento de riesgos de procesos recibida de cada uno de los funcionarios a cargo de cada uno de los procesos, para ser remitida al Comité de Control Interno y Gestión de Riesgos en la frecuencia que se determine, permitiendo de esta manera que se efectúen los ajustes, toma de decisiones u otra acción que dicho órgano considere necesario.

IX.- ANÁLISIS COSTO – BENEFICIO

El análisis Costo / Beneficio forma parte de la "*FASE 4 – EVALUACIÒN DE RIESGOS*", y se establece como condición fundamental en la determinación y aprobación de los Planes de Acción. A continuación, se detalla el procedimiento:

ANÁLISIS CUANTITATIVO

Estimación de los costos

Prácticamente todas las respuestas al riesgo implican un costo directo o indirecto que se debe manejar en relación con el beneficio que esta genera, en este caso particular el beneficio está directamente vinculado con la pérdida que se espera reducir.

De acuerdo con lo anterior, el Responsable del Proceso estimará el costo inicial del diseño e implementación de una respuesta (procesos, personal y tecnología), así como el costo de mantenerla en el tiempo, a fin de obtener los costos totales para el tratamiento propuesto, y su presentación a la Gerencia del área para su aprobación.

Estimación de pérdidas

Con base en las estimaciones de impacto monetario resultado de la evaluación de riesgos, se determinará con mayor precisión aquellos costos asociados que se originarían si el riesgo se materializara. A continuación, presentamos algunos ejemplos de pérdidas asociadas a la materialización de los riesgos:

- Costo de activos a reemplazar (equipos de medición, equipamiento de sedes de producción, otros)
- Monto de pérdida por fraudes
- Diferencias por errores en facturación
- Gastos legales de solución de contingencias con clientes
- Multas y sanciones económicas (reguladores)

ANÁLISIS CUALITATIVO

Es importante identificar los impactos desde las perspectivas intangibles, los cuales no necesariamente se ven traducidas en términos monetarios como son la Reputación, Seguridad de la Información y Continuidad del Negocio, por citar algunos, para lo cual se utilizarán las

variables de “IMPACTO / SEVERIDAD” presentadas en la *“FASE 4 – EVALUACIÒN DE RIESGOS”* y en función a los niveles de Apetito, Tolerancia y Capacidad definidos para el riesgo administrado.

El análisis cuantitativo será complementado con el cualitativo y en función al análisis de ambos resultados, se decidirá la viabilidad integral del tratamiento.

Análisis del Beneficio vs Costo

El Responsable del SEAR comparará las relaciones de beneficios a costos para los tratamientos propuestos y seleccionará aquella que aporta un mayor beneficio, resultando en una relación de Beneficios a Costos mayor.

X.- EVALUACIÓN DE RIESGOS ANTE CAMBIOS SIGNIFICATIVOS

Identificación de Cambios Significativos

Cada Gerencia reportará anualmente, la identificación de cambios generados y aquellos que se tengan previstos en el corto y mediano plazo, a fin de requerir las evaluaciones de riesgos respectivas oportunamente, siendo factores de cambios significativos los siguientes:

- Entorno Externo (entorno externo económico, político, regulatorio, entorno físico y ambiental)
- Modelo de Negocio (Convenios, contratos asociativos, participación en negocios / acciones conjuntas, Reorganización empresarial, Adquisiciones o desinversiones significativas, crecimiento no previsto, Nuevas tecnologías, Infraestructura)
- Cambios en la Dirección y personal clave

A continuación, se presenta una relación de los principales cambios significativos y la Gerencia responsable por gestionar los riesgos del mismo:

TABLA 4: CAMBIOS SIGNIFICATIVOS EN LA ORGANIZACIÓN

CAMBIOS SIGNIFICATIVOS	RESPONSABLE
Requisitos legales y regulatorios	Asesoría Legal
Convenios, contratos asociativos, participación en negocios / acciones conjuntas	Asesoría Legal
Reorganizaciones empresariales	Gerencia General
Subcontrataciones significativas	Sub Gerencia de Logística
Infraestructura tecnológica (software y hardware)	Sub Gerencia de Informática
Ampliaciones / modificaciones de las oficinas principales y locales comerciales / de atención	Sub Gerencia de Logística
Adquisiciones o desinversiones significativas	Gerencia responsable de la adquisición y/o venta significativa
Cambios en Alta Dirección y Personal clave	Sub Gerencia de Recursos Humanos

FUENTE: Elaborado en base a la propuesta de implementación del Sistema de Prevención de Delitos D. Leg. 1352 de Electro Perú S.A.

XI.- MONITOREO Y REVISIÓN DEL MANUAL DE GESTIÓN INTEGRAL DE RIESGOS.

El cumplimiento del presente Manual será monitoreado permanentemente por el Directorio, con el propósito de asegurar su aplicación continua y relevancia. Asimismo, el Manual será revisado y actualizado anualmente y/o cuando ocurran cambios en el ambiente en el que la **EMPRESA DEL SECTOR ELÉCTRICO** desarrolla sus operaciones.

TABLA 5: MATRIZ DE RIESGOS

Descripción de la Actividad	Código Riesgo	Causas	Vulnerabilidad dad	Amenaza	Descripción del Riesgo	Categoría de Objetivo	Recurrencia del Riesgo	Categoría de Riesgo	Riesgo Inherente		
									Impacto	Probabilidad	Nivel de Riesgo
Actividad asociada al tratamiento de los datos personales o cualquier otra actividad de riesgo	Código interno que identifica al riesgo	Factor que origina el Riesgo	Grado de exposición a las brechas de seguridad en la información, u otro.	Factor de riesgo con potencial de impacto en la recopilación de información.	Descripción del EFECTO y CAUSA del riesgo.	Estratégicos Operacional Supervisión Cumplimiento	Rutinarios No Rutinarios	Estratégicos Operacional Reporte Cumplimiento	Bajo Medio Alto Extremo	Bajo Medio Alto Extremo	Bajo Medio Alto Extremo

FUENTE: Elaborado en base a la propuesta de implementación del Sistema de Prevención de Delitos D. Leg. 1352 de Electro Perú S.A.

TABLA 6: MATRIZ DE CONTROLES

Descripción del Control	Tipo de Controles			Clasificación del control			Frecuencia del Control	Código Control	Responsable del Control
	A	SA	M	P	D	C			
Control en el manejo de la información, debiendo ser notificado al órgano de control (Autoridad Nacional de Protección de Datos Personales),	Automático	Semi automático	Manual	Preventivo	Detectivo	Correctivo	Periodicidad con la que se ejecuta el control: -Diario -Semanal -Mensual -Anual -Eventual	Código interno que identifica al riesgo	Delegado de Protección de Datos Órgano Estatal Supervisor Autoridad Nacional de Protección de Datos Personales

FUENTE: Elaborado en base a la propuesta de implementación del Sistema de Prevención de Delitos D. Leg. 1352 de Electro Perú S.A.