FACULTAD DE POSTGRADOS

MAESTRÍA EN DERECHO DIGITAL E INNOVACIÓN

TÍTULO DE LA INVESTIGACIÓN

PLAN DE IMPLEMENTACIÓN DEL CONSENTIMIENTO INFORMADO EN DOCUMENTOS Y FORMULARIOS A SER EMPLEADOS POR UNA ENTIDAD FINANCIERA NACIONAL EN CUMPLIMIENTO A LO ESTABLECIDO EN LA LOPDP.

ECUADOR – MARZO 2023

Profesora

Dra. Lorena Naranjo G.

Autores

Fernando Javier Cobo Chacón

Juan Carlos Crespo Cruz

2023

RESUMEN

La presente investigación, dentro de las limitaciones de síntesis metodológica impuesta sobre el trabajo, busca ser sobre un punto concreto (consentimiento informado), fórmula perfectible de aplicación de la Ley Orgánica de Protección de Datos Personales. Punto que atiende al consentimiento informado en su real dimensión y buscando ser un aporte de aplicación práctica en documentos y formatos que aplicará una Institución Financiera de primer orden, claro está buscando cumplir con los derechos y principios consagrados en la referida normativa. Trabajo que si bien ha sido desarrollado sobre la base ideológica recibida en la maestría cursada por los autores, evidencia la línea de pensamiento propio que en varios puntos cuestiona la incertidumbre en la cual la norma central que es el paraguas de este trabajo, efectivamente se practicará en todos los ámbitos. Llegando a ser, en criterio de los autores, este trabajo un aporte efectivo en el desarrollo documental práctico para la propia Institución Financiera analizada, resultado que se evidencia de los Anexos al trabajo y que reúnen de forma sistemática con la mayoría de los aspectos trabajados a lo largo del presente documento. Concluyendo que con mucho esfuerzo se puede lograr cierta armonía entre lo que la norma pretende y la realidad de los titulares de los datos personales entienden.

ABSTRACT

The present research, within the limitations of methodological synthesis imposed for this investigation, seeks to be on a specific point (informed consent), a perfectible formula for the application of the Ecuadorian Organic Law on Personal Data Protection. Point that attends to the informed consent in its real dimension and seeking to be a contribution of practical application in

documents and formats to be applied by a first class Financial Institution, of course, seeking to comply with the rights and principles enshrined in the aforementioned regulation. Although this work has been developed on the ideological basis received in the master's degree studied by the authors, it evidences their own line of thought that in several points questions the uncertainty in which the central norm, which is the umbrella of this work, will be effectively practiced in all areas. In the authors' opinion, this work is an effective contribution in the practical documentary development for the Financial Institution analyzed, a result that is evidenced in the Annexes to the work, which systematically gather most of the aspects worked throughout this document. Concluding that with a lot of effort it is possible to achieve certain harmony between what the norm intends and the reality of the holders of personal data understand.

Tabla de contenido

1. INTRODUCCIÓN.

1.1 Contexto del Entorno Interno de la Organización:

1.1.1 Reseña histórica.-

La compañía en la que se realiza este proceso de investigación, es una entidad financiera AAA constituida en el Ecuador en el año 1973, mantiene operaciones en todo el territorio ecuatoriano, prestando sus servicios a más de quinientos mil clientes. Su solidez, amplia cobertura nacional y su enfoque en el sector productivo; así como su liderazgo en servicios y actividades de comercio exterior le ha permitido ser el cuarto banco más solvente y grande del país. Por las cifras de su gestión y su sobresaliente trayectoria, por seis años consecutivos ha sido considerado como la entidad financiera más eficiente del Ecuador. Forma parte del Grupo IF que opera en América y es uno de los principales grupos financieros-industriales de la Región. (BANCO INTERNACIONAL S.A., 2022)

1.1.2 Misión y visión de la empresa.-

"*La misión de esta entidad financiera es ser más, respondiendo con solidez, eficiencia y calidad de las necesidades financieras de sus clientes. Su visión es ser el mejor Banco del Ecuador por medio de un crecimiento sólido y rentable, de su talento humano, prudencia en la gestión integral de riesgos, en su calidad y servicio, ser eficientes y productivos. Los valores corporativos que le caracterizan son; ejemplaridad, solidez, decisión y cercanía*." (BANCO INTERNACIONAL S.A., 2022)

1.1.3 Productos y servicios de la organización.-

Si bien esta entidad financiera tiene la facultad de atender a sus clientes con todos los productos y servicios que el Código Orgánico Monetario y Financiero permite, se ha especializado en productos enfocados en las grandes corporaciones y las más grandes compañías del País brindando financiamiento productivo y amplias facilidades en operaciones de comercio exterior. Empeñando sus esfuerzos en los últimos años en lograr un salto tecnológico para brindar a sus Clientes canales modernos y eficientes que agiliten todos sus procesos, buscando los mayores beneficios para aquellos. (BANCO INTERNACIONAL S.A., 2022)

1.1.4 Clientes de la organización.-

En base a la entrevista realizada al Gerente de Inteligencia de Negocios de la institución, esta entidad financiera cuenta con más de 500.000 clientes a nivel nacional. Desde su constitución ha trabajado continuamente para el desarrollo y oferta de servicios financieros de calidad, con una visión a largo plazo y con una oferta de valor clara y enfocada tanto a pequeñas, medianas y grandes empresas, además de banca personas y sus familias. Actualmente esta entidad financiera tiene 53.556 clientes cuentacorrentistas, de los cuales 17.933 son personas jurídicas y 35.623 son personas naturales. Estos clientes acceden a los servicios ofrecidos por la institución a través de los diferentes canales; presenciales, Banca Móvil, etc. (Pico, 2022)

1.1.5 Proveedores de la organización.-

Al ser una entidad financiera, para la contratación de prestación de servicios con sus proveedores, requiere regirse a lo establecido en la Codificación de Resoluciones de la Superintendencia de Bancos, en especial a lo señalado en “Libro I.- normas de control para las entidades de los sectores financieros público y privado en relación a servicios provistos por

terceros". Para lo cual, sus proveedores deben cumplir con una serie de requisitos y los contratos deben contener un clausulado mínimo según lo previsto en el referido ordenamiento jurídico. En la actualidad esta entidad financiera tiene más de 65 proveedores de servicios, en los que destacan; las prestadoras de servicios auxiliares del sistema financiero, servicios complementarios como lo son; seguridad, limpieza y alimentación, prestadores de servicios tecnológicos, proveedores de internet, entre otros. Estos son contratados con la finalidad de cumplir su giro de negocio de intermediación financiera y brindar productos y servicios de calidad y seguros para sus clientes. (Superintendencia de Bancos, 2022)

1.1.6 Principales competidores de la organización.-

De conformidad a reportes de data e información elaborados por la Asociación de Bancos para el mes de febrero del año 2022, esta entidad financiera es el sexto banco más grande del Ecuador y actualmente es el banco con la mejor Rentabilidad Patrimonial (ROE) dentro del sistema financiero nacional, con un 14.2%, de activos productivos con 94.99% frente al total; y su mejor eficiencia 2.9%. Sus competidores directos son; el Banco de Guayaquil, Produbanco, Banco Bolivariano y Banco del Austro. (Asociación de Bancos del Ecuador, 2022)

1.1.7 Estructura tecnológica y de innovación de la organización.-

En base a la entrevista realizada a personal de la Vicepresidencia de Operaciones y Tecnología de la entidad financiera objeto de este trabajo de investigación, realizada en el mes de marzo de 2022, se pudo conocer y determinar que esta entidad financiera, se encuentra en un constante proceso de renovación tecnológica. Es por eso, que en el año 2020 actualizó su Core Bancario y realizo la implementación de soluciones tecnológicas mediante el proyecto Gibs. Este Banco, a partir de dicho año se ha caracterizado por priorizar servicios y experiencias digitales

más ágiles, sencillas y ciberseguras para sus clientes, por lo que, en los últimos dos años ha realizado actualizaciones en su página web, banca online y banca móvil. El objetivo de esta institución de cara al futuro, es ser un Banco Ciberresiliente y ofrecer a sus clientes cada vez más servicios de forma digital y a través del uso de las diferentes herramientas tecnólogas. Para lo cual, se creó una gerencia en Transformación Digital e Innovación, con la finalidad de mejorar la experiencia de sus clientes, impulsar a una cultura organizacional basada en innovación y ser más competitivos en el mercado financiero ecuatoriano. (Moreano, 2022)

1.2 Contexto del entorno externo de la organización:

1.2.1 Entorno económico del Ecuador.-

La situación económica del Ecuador no es la mejor y mucho menos después de la crisis petrolera y de más de una década en la que se vio afectado por los casos de corrupción y los problemas económicos generados en el país, tal como se desprende de los procesos judiciales e investigativos que han sido puestos en conocimiento de la población. “La emergencia sanitaria causada por la COVID-19 generó una profunda recesión que provocó un repunte de la pobreza. Esta crisis amplificó los desequilibrios macroeconómicos que el país estaba intentando subsanar desde el fin del boom de los precios del petróleo”. (Banco Mundial, 2022).

No obstante de aquello, actualmente el sistema financiero nacional se encuentra sólido y con excelentes índices de liquidez y solvencia. No es la excepción de la entidad financiera en sobre la que versa esta investigación, que cerró el ejercicio fiscal 2021 con una utilidad neta de USD 42.049.561,31, y un crecimiento del 33% en relación al ejercicio fiscal 2020, año en el que el país y el mundo se vio afectado por la pandemia COVID-19. Cabe señalar que según los índices económicos generados por la Asociación de Bancos Privados del Ecuador, ASOBANCA “*el*

crecimiento de la economía ecuatoriana cerró el 2021 con 4,2%. Este aumento está apalancado por el plan de vacunación, incremento de remesas, mayor acceso a créditos, inversión extranjera y desempeño de las exportaciones"**.** (Asociación de Bancos del Ecuador, 2022)

1.2.2 Entorno político del Ecuador.-

El gobierno actual del Ecuador busca crear oportunidades para los ecuatorianos a través de un Plan de Gobierno focalizando acciones en cinco ejes: económico, social, seguridad integral, transición ecológica e institucional. (Banco Mundial, 2022). Plan que está siendo obstaculizado por las funciones legislativa, judicial y la mal llamada "función de Transparencia y Control Social", al punto de volver ingobernable la situación al Ejecutivo. El más claro ejemplo de lo mencionado, es la resistencia por parte de la Asamblea Nacional a los diferentes Proyectos de Ley presentados por el Presidente de la Republica y de las diferentes fuerzas políticas que se han enfocado en atacar al gobierno actual.

En el Ecuador las entidades financieras luchan por tener una aceptación por parte de la sociedad en general, pese a que el sector financiero y bancario ha sido de gran soporte y apoyo a la situación económica del país en los peores momentos de crisis y contribuyen con el crecimiento y desarrollo económico de grandes, pequeñas y medianas empresas, así como el de personas naturales. Esta resistencia se debe gracias a decisiones y acciones gubernamentales de gobiernos anteriores que han buscado desprestigiar a la banca y a sus diferentes instituciones, pretendiendo afectar a un sector productivo fundamental como es el financiero. Cabe señalar que las entidades financieras, son las que mayor carga impositiva tienen y la que más pagan impuestos al fisco.

1.2.3 Entorno socio cultural del Ecuador.-

En el Ecuador cada vez existen más usuarios del sistema financiero y en los últimos 4 años se incrementó en 3.7 millones de personas. Esto se debe a que hoy en día, cada vez es más frecuente la utilización de otros medios de pago adicionales al efectivo. Según cifras del Banco Central del Ecuador a septiembre del 2020, 8.5 millones de adultos se encuentran incluidos en el sistema financiero nacional. Esto se resume en una cifra que evidencia que 75 de cada 100 ecuatorianos adultos tiene acceso a servicios y productos financieros, de los cuales 72% de esa población cuenta con cuentas de ahorros y el 4% de cuentas corrientes. Dicho esto, la entidad financiera en la que versa esta investigación, abarca aproximadamente el 17% de la población de clientes del sistema financiero que mantienen cuentas corrientes en el Ecuador. (Banco Central del Ecuador, s.f.) Estas cifras destacan el buen manejo de las entidades financieras y la confianza que han generado en el usuario del sistema financiero, a través de buenas prácticas y de la promoción de la inclusión financiera en el país.

Estas cifras crecen anualmente gracias a que las entidades del sistema financiero han venido desarrollando productos y servicios que se adaptan a las necesidades de cada segmento, se ha ampliado la cobertura de los sistemas financieros y por la reducción de la brecha digital que se busca en el país. El Banco Interamericano de Desarrollo (BID), señala que "*la inclusión financiera hace referencia al acceso a servicios financieros (crédito, ahorro, seguros y servicios de pago y transferencias) formales y de calidad, y su uso por parte de hogares y empresas, bajo un marco de estabilidad financiera para el sistema y los usuarios*". (Banco Interamericano de Desarrollo (BID), 2015) Es importante destacar que para para poder referirse a inclusión financiera, es necesario que exista una regulación óptima que fomente la inclusión financiera, se implementen derechos que protejan al consumidor del sistema financiero y que se promueva la educación financiera.

1.2.4 Entorno tecnológico del Ecuador.-

El desarrollo de las sociedades siempre ha estado marcado por la presencia de la tecnología y hoy en día, con mayor presencia de las tecnologías digitales**.** Las Naciones Unidas establecen que:

> *"Las tecnologías pueden ayudar a que nuestro mundo sea más justo, más pacífico y más equitativo. Los avances digitales pueden apoyar y acelerar el logro de cada uno de los* ***Objetivos de Desarrollo Sostenible,*** *desde el fin de la pobreza extrema hasta la reducción de la mortalidad materna e infantil, la promoción de la agricultura sostenible y el trabajo decente, y el logro de la alfabetización universal. Sin embargo, las tecnologías también pueden amenazar la privacidad, comprometer la seguridad y alimentar la desigualdad. Tienen implicaciones para los derechos humanos y la actividad humana. Al igual que generaciones anteriores, nosotros, gobiernos, empresas e individuos, tenemos que decidir cómo aprovechar y gestionar las nuevas tecnologías"*. (Naciones Unidas, 2022).

El reducir la brecha digital en el Ecuador, generaría igualdad de oportunidades, más acceso al conocimiento, inclusión social, creación de plazas de empleo, difusión de la cultura, ayudaría en el mejoramiento de la productividad, desarrollo de nuevos sectores, ahorro de costos y de tiempo, contribuiría en la eficiencia de los servicios públicos, entre otros.

A raíz de la emergencia sanitaria causada por Covid-19 varias actividades dejaron de ser presenciales en el país y se convirtieron en virtuales, lo que produjo que, durante el 2020, el internet sea un "servicio básico" para el trabajo, los estudios y la salud. Si bien esto aceleró la digitalización, actualmente existe una considerable brecha de asequibilidad y accesibilidad del internet y de las tecnologías digitales en el Ecuador. De conformidad al estudio realizado por el Banco Interamericano de Desarrollo (BID), Banco de Desarrollo de América Latina (CAF),

Instituto Interamericano de Cooperación para la Agricultura (IICA) y Microsoft, "*un 32% de la población de América Latina y el Caribe, o 244 millones de personas, no accede a servicios de internet. El estudio, que concentró su trabajo en 24 países, revela que un 71% de la población urbana cuenta con opciones de conectividad, ante menos de un 37% en la ruralidad*". (BANCO DE DESARROLLO DE AMÉRICA LATINA, 2021).

1.2.5 Entorno ambiental del Ecuador.-

En base a entrevistas realizadas al oficial ambiental de la entidad financiera sobre la que se ha basado este trabajo de investigación, en el mes de mayo de 2022, se ha calculado que en el 2021 la entidad financiera consumió un total de 3334 toneladas de CO2, equivalente al consumo de 7065 barriles de petróleo, o el consumo de 343397 galones de gasolina o 658 autos a gasolina conducidos durante un año. Dentro de los procesos que mayor contaminación generan, es el consumo de electricidad que representa el 23%, la movilización de colaboradores el 19%, transporte de valores y valija el 14% y la visita de clientes el 8%. Es por esto, que como objetivo del 2022 y de los años siguientes, esta entidad financiera se ha planteado reducir su huella de carbono en al menos un 20%. Para lograrlo se encuentra implementando teletrabajo, promoviendo proyectos de transformación digital y banco digital, campañas de reducción de utilización de vehículos y utilización de bicicletas y otros en sus colaboradores, campañas reducción de impresiones de papel, entre otras prácticas que seguro contribuirán con alguna mejora en el medio ambiente del Ecuador y el mundo. (Iturralde, 2022).

1.3 Problema de la investigación.

La Ley Orgánica de Protección de Datos Personales publicada en el Ecuador el día 26 de mayo de 2021, consagra una serie de obligaciones y un régimen de sanciones pecuniarias frente al

incumplimiento de los principios y normativas consagradas en la referida Ley. La entidad financiera sobre la que se basa este trabajo de investigación, no mantiene a la fecha debidos soportes documentales en relación al consentimiento informado que deben conferir los titulares de datos personales. Por lo que, de conformidad con lo establecido en esta Ley, para garantizar los derechos de los titulares de datos personales a ser utilizados, requiere implementarlo dentro de sus contratos y formularios.

2. REVISIÓN DE LITERATURA

Analizadas que han sido varias fuentes serias de consulta en Internet, podemos comentar que existe una vasta difusión y lecturas sobre el eje central del objeto de este trabajo, el CONSENTIMIENTO INFORMADO y la LEY ORGÁNICA DE PROTECCIÓN DE DATOS PERSONALES, considerando más de 20 Tesis de Pre grado y algunos títulos de connotados autores como: Pablo A. Palazzi, José Luis Piñar Mañas, Lina Ormelas Núñez, publicados dentro de los últimos 2 años; hemos apreciado desde marcos teóricos y conceptuales anteriores y posteriores al 26 de mayo de 2021, fecha de la expedición de la referida Ley en el Ecuador, evidenciando que todos, destacan las deficiencias normativas, frente a los derechos que se pretende precautelar, particularmente el alcance del Consentimiento Informado que otorgan los usuarios del sistema financiero sobre sus datos personales. Dando realce a la valoración y/o monetización del dato como un activo de suma importancia; dejando de lado planes más cercanos que permitan su implementación efectiva, tema que lo hemos visto en propuestas de valor de algunas empresas Consultoras y Auditoras.

2.1 Antecedentes teóricos del problema.

Según lo analizado y referido previamente, de las investigaciones efectuadas nos queda claro que si bien los alcances, historia, antecedentes y proyecciones que se han desarrollado sobre la Ley de Protección de Datos Personales han sido abundantemente tratados con más o menos profundidad en el mundo, pero específicamente sobre planes de implementación de la misma, o en lo que se refiere al Consentimiento Informado, desde una óptica académica, no se han encontrado trabajos que merezcan su referencia, menos en el Ecuador.

Hallando únicamente ciertas aproximaciones a dicho alcance desde una visión práctica exclusivamente desde propuestas comerciales que han presentado algunas empresas Auditoras y Consultoras, que en general han presentado planes de implementación atados a paquetes de software que comercializan, mismos que entendemos buscan establecer controles y restricciones para el manejo de datos vía procesos de anonimización de los datos, considerando al consentimiento informado como un aspecto secundario. Lo cual a nuestro entender viene a ser un enfoque insuficiente, toda vez que los alcances de la referida Ley demandan de procesos más robustos, en especial la necesidad aterrizar en Implementación que se formularán como sugerencias a estructurar en formularios y contratos, para que tenga vida real dicho consentimiento frente al cumplimiento de la normativa.

En línea de lo señalado, consideramos que la problemática de la Implementación de la Ley de Protección de Datos Personales en términos generales y no se diga en un aspecto específico como el que tratamos en este documento, ha sido tratada exclusivamente desde una visión académica normativa y bajo las mismas formas clásicas de entender los derechos y principios de primera o segunda generación. Lo cual a nuestro entender dista mucho de lo que una implementación de un derecho de tercera generación debería contener. Esto bajo la premisa que el mundo que actualmente conocemos es dirigido por lo que se ha venido a llamar como un economía

digital, en la cual cientos de miles de transacciones y procesos se ejecutan de manera automatizada, evidenciando que las nuevas tecnologías están desarrollando factores del crecimiento y producción de riqueza, llegando a emplearse terminología como “capitalismo de la vigilancia de datos”. Por las evidentes ventajas monetarias que representan para las diferentes industrias el controlar la información de preferencias y desarrollo de patrones de conducta sobre la data que es almacenada y conocida por todos los entes a los cuales se les brinda abiertamente nuestra información personal. No por ello dejaremos de reconocer y someramente referir los posibles riesgos y afectaciones que trae consigo el dinamismo tecnológico frente al tratamiento correcto de datos personales y consentimiento informado por parte de los clientes del sistema financiero.

Ante lo expuesto consideramos que se ha abordado el tema materia de este ensayo de formas más bien doctrinarias que no consideran los factores prácticos que cualquier cambio normativo tiene, en especial frente a un ente que por su naturaleza está llamado a conocer y procesar información personal y sensible, como lo es la banca. En donde es fundamental contar con documentos, formularios y contratos en los que se incluya el consentimiento libre, especifico e informado de los clientes para el tratamiento de sus datos personales.

De las investigaciones en la literatura científica que pudo ser revisada, se aprecia que la gran mayoría de las investigaciones que se han realizado sobre el tema objeto de este trabajo, atiende a los casos y su análisis se fundamenta en fuentes secundarias que reprocesan y condensan cierta información de primera mano, que diversos autores han plasmado en libros y tesis que desarrollan sus escritos sobre conceptos y principios conceptuales. Puntualizando que esta afirmación alude a la Normativa base sobre la que planteamos nuestra investigación, el Consentimiento informado en la Ley Orgánica de Protección de Datos Personales. Sobre el mismo punto consideramos relevante el indicar que este trabajo va más allá de la base normativa, ya que

nos permitimos desarrollar un plan de implementación, acotado a la inclusión del Consentimiento Informado en; documentos, formularios y contratos a ser utilizados por el BANCO, Institución Financiera a la cual los maestrantes prestamos nuestro contingente profesional y que en dicho caso contaremos con fuentes primarias de información, que provendrán de testimonios y evidencias directas.

El presente trabajo, lo estructuramos en atención a un caso concreto, el plan de implementación del Consentimiento Informado en documentos, contratos y formularios a ser empleados por la entidad financiera objeto de este trabajo de investigación, en cumplimiento de la Ley Orgánica de Protección de Datos Personales, considerando únicamente como muestras la estructura, alcance, organigrama y niveles de aprobación ya definidos por y para la referida Institución Financiera, buscando un plan que evidencie eficiencia en los manuales y procedimientos y un absoluto complimiento normativo de acuerdo a los estándares y apetito de riesgo que tiene la Institución.

Hemos considerado el emplear fuera de las bibliotecas propias de los autores de este texto, los buscadores bibliográficos a través de Internet que permiten la búsqueda específica académica, tomando como fuente principal a la información que en su página Web, presenta la Red Nacional de Investigación y Educación del Ecuador (REDCEDIA); así como algunos de los libros que en los últimos cinco años se han presentado sobre el Consentimiento Informado y la Protección de Datos Personales y que se han encontrado en la página de Google Académico, accediendo a aquellos a través de la Red de Bibliotecas que se habilitan desde la página Web de la biblioteca de la UDLA.

Como hemos referido a lo largo del texto hasta el momento, el trabajo ha sido proyectado de la forma más acotada y específica posible considerando el contexto de la aplicación de la Ley

Orgánica de Protección de Datos Personales en lo atinente a obtención de un consentimiento informado de parte de los clientes del Banco generando un plan de Implementación y documentación que atienda a los requerimientos de la referida Ley en lo que concierne al consentimiento informado. Plan que deberá ser implementado hasta 26 mayo del año 2023, fecha en la que se espera, entre en vigencia plena las sanciones pecuniarias ante el incumplimiento de obligaciones normativas. Reconociendo dichas situaciones -realidades de cumplimiento normativo- y alcance el trabajo se ha sido diagramado y será estructurado.

Finalmente, hemos elegido y considerado, que dada la naturaleza del trabajo que deseamos implementar seguiremos una ruta de investigación mixta que considere información cuantitativa y cualitativa en atención al referido apetito de riesgo y alcance numérico de la masa de clientes sobre la que centraremos el análisis, siempre bajo la premisa del cumplimiento normativo en lo que concierne al pleno cumplimiento de la Ley, abordando la labor bajo el conocimiento empírico que nos brinda el ser funcionarios de la referida Institución Financiera, sumado a la experticia que como abogados financieros hemos adquirido.

3. IDENTIFICACION DEL OBJETO DE ESTUDIO.-

La presente Investigación tiene como objeto central el estudio en la Implementación del consentimiento informado en cumplimiento a lo establecido en la Ley Orgánica de Protección de Datos Personales del Ecuador. Para su aplicación se tomará los documentos y formularios a ser empleados por Banco. El periodo temporal que abarcará la investigación corresponde al año del 2022.

4. PLANTEAMIENTO DEL PROBLEMA.

Se basa en el título de este trabajo, sobre la Ley Orgánica de Protección de Datos Personales publicada en el Ecuador el día 26 de mayo de 2021, consagra una serie de obligaciones y un régimen de sanciones pecuniarias frente al incumplimiento de los principios y normativas consagradas en la referida Ley. La entidad financiera objeto del presente trabajo de investigación, no mantiene a la fecha debidos soportes documentales en relación al consentimiento informado que deben conferir los titulares de datos personales. Por lo que, de conformidad con lo establecido en esta Ley, para garantizar los derechos de los titulares de datos personales a ser utilizados, requiere implementarlo dentro de sus contratos y formularios. A fin de blindar y ahorrar inconvenientes al Banco y sus Clientes.

5. OBJETIVO GENERAL.

Siendo nuestro Objetivo General el desarrollar, el cómo se va a Implementar el consentimiento informado en documentos y formularios del Banco. en cumplimiento a la Ley Orgánica de Protección de Datos Personales publicada en el Ecuador, hasta marzo de 2023, con el fin de cumplir con las obligaciones consagradas en dicho cuerpo normativo y evitar sanciones pecuniarias a la institución.

6. OBJETIVOS ESPECÍFICOS.

Visualizando como objetivos específicos que esperamos poder atender con nuestro trabajo son:

1.- Identificar los datos personales que se busca proteger y sobre los cuales se pretende dar un aprovechamiento legítimo y autorizado, considerando los conceptos del capitalismo de la vigilancia de los datos.

2.- Describir las barreras que prevemos el consentimiento informado, podría tener.

3.- Establecer los procesos, su inclusión en manuales de procedimientos y formularios adecuados que cumplan con los requerimientos normativos y que pondremos a disposición de la Administración del Banco a fin de que se autorice su implementación y aplicación.

7. JUSTIFICACIÓN Y APLICACIÓN DE LA METODOLOGÍA.-

A continuación justificamos la metodología que se va a utilizar para alcanzar los objetivos específicos planteados:

1.1. Al ser un fenómeno poco conocido, en el Ecuador, tanto en lo teórico como en lo práctico, el nivel de estudio que emplearemos es el exploratorio que se estructura en base a revisiones bibliográficas, conocimientos previamente y opiniones de expertos en el tema.

1.2. Por las características de los autores, la atención al problema planteado y el beneficiario del resultado del proceso de investigación, consideramos que la modalidad de investigación será principalmente documental, buscando ser un proyecto de desarrollo para el Banco.

1.3. Toda vez que se utilizará en el proceso de búsqueda de una solución al problema planteado, a partir de la información conocida y recopilada consideramos aplicar el método inductivo-deductivo, hasta llegar a conclusiones.

1.4. En el caso objeto de nuestro trabajo consideramos que no es necesario hacer cálculo de población y muestra toda vez que es análisis netamente cualitativo que no obliga el uso de un cálculo de una muestra.

1.5. Dentro del proceso metodológico, la selección de instrumentos válidos y confiables de la investigación que consideramos emplear es el Análisis de documentos y el manejo de entrevistas.

1.6. Para el desarrollo del procesamiento de datos se va a utilizar las herramientas tecnológicas que brinda Microsoft en su paquete de Office, tales como Word, Excel y PowerPoint. En

el cual el manejo de todos los textos van a ser procesados a través de Word, en el caso de recurrir al procesamiento de datos utilizaremos Excel y para la presentación final del proyecto utilizaremos PowerPoint.

1.7. Secuencia detallada para el cumplimiento de los objetivos, especialmente para los capítulos 1 y 2 referidos en el Índice Temático, dado que lo consideramos en aquellos el marco conceptual del trabajo, en un máximo de aproximadamente 7 páginas por cada capítulo, dejando el capítulo 3 al aporte específico desarrollado en base de los conocimientos adquiridos.

1.7.1. Análisis normativo de obligaciones y sanciones, en los autores y títulos referidos en el numeral 2 de la página 7 del presente documento.

1.7.2. Instrumentación de documentos y formularios del Banco, propuesta/borrador de trabajo.

1.7.3. Validación del consentimiento informado en dichos documentos, con usuarios capacitados dentro de la Institución.

1.7.4. Revisión de Manuales y procedimientos del Banco, para luego de análisis de procedencia e inclusión del consentimiento informado en los manuales de procesos y procedimientos del Banco.

1.7.5. Validación final del cumplimiento normativo con los textos modificados.

1.7.6. Presentación para aprobación de los textos en la alta gerencia del Banco.

1.7.7. Socialización con el Delegado de Protección de Datos y posterior capacitación del manejo y aplicación de los documentos.

8. MARCO CONCEPTUAL.-

8.1 Generalidades

Partimos de un análisis general sucinto de los conceptos y principios que a nuestro criterio conforman la espina dorsal de la norma y que son enunciados en la Ley, con énfasis en el consentimiento informado, para aterrizar en procesos de Implementación que se formularán como sugerencias a estructurar en formularios y contratos, para que tenga vida real dicho consentimiento frente al cumplimiento de la normativa, en los diferentes productos que el Banco comercialice. Conceptos como son: Consentimiento, Consentimiento Informado, vicios del Consentimiento las Bases de datos o ficheros, Datos personales crediticios, Fuente accesible al público, la Autoridad de Protección de Datos Personales, Delegado de protección de datos, Responsable de tratamiento de datos personales, Titular, Transferencia, Tratamiento, Vulneración de la seguridad de los datos personales como consideración a cualquier incidente de seguridad que afecta la confidencialidad y disponibilidad e integridad de los datos personales. Para lo cual se decanta en el siguiente marco conceptual.

8.2 Ley De Protección De Datos Personales.-

En el Ecuador desde el 26 de Mayo de 2021, efectivamente contamos con la Ley Orgánica de Protección de Datos Personales, misma que responde a una realidad que consideramos irrebatible, y esta es que se necesita, frente al avance de las tecnologías de la Información y Comunicación, mecanismos que eviten la transgresión a derechos fundamentales que bajo este nuevo mundo digital se pueden presentar. Debiendo aclarar que hablamos de derechos fundamentales al referirnos a los datos personales, dada la evolución que efectivamente ha tenido dicho concepto, como "… *una exigencia de la dignidad de la persona y del libre desarrollo de la personalidad*…[i]". (LEY ORGÁNICA DE PROTECCIÓN DE DATOS PERSONALES, 2021) Hoy en día se ha evolucionado no sólo a la simple valoración del dato intimo o sensible desde, un no simple recurso

de la intimidad de la persona, sino desde la trascendencia e impacto que puede tener los datos personales hasta referidos por algunos autores como los "inocuos" frente a cualquier sujeto en relación a individuos o colectivos, que con las referidas tecnologías pueden tener acceso a aquellos. Siguiendo la línea argumental de la relevancia que la teoría del mosaico, hoy podría tener.

Este enfoque si bien somero, no quiere dejar de desconocer lo que evidentemente tiene un sustrato económico de envergadura, toda vez que como lo hemos analizado en varias asignaturas de nuestra Maestría. Sin necesidad de, en este documento, mayor análisis podemos afirmar y creo que sin cuestionamientos que en el mundo moderno los datos de han convertido en elementos de valor casi incalculable, por sus alcances y potencialidad, tanto en positivo como en negativo. Tema que igualmente lo comentaremos brevemente en adelante.

8.3 Derechos de protección.

Dentro del enfoque aplicado a este trabajo y en especial al reconocimiento de los datos personales como la protección de aquellos por un mecanismo de defensa de derechos de la dignidad personal, como la propia determinación informativa que cada persona asume sobre sí. Como bien refería en clase nuestra profesora la Dra. Laura Nahabetián, "El dato soy Yo".

En este marco debemos regresar a ver, a los conocidos como derechos "ARCO Plus"; acceso, rectificación, cancelación y oposición. Que se soportan en principios definidos en nuestra LOPDP tales como son el de: juridicidad, lealtad, transparencia, finalidad, pertinencia y minimización de datos personales, proporcionalidad del tratamiento, confidencialidad, calidad y exactitud, conservación, seguridad de datos personales, responsabilidad proactiva y demostrada, aplicación favorable al titular, e independencia del control. Sin que podamos extendernos en mayores precisiones sobre cada uno de ellos, si debemos mencionar en este punto que: i) todos los referidos

derechos ARCO, se encuentran contemplados y debidamente tutelados en nuestro actual marco normativo, mediante mecanismos que en su oportunidad serán probados por nosotros como abogados conocedores de la materia, en la práctica para la efectiva protección de los derechos de las personas; y, ii) como referiremos en mayor detalle en el capítulo II de este trabajo, el consentimiento informado lo consideramos una de las piedras angulares para que se pueda dar un debido y adecuado cumplimiento de los derechos y principios referidos previamente, esto por el alcance y consecuencias frente a un concepto jurídico evidente, y este es, que cada individuo sólo puede brindar su consentimiento (como una adecuada manifestación de su voluntad) sobre algo que conozca en debida profundidad y alcance, como expresión indubitable de una efectiva autodeterminación informativa.

8.4 Tratamiento legítimo de datos personales.

En atención a lo referido, partimos por contextualizar dentro del marco normativo del Art. 7 de la Ley Orgánica de Protección de Datos Personales, lo que consideramos como un tratamiento legítimo y lícito de los datos personales conforme la referida norma enumera, destacando que: i) la norma tuvo la previsión y acierto de basar dicha enumeración en condiciones y no en conceptos rígidos que en el tiempo podrían quedarse cortos frente a los avances de la Ciencia y la Tecnología, permitiendo en un futuro un adecuado desarrollo pudiendo ser hasta jurisprudencial, de dichos elementos; y, ii) que la primera condición en la referida norma es el "consentimiento del titular para el tratamiento de sus datos personales, para una o varias finalidades específicas.".

Concepto que relevamos ya que sin entrar en las otras condiciones alternativamente previstas en la norma, tiene un particularismo recogido por legislaciones mucho más maduras en la materia de protección de datos personales y esto es que el consentimiento deba ser informado, en atención a las finalidades específicas a las cuales, dichos datos serán empleados. Tema por demás

interesante y que nos podría tomar muchísimo tiempo y discusión, dado lo importante que el "valor" dato, tienen en el mundo moderno, ya que como referimos previamente el dato en si es neutro, pero su empleo puede traer consecuencias positivas o negativas tanto para el titular como para terceros.

Afirmación que la sustentamos en que siempre se buscará maximizar el aprovechamiento de la información. Esto por considerar que es parte de la naturaleza humana, el buscar maximizar el beneficio y lo pragmáticos en que nos volvemos los seres humanos buscando el bienestar, por lo que el pedir a cualquier titular de sus datos que brinde su consentimiento para finalidades o actividades específicas, siempre debería estar limitado al concepto temporal de lo que se pretende hacer con cualquier dato al momento en que se brinde el consentimiento, en cualquiera de sus formas de expresión indubitable e inequívoca. Sobre este punto que si bien también lo hemos discutido abundantemente en nuestras clases de Maestría, tenemos una lectura personal que buscaría un máximo aprovechamiento de la data bajo el entendimiento de los fines positivos que podría tener, no por eso dejamos de reconocer que el espíritu y literalidad de la normativa a nivel internacional y en la nuestra Ley Orgánica de Protección de Datos Personales, es otro. La determinación del conocimiento que debe expresar el titular es limitado a una o varias finalidades específicas, y en dicho sentido hemos planteado los instrumentos que nos hemos permitido presentar a la Institución a la cual brindamos nuestros servicios y que constan como Anexos al presente Trabajo.

8.5 Protección de datos por diseño y por defecto.-

Sobre este punto, debemos partir de ciertas presiones que podrían ser vistas como técnicas, consideramos necesario dejarlas planteadas, toda vez que en el desarrollo y medición planteada de los conceptos de riesgo e impacto, que igualmente se aportan a este trabajo, son considerados y

estos es que el concepto de protección al que atendemos en los modelos propuestos como "consentimiento informado" para diferentes actores y finalidades en el Banco objeto de este trabajo de investigación, parte de la premisa que la protección en este enfoque atiende a la privacidad de la data y que la misma debe ser estructurada y atendida desde el diseño como el deber del responsable del tratamiento de tener en cuenta, y esto desde las primeras fases de concepción y diseño del proyecto que busca estructurar una serie de procesos, mecanismos, procedimientos e instrumentos (como los que proponemos) para precautelar el cumplimiento normativo que busca la LOPDP, bajo la base cierta que determinados tipos de tratamiento de datos personales podrían entrañan una serie de riesgos para ciertos derechos de los titulares en atención al estado de la técnica, naturaleza y fines del tratamiento, para lo cual, desde el diseño se ha de considerar el implementar las medidas técnicas, organizativas y de cualquier otra índole, con miras a garantizar el cumplimiento de las obligaciones que la LOPDP, nos impone a todos en materia de protección de datos personales. Y si bien estas presiones deben ser al alcance del diseño, no deja de existir variables que usualmente no pueden ser previstas o atendidas en una primera instancia, siendo allí donde ingresan los conceptos de la protección de los datos personales por defecto, sin ser esto otra cosa que la referencia a que el responsable dentro de sus competencias y capacidades de definición y niveles de autoridad, deba tener competencia y capacidad para aplicar las medidas técnicas y organizativas adecuadas con miras a que, por defecto, solo sean objeto de tratamiento los datos personales que sean necesarios para cada uno de los fines del tratamiento, en los términos de la normativa (principio de la menor exposición).

8.6 Transferencia de datos personales.-

En este punto, partimos por reconocer que el mismo podría ser tratado individualmente como un tema por separado, dada la relevancia y cuidado que ha puesto la normativa al proteger la

transferencia que los datos personales, podrían llegar a tener. Si bien esto no es algo que deba sorprender por las connotaciones económicas previamente referidas, toda vez que reconocemos a los datos como activos de altísimo valor, que debidamente procesados a efectos de ser monetizados (como actualmente ya ocurre) pueden ser útiles a cualquier conglomerado, sujeto o inclusive nación.

Por lo que, siguiendo la misma línea argumental regresamos a ver las estipulaciones que la Ley Orgánica de Protección de Datos Personales trae, en cumplimiento de las garantías y principios que la referida Ley busca precautelar, partiendo del alcance que las definiciones de la misma normativa nos trae al señalar que la transferencia de datos personales, es la:

> "*Manifestación, declaración, entrega, consulta, interconexión, cesión, transmisión, difusión, divulgación o cualquier forma de revelación de datos personales realizada a una persona distinta al titular, responsable o encargado del tratamiento de datos personales. Los datos personales que comuniquen deben ser exactos, completos y actualizados"*. (Ley Orgánica de Protección de Datos Personales, 2021)

Bajo dicha conceptualización, aparece como uno de los derechos consagrados en el artículo 12, de la referida Ley, se evidencia y nos parece relevante como específicamente la Transferencia de los Datos Personales, se determina como parte de los derechos que se buscan precautelar, como el derecho con el que contamos a la información y en consecuencia con la que debe contar el titular que otorga su consentimiento informado. Recalcando que los datos a ser transferidos de forma nacional o internacional contenida en el Artículo. 55; disposición transitoria Cuarta de la Ley Orgánica de Protección de Datos Personales, deben ser exactos, completos, actualizados, debiendo establecerse específicamente quienes pueden ser los destinatarios de dichos datos, sus clases; por supuesto soportando e informando cuales son las finalidades previstas y que motivan una posible

transferencia (LEY ORGÁNICA DE PROTECCIÓN DE DATOS PERSONALES, 2021). Estableciendo la normativa que nos ocupa claramente las garantías de protección mínimas que sobre la base de legitimidad el responsable del tratamiento de los datos personales debe precautelar en atención a la protección con la que debe contar el Titular de los mismos. Derecho que apreciamos va de la mano del derecho con el que cuenta todo titular, a la portabilidad de sus datos y que se encuentra igualmente consagrada en el Artículo 17 y específicamente en el capítulo V, referente a la Transferencia o Comunicación y Acceso a Datos Personales por Terceros. Estableciendo dichas premisas y alcances, bajo lo que expresamente requiere el segundo inciso del Artículo 33 de la Ley Orgánica de Protección de Datos Personales, que establece:

> *"(...) Se entenderá que el consentimiento es informado cuando para la transferencia o comunicación de datos personales el Responsable del tratamiento haya entregado información suficiente al titular que le permita conocer la finalidad a que se destinarán sus datos y el tipo de actividad del tercero a quien se pretende transferir o comunicar dichos datos".* (Ley Orgánica de Protección de Datos Personales, 2021)

Cabe señalar que hemos tratado de materializar de igual forma en los instrumentos que hemos recomendado sean aplicados por la entidad financiera en la que basa este trabajo de investigación y que obran como Anexos a este trabajo, recordando que el incumplimiento de las disposiciones de la Ley Orgánica de Protección de Datos Personales dará lugar a la aplicación del régimen sancionatorio establecido en dicha Ley.

8.7 Delegado de protección de datos personales.-

Dada la extensión del presente trabajo de titulación no hemos considerado procedente el generar un análisis detallado de las obligaciones, funciones y atribuciones con las que debe contar

el delegado de Protección de Datos Personales, ya que se encuentran perfecta y claramente establecidas en el capítulo VII de la LOPDP, pero si consideramos procedente en este punto y al ser el Delegado de Protección de Datos Personales una simple persona natural, con todos los sesgos y limitaciones que aquello podría tener, y que dentro de la normativa es visto como un elemento relevante y con muchas responsabilidades asignadas en la protección de los datos personales, nos alejamos de una análisis doctrinario o purista del concepto, y vemos que desde un enfoque práctico dicha persona debe tener destrezas y habilidades que consideramos poco o nada desarrolladas a la fecha en el mercando profesional ecuatoriano, ya que al ser el responsable de informar a encargado del tratamiento de sus obligaciones legales. Este debe ser un conocedor profundo de la Ley Orgánica de Protección de Datos Personales, con una visión muy amplia del derecho comparado, toda vez que en nuestro país aún faltan por definirse y nombrarse varios elementos que integrarán un sistema adecuado de protección de datos personales;

Así mismo debe tener un grado jerárquico superior en las diferentes organizaciones que manejan data en las proporciones y condiciones que la Ley establece; ya que no es poca cosa el tener que velar y supervisar el cumplimiento normativo. Para cumplir con tan amplia labor consideramos que fuera de su nivel jerárquico debe contar con igualmente destrezas técnicas que le acerquen a un conocimiento profundo de la organización (sus sistemas y procesos) a la cual soporta en la materia que nos ocupa y a su giro de negocio y mercado, ya que "debe tomar medidas tecnológicas, físicas, administrativas, organizativas y jurídicas necesarias para prevenir, impedir, reducir, mitigar y controlar los riesgos y las vulneraciones identificadas".

Además el perfil del referido Delegado debe tener una capacidad no cuantificable y de difícil evaluación a priori, y es una ética intachable, ya que por la naturaleza y delicado desempeño de sus funciones estará siempre expuesto a un sin número de tentaciones y presiones, que si bien son

fácilmente predecibles, son muy difíciles de manejar en el día a día de las organizaciones, ya que seguimos hablando de conceptos nuevos en el País con activos de incalculable valor y con niveles de afectación igualmente incalculables, frente a vulneraciones.

8.8 Multas y sanciones.-

Sobre ese punto, Capítulo XI de la Ley Orgánica de Protección de Datos Personales, que versa sobre Medidas Correctivas, Infracciones y Régimen Sancionatorio, consideramos que es el más controversial sobre el cual no quisiéramos ahondar, ya que como lo hemos expresado a lo largo del desarrollo de nuestra malla académica, no consideramos existe una institucionalidad fuerte y adecuada que respalde, a priori a autoridades y estructuras burocráticas que garanticen un adecuado cumplimiento de los loables principios y derechos que la Ley Orgánica de Protección de Datos Personales , puede contener.

Nos limitamos a comentar, para triste recordación lo ocurrido como ejemplo en varios casos que se generaron años atrás y que trajeron polémicas a nivel nacional sobre la aplicación de la Ley Orgánica de Regulación y Control del Poder de Mercado y su Superintendencia.

8.2 Consentimiento.-

8.2.1 Consentimiento Informado.-

Dentro del marco de este trabajo, partimos de la definición que trae la propia Ley Orgánica de Protección de Datos Personales, que en su artículo 4, señala que el consentimiento es la "*manifestación de la voluntad libre, específica, informada e inequívoca, por el que el titular de los datos personales autoriza al responsable del tratamiento de los datos personales a tratar los mismos.*" (LEY ORGÁNICA DE PROTECCIÓN DE DATOS PERSONALES, 2021)

Convirtiendo a la referida manifestación de voluntad, en un elemento gravitante, ya que, para los efectos de aplicación de la referida Ley, la misma debe cumplir con las características de ser libre, es decir sin que medie ningún vicio del consentimiento; que sea específica, esto es que este claramente delimitada en su alcance, objeto y destino; así como informada e inequívoca, lo cual exige que el titular de los datos personales que otorga su autorización mediante una expresión clara e inequívoca de su voluntad, se encuentre en capacidad de hacerlo sobre la base de que ha sido inteligenciado sobre lo que está otorgando y para qué. Elementos que a nuestro criterio responden a la importancia que el legislador ha brindado a los derechos fundamentales que se están buscando precautelar en la Ley Orgánica de Protección de Datos Personales. Ya que el fin último de la referida manifestación de voluntad, es permitir el tratamiento legítimo y lícito debidamente autorizado de los datos personales, en primera instancia por el responsable del tratamiento.

Si bien consideramos que el desarrollo de este concepto (consentimiento) según la Ley Orgánica de Protección de datos Personales, es completo y correcto, al sistematizar todos los derechos y principios que se deben garantizar en un desarrollo normativa de tercera generación y atendiendo a la autonomía de la voluntad del titular de los datos personales. Lo que caracteriza al consentimiento informado según Bedrossian y Fernández, en un artículo publicado en 2001, citados por Roberto Cañete, se refieren a algunas características que atienden usualmente a las generalidades éticas del Consentimiento en relación con el área que detectamos en nuestra investigación, ha sido la más desarrollada al respeto por su relevancia, la bioética. (Cañete, Guilhem, & Katia, 2012)

Señalando que, el consentimiento es un proceso de comunicación, que debe someterse a las características ya comentadas, que culmina con la autorización o no del titular para un tratamiento específico. Se conceptualiza al consentimiento como lo que es, un derecho del titular;

por lo que proporcionar la información sobre el alcance del tratamiento, es un deber del responsable del tratamiento. Siendo la información y la comprensión las herramientas decisivas para que el consentimiento sea otorgado en debida forma, atendiendo a la especificación de los alcances en orden a la frecuencia y gravedad y/o sensibilidad de los datos a ser tratados. Debiendo la información adecuarse a las condiciones particulares de cada titular, si bien esto un concepto por demás discutido, no menos digno de ser relevante. Pudiendo en el desarrollo de una relación de larga data requerirse nuevos y sucesivos consentimientos.
Y como ya se menciono debe ser claro que el Titular tiene derecho, entre otros a revocar su consentimiento en cualquier etapa del desarrollo de la relación con la Institución Financiera, sin que ello conlleve al detrimento en la calidad de su atención.

Si bien no es una de las características de las que venimos comentando, idealmente, el consentimiento debería otorgarse o no, después de contar con período adecuado de reflexión. Dado que no se trata de un mero acto administrativo y el responsable del tratamiento debería tenerlo siempre presente. Ya que todo consentimiento se invalida cuando, existe uno o varios vicios del consentimiento, por ejemplo en cuando la condición del Titular no le permita estar en condiciones de elaborar un juicio crítico al respecto como en caso de tratarse de incapaces declarados por ley (menores de edad, discapacitados mentales, etc.). Y terminamos este breve análisis señalando que el consentimiento no es una dispensa de culpa, si no se cumple con el deber de informar y advertir con información suficiente y de calidad, adecuando la información al nivel de quien la recibirá y precautelando la libre voluntad del Titular, sin coerción de forma que la comprensión se convierte en un elemento clave del Consentimiento, ya que aun cuando se hable el mismo idioma, es frecuente que existan malentendidos en la información que se comparte.

8.2.2 Vicios del consentimiento.-

8.2.2.1 Error.-

Partimos de una definición generalmente aceptada por varios tratadistas que señala que el error es el conocimiento falso de una cosa o un hecho y en consecuencia que el error como un vicio del consentimiento podría en un determinado escenario, generar una excepción dentro de un proceso contencioso en el que se debata sobre si un consentimiento informado para el tratamiento autorizado de datos personales en la Institución Financiera objeto del análisis, defendemos la hipótesis de que debe partir de las consideraciones de nuestro ordenamiento civil, que establecen a partir del Art. 1468 del Código Civil, conceptos que encasillan el alcance del vicio, al señalar que el error no vicia el consentimiento si versa sobre un punto de derecho y que en cambio sí lo vicia si existe error sobre la especie del acto o contrato que se celebrará o sobre el objeto o la identidad de la cosa específica que se transa y/o contrata, aclarando la normativa que la calidad del objeto transado, si puede ser motivo para viciar el consentimiento si fue dicha calidad o la persona (contra parte) lo que motivo la contratación. Puntos consistentes y que consideramos no reñidos con la LOPDP, pese a que debe ser objeto de importante atención procedimentalmente, ya que se deben minimizar los riesgos de que se pueda cuestionar que el Consentimiento, con el que se contará, fue plena y ampliamente informado al Titular, en su alcance, fin, tratamiento y destino. Respaldando así al Titular de los datos personales en el efectivo goce de todos los derechos que le asisten en la LOPDP.

8.2.2.2 Fuerza.-

Dentro de la misma lógica del punto anterior, la Fuerza podría viciar un consentimiento informado para el tratamiento autorizado de datos personales en la Institución Financiera objeto del análisis, de igual manera siguiendo la premisa de la guía que nos brinda el Código Civil (Art. 1472), sólo si dicho vicio puede dentro de un concepto de racionalidad influir de forma importante (fuerte) en atención a ciertas circunstancias y calidad de la persona que otorga su consentimiento; pudiendo influir cualquier tercero en su manifestación de voluntad o expresión del consentimiento por un justo temor. Dentro de los parámetros expuestos, vemos poco probable que en el caso analizado pueda ocurrir este vicio del consentimiento, toda vez que el acceso a los productos y/o servicios financieros no es potestativo o exclusivo de una sola parte y en consecuencia cualquier Titular de Datos Personales, puede optar facultativamente por requerir de dichos productos y/o servicios con cualquier Institución Financiera, atendiendo a sus preferencias, de tal forma que difícilmente se podrá oponer una excepción de este tipo para calificar que un consentimiento informado, pudo adolecer de un consentimiento viciado por fuerza.

8.2.2.3 Dolo.-

Y finalmente dentro del mismo hilo conductor podemos comentar que el dolo solamente podrá viciar el consentimiento si es un acto intencionado de una de las partes de la relación, aclarando que el dolo incidental es el que genera una obligación de indemnizar daños y perjuicios; y, que se evidencie que sin dicha actuación no se hubiere otorgado el consentimiento informado, dejando claramente establecido que el dolo no se presume, salvo los casos expresamente previstos por la Ley, y debe ser probado. Problema diferente sería la posibilidad de que el dolo fuese empleado por un tercero ajeno a la relación. Y si bien la interpretación de nuestro Código Civil, impide que dicho vicio del consentimiento pueda afectar a la relación a instaurarse entre las partes,

si bien la doctrina más moderna, tiende a visibilizar un hecho que el dolo cuando es aprovechado por uno de los contratantes conocedor del engaño, no puede beneficiarse del mismo.

De igual manera que en los comentarios del numeral que antecede, vemos poco probable que en el caso analizado pueda ocurrir este vicio del consentimiento, toda vez que el acceso a los productos y/o servicios financieros generalmente están amparados por un principio de "trust" universalmente extendido y que es pilar la confianza que se brinda por las entidades financieras a sus Clientes, por lo cual es jugar con un vicio del consentimiento que pueda poner en riesgo la reputación de la entidad financiera objeto del análisis, es para nosotros casi impensable. Ya que las consecuencias fuera de constituir una violación normativa ante el ente Rector (Superintendencia de Bancos) puede conllevar efectos impredecibles., concluyendo de igual manera que difícilmente se podrá oponer una excepción de este tipo para calificar que un consentimiento informado, pudo adolecer de un consentimiento viciado por dolo.

8.3 Consideraciones del consentimiento informado.-

El consentimiento informado en materia de protección de datos personales, es la manifestación expresa que confiere el titular de datos personales, para que terceros recolecten, almacenen, utilicen, transfieran cualquier información de carácter personal que le hagan identificable, dentro del alcance y términos previstos por la ley. Este consentimiento tendrá que ser expreso y no deberá adolecer de vicios del consentimiento. Para lo cual, el responsable del tratamiento deberá tratar estos datos con fines específicos y lícitos y garantizar que se cumplen con todos los principios consagrados en la Constitución de la Republica y la Ley. (Ley Orgánica de Protección de Datos Personales, 2021)

8.3.1 Tratamiento legítimo de datos personales.-

Tal como lo prevé el artículo 7 de la Ley Orgánica de Protección de Datos Personales, el tratamiento será lícito si se cuenta con el "consentimiento del titular para el tratamiento de sus datos personales, para una o varias finalidades especificas o si se tratan los datos personales en cumplimiento de obligaciones contractuales perseguidas por el responsable del tratamiento". (LEY ORGÁNICA DE PROTECCIÓN DE DATOS PERSONALES, 2021). Condiciones que son indispensables para que se pueda llegar a tratar los datos personales de usuarios o clientes del sistema financiero.

8.3.2 Condiciones revocatoria consentimiento informado.-

Tal como se ha detallado anteriormente, únicamente se podrá tratar los datos personales cuando se cuente con el consentimiento entregado por su titular en legal y debida forma, tal como se ha detallado anteriormente. Mismo que de conformidad con lo previsto en el artículo 8 de la Ley Orgánica de Protección de Datos Personales, "*podrá revocarse en cualquier momento sin que sea necesaria una justificación, para lo cual, el responsable del tratamiento de datos personales establecerá mecanismos que garanticen celeridad, eficiencia, eficacia y gratuidad, así como un procedimiento sencillo, similar al proceder con el cual recabó el consentimiento*". (LEY ORGÁNICA DE PROTECCIÓN DE DATOS PERSONALES, 2021) Para lo cual, el responsable del tratamiento deberá brindar las facilidades del caso y será encargado de gestionar y proceder con la revocatoria del consentimiento informado.

9. CONCLUSIONES Y RECOMENDACIONES.-

9.1 Plan de implementación del consentimiento informado.-

9.1.1 Recomendaciones modificación contratos y formularios.

El alcance de este trabajo de investigación, es definir el contenido de consentimiento informado para el tratamiento de Datos Personales, a ser implementado en documentos y formularios a suscribirse por clientes y usuarios de la entidad financiera sobre la que se basa este trabajo de investigación y que estos se encuentren dentro de los propósitos específicos y lícitos, conforme con lo establecido en la Ley Orgánica de Protección de Datos Personales. Por lo que, para poder cumplir con la normativa en cuestión y contar con buenas prácticas de Protección de Datos Personales, las áreas de Calidad de la Data, Jurídico y Riesgo Integral, en conjunto con la consultora extranjera, especialista en protección de datos personales, realizaron una Metodología de Evaluación de Riesgos y de implementación, con el fin categorizar el tratamiento de datos según responsables, áreas usuarias, tipo de dato, entre otras, y así contar con procedimientos y flujos para cada uno de estos. En este trabajo académico, se centró la investigación y desarrollo de los requisitos que debe contener el consentimiento informado en la categoría de clientes y usuarios de la entidad financiera objeto de este trabajo investigativo.

El artículo 4 de la Ley Orgánica de Protección de Datos Personales, establece que un Dato Personal "es aquel que identifica o hace identificable a una persona natural, directa o indirectamente". (Ley Orgánica de Protección de Datos Personales, 2021). Es por ello, que se ha elaborado documentos de consentimiento informado a ser suscrito por los usuarios del sistema financiero de la entidad financiera objeto de este trabajo investigativo y anexos de protección de datos personales a suscribirse con proveedores, cuando por la necesidad del servicio exista una relación de transferencia de información de responsable el tratamiento a encargado de Datos Personales, documentos que han sido elaborados en pleno cumplimiento del ordenamiento jurídico en materia de protección de datos. Además de estos documentos, esta entidad financiera se

encuentra trabajando en la implementación y uso de herramientas tecnológicas que contribuyan en la protección de datos personales de sus usuarios y clientes, para de esta forma garantizar plenamente sus derechos.

Esta entidad financiera en el desarrollo de su actividad económica, realiza varias operaciones financieras que involucran el tratamiento de Datos Personales de clientes y usuarios del sistema financiero. Por lo que, el objetivo de la implementación del consentimiento informado en documentos y formularios de esta entidad financiera, no solo busca cumplir con lo establecido en la Ley Orgánica de Protección de datos Personales, sino que, garantizar la protección de los derechos de las diferentes personas, para lo cual, se definió que los datos personales sujetos a tratamiento por parte del Banco, deberán someterse únicamente a la finalidad debidamente puesta en conocimiento y aprobada expresamente por parte de sus usuarios y clientes. Dicho esto, el Banco realizó un levantamiento de los datos que son recopilados, según cada uno de sus procesos, entendiendo cuál es su finalidad y pertinencia de solicitarlos, proporcionalidad de su tratamiento, tiempo de conservación y demás principios consagrados en el artículo 10 de la Ley Orgánica de Protección de Datos Personales (LEY ORGÁNICA DE PROTECCIÓN DE DATOS PERSONALES, 2021).

Este trabajo académico ha sido enfocado, en la implementación de soportes documentales en relación al consentimiento informado que deben conferir los titulares de datos personales, en la categoría de clientes y usuarios del sistema financiero. Siendo la categoría de “Clientes” la información que se obtiene de personas naturales que contratan los servicios y productos ofrecidos por la entidad financiera objeto de este trabajo investigativo, en el curso de su actividad principal y la de “usuarios” correspondiente a la Información que se obtiene de clientes y potenciales clientes con fines comerciales y de prospección comercial. Para lo cual, en atención a la metodología para

la implementación de riesgos en Protección de datos Personales de la entidad financiera objeto de este trabajo de investigación, prevista en el Anexo 1 de este trabajo, se realizó un check-list de cumplimiento normativo para estas categorías, con el fin de realizar un mapeo y contar con una matriz de hallazgos de posibles incumplimientos, dentro de los procesos del Banco en las referidas categorías. Habiendo realizado este ejercicio, se concluyó que si bien esta entidad financiera cumplía parcialmente con el marco normativo en materia de protección de datos personales, era necesario realizar modificaciones a ciertos procesos, formularios y contratos. Dicho esto, consideramos pertinente se cree el documento de consentimiento informado, mismo que deberá ser suscrito por clientes y usuarios de esta entidad financiera, mismas que se detallan a continuación.

En línea con las recomendaciones realizadas por la Comisión de la Unión Europea en lo que concierne al principio de transparencia, igualmente consagrado en la Ley Orgánica de Protección de Datos Personales, el consentimiento informado del BANCO, ha sido elaborado en un lenguaje fácil de entender, detallado de forma clara y concisa y cumpliendo con todos los requisitos del deber de informar, contenidos en el Artículo 12 de la Ley Orgánica de Protección de Datos Personales. (Comisión de la Unión Europea, 2022).

9.1.2 La base legal para el tratamiento.-

En lo que concierne a la legalidad para el tratamiento, dentro del consentimiento informado, se detalla la base normativa, por la que el Banco solicita la información al cliente y por ende a la que se realizará el tratamiento de datos personales, en estricto apego al principio de juridicidad. Mediante este apartado, se pretende dejar claro que los Datos Personales de usuarios y clientes de esta entidad financiera, son tratados en estricto apego y cumplimiento de los derechos

fundamentales, principios y obligaciones consagradas en la Constitución de la República, así como la presente Ley, por lo que se generó el texto según el siguiente detalle:

> *"De conformidad con lo dispuesto en el artículo 12 de la Ley Orgánica de Protección de Datos Personales, el* ***XXXXXXXXXXXXXX.,*** *identificado con RUC No. XXXXXXXXXX, con domicilio en la ciudad de XXXXXXXXXXXXXXXX****,*** *cumple con el deber de informar relacionado al tratamiento de los datos personales de sus* ***clientes****. En ese sentido, en base a la Ley Orgánica de Protección de Datos Personales, promulgada en el Registro Oficial Suplemento No. 459 de 26 de mayo de 2021, (en adelante, la "LOPDP")* ***EL CLIENTE*** *declara haber sido apropiadamente informado respecto del tratamiento de los datos personales, en los términos siguientes:"*

9.1.3 Los Fines de tratamiento.-

En lo que concierne a la finalidad del tratamiento de Datos Personales y de conformidad a lo estipulado en los principios previstos en el Artículo 10 de Ley Orgánica de Protección de Datos Personales, se ha establecido que las finalidades del tratamiento sean "determinadas, explícitas, legítimas y comunicadas claramente al titular." (Ley Orgánica de Protección de Datos Personales, 2021) Además dentro de los procesos y procedimientos de los responsables del tratamiento, de las diferentes áreas de esta entidad financiera., se definió que los datos personales no podrán tener finalidades distintas para las que fueron recopiladas, salvo en casos que la misma Ley los excluye.

"Finalidad: *Los datos personales serán utilizados para cumplir con las siguientes finalidades:*

(i) Cumplir con la norma Conozca a su Cliente.

(ii) Prestación de servicios o productos financieros, como apertura de cuentas bancarias de ahorros, cuenta corriente, cuenta de ahorro programado, cuenta de ahorro rentable, entre otras, emisión de tarjetas de crédito y débito, entre otros, certificados de depósito,

créditos vehiculares, hipotecarios y de consumo, entre otros productos, así como lo referente al contrato de vinculación.

(iii) Transferencia de los datos del cliente a las empresas procesadoras y emisoras de tarjetas de crédito.

(iv) Velar porque el proceso y calidad de los datos sean correctos y actualizados.

(v) Mejorar el uso de los datos, definir los procesos que serán ejecutados por el área comercial.

(vi) Verificación de la información proporcionada por el cliente mediante fuentes públicas y privadas para cumplimiento de normas de prevención de lavado de activos y financiamiento de terrorismo, previo al otorgamiento de servicios o productos bancarios.

(vii) Recopilación de datos del equipo móvil, para procesos de autenticación de banca móvil.

(viii) Envío de SMS para autenticación de uso de contraseñas o movimientos en cuentas o productos relacionados con el Banco.

(ix) Prestación de servicios de banca online y móvil como servicios auto gestionables por parte del cliente para bloqueos de cuenta.

(x) Verificación de transacciones mediante uso de cajeros automáticos (retiro o depósito, pago servicios).

(xi) Coordinación de entrega o envío de información o comunicaciones relacionadas a los productos contratados con el Banco, envío de plásticos de tarjetas de crédito o débito, comunicaciones de seguimiento respecto de los productos o servicios solicitados por el Cliente."

Asimismo en un apartado diferente, mismo que requiere una aceptación expresa del cliente, se detalla la finalidad del tratamiento de datos personales, con fines de marketing, y para que los clientes y usuarios del sistema financiero puedan recibir información publicitaria respecto a productos o servicios. Cabe señalar que la negativa al consentimiento del tratamiento de datos personales con fines de marketing, no limita el acceso a los diferentes productos o servicios puestos a disposición del Banco.

Datos Personales con fines de Marketing. *Los datos requeridos de los usuarios en la interacción con las distintas plataformas (digital, redes sociales y telefónica) del* ***XXXXXXXXXXX*** *son los siguientes:*

(i) ***Datos de carácter identificativo:*** *Nombres y apellidos, número de cédula (sólo en página), correo electrónico, dirección, teléfono.*

(ii) ***Datos de características personales:*** *edad, estado civil, sexo, relación laboral*

(iii) ***Datos de carácter social:*** *hábitos de navegación y tipo de transacciones.*

(iv) ***Datos de carácter económico y financiero:*** *ingreso mensual (dependiente/independiente), actividades económicas.*

Cabe señalar que estos datos son solicitados en función normativa financiera, mediante la cual establece los datos mínimos que se deben ser solicitados para la oferta de productos y servicios del sistema financiero.

Finalidad y Usos. *El Usuario tiene conocimiento que los datos proporcionados al* ***XXXXXXXXX*** *se otorgan con el fin de cumplir con las siguientes finalidades:*

(i) Desarrollo de productos, servicio al cliente e inteligencia de negocios.

(ii) Desarrollo de marca (comunicación externa, comunicación digital, relaciones públicas, y sostenibilidad).

(iii) Manejo de comunicación externa, digital, relaciones públicas y sostenibilidad. Se incluye página web y mail marketing, redes sociales.

(iv) Desarrollo de productos, relacionados a activo, pasivo, banca seguros y transporte de valores, factoring y confirming.

(v) Oferta de valor para nuevos segmentos.

(vi) Servicio al cliente. Revisión de la llamada de servicio al cliente.

(vii) Inteligencia de negocios. Generar conocimiento a través de la información de los clientes, generación de campañas comerciales, paneles de visualización.

(viii) Aplicación de modelos de ciencia de datos (machine learning) para modelos de segmentación de clientes, modelos de retención, modelos para realización de ventas cruzada, uso de y evaluación de métricas de precisión, modelo para evaluar el perfil digital del cliente.

(ix) Campañas en la web pública y los mensajes de inbox de redes sociales, en relación a potenciales clientes para captación de nuevos productos.

(x) Impulso de ventas a través de canales de contact center, mediante canales de comunicación de nuevos productos o servicios.

(xi) Fortalecer el uso de aplicaciones móviles del banco.

En cumplimiento de la LOPDP, el Usuario acepta el tratamiento de sus datos personales, y al hacer "clic" en la sección "Otorgo mi consentimiento", otorga su consentimiento libre, previo, expreso, informado e inequívoco para que sus datos personales, sean incorporados en sus bases de datos personales y sean tratados con todas las medidas de seguridad y confidencialidad establecidas en el marco legal aplicable

○ Sí otorgo mi consentimiento. ○ No otorgo mi consentimiento	*Tratamiento de mis datos personales para finalidades asociadas a marketing, publicidad o perfilamiento.*

El consentimiento informado con finalidades de mercadotecnia, se encuentra individualizado y requiere una aceptación expresa e independiente del titular de datos personales, tal como lo prevé el artículo 16 de la Ley Orgánica de Protección de Datos. Cabe señalar que este consentimiento no limita al usuario del sistema financiero la contratación de diferentes productos y servicios financieros, sino que es una manifestación expresa en la que consiente o no que el Banco le pueda remitir información con finalidad de marketing, previa aceptación de su titular. Adicionalmente, dentro del proceso que ha sido considerado por el Banco se ha establecido que *"el tratamiento de datos personales tenga por objeto la mercadotecnia directa; el interesado tendrá derecho a oponerse en todo momento al tratamiento de los datos personales que le conciernan, incluida la elaboración de perfiles; en cuyo caso los datos personales dejarán de ser tratados para dichos fines"*. (LEY ORGÁNICA DE PROTECCIÓN DE DATOS PERSONALES,

2021) Por lo que, en el caso que un cliente haya otorgado su consentimiento para recibir información con fines de mercadotecnia, podrá oponerse en cualquier momento.

En el consentimiento informado a utilizarse por parte del Banco, se detalla claramente los datos que son solicitados y necesarios para la prestación de los servicios y productos financieros a ser contratados por los clientes. Cabe señalar que estos datos son pertinentes y se encuentran limitados a lo estrictamente necesario para el cumplimiento de la finalidad del tratamiento y además es adecuado, necesario, oportuno, relevante y no excesivo, en relación a las finalidades para los que han sido recogidos, de conformidad con lo establecido en los principios de pertinencia y minimización, proporcionalidad, calidad y exactitud, mismos que se encuentran consagrados en el artículo 10 de la Ley Orgánica de Protección de Datos Personales. (Ley Orgánica de Protección de Datos Personales, 2021)

> ***“Base de Datos. XXXXXXXXXXX.*** *es titular de la base de datos denominada “CLIENTES” y “MARKETING Y DESARROLLO DE NEGOCIOS”, las cuales serán oportunamente registradas ante la Autoridad de Protección de Datos Personales. Las bases de datos son manejadas directamente desde el domicilio de XXXXXXXXXX ubicado en la ciudad XXXXXXXXXXXXXX.*
>
> ***Datos Personales Obligatorios para cumplimiento de relación contractual que el cliente mantenga con XXXXXXXXXXXXXXX.***

EL CLIENTE *tiene conocimiento que los datos proporcionados al* ***BANCO,*** *que se otorgan son obligatorios con motivo de la preparación, suscripción y/o ejecución de una relación contractual mediante la cual* ***EL CLIENTE*** *adquiere productos o servicios bancarios. Los datos personales requeridos son: Identificación; Nombre y Apellido; Barrio/Distrito de nacimiento; Dirección de domicilio; Celular, correo personal; Teléfono de trabajo; Fecha de nacimiento; Nacionalidad; Género; Estado Civil; Cónyuge; sociedad conyugal; Nivel de educación; teléfono móvil para interacción con banca móvil; Datos crediticios; Persona Expuesta Políticamente, Relación Laboral; Dirección de trabajo; Información tributaria (impuestos en el exterior); Actividad Económica, Fuente de ingresos; Activos, Pasivos, Patrimonio; Dirección de tributación en exterior, ingresos y egresos mensuales; además de cualquier otra información necesaria para la relación contractual, por lo tanto el* ***BANCO*** *tiene una necesidad legítima de acceder y procesar los datos para los fines anteriormente indicados".***

9.1.4 Tiempo de Conservación.-

La Ley Orgánica de Protección de Datos Personales, establece que "los datos personales serán conservados durante un tiempo no mayor al necesario para cumplir con la finalidad de su tratamiento." (Ley Orgánica de Protección de Datos Personales, 2021). Este particular ha generado varias discusiones a nivel interno de la organización, toda vez que, al ser la compañía objeto del presente trabajo de investigación, una entidad financiera, se rige ante lo dispuesto en el Código Orgánico Monetario y Financiero, en el que, en su artículo 225 señala que "*las entidades del sistema financiero nacional mantendrán sus archivos contables físicos, incluyendo los respaldos respectivos, por el plazo de diez años contados a partir de la conclusión de la operación correspondiente y por quince años en el formato digital autorizado por las superintendencias*".

(CÓDIGO ORGÁNICO MONETARIO Y FINANCIERO, 2014) Por lo que, para cumplir con la base normativa en cuestión, en el consentimiento informado, se detalla que el plazo de conservación de los datos de los clientes está sujeto a las condiciones de la vigencia del Contrato, así como a los plazos previstos en el Código Orgánico Monetario y Financiero:

> ***"Plazo.*** *El plazo de conservación de los datos se sujeta al plazo de vigencia del Contrato, y serán conservados por los plazos establecidos en el Código Orgánico Monetario y Financiero y demás normas conexas o hasta que usted ejercite el derecho de revocación o cancelación conforme a la LOPD, sin embargo, el* ***BANCO*** *se reservará el derecho de retener los datos en caso que la cancelación no sea posible por mandato legal o motivo debidamente fundamentado."*

9.1.5 Transferencia de Datos Personales.-

En base a lo establecido en el numeral 10 del artículo 12 de la Ley Orgánica de Protección de Datos Personales, en el consentimiento informado, se le comunica al cliente que para el cumplimiento de las finalidades descritas en el mismo documento, se requiere transferir sus Datos Personales, para lo cual se detalla a los proveedores y entidades a las que se les transferirá la Información, según el siguiente detalle:

> ***Transferencia de Datos Personales.*** *Para cumplir con los fines indicados en el punto 3, los datos personales de* ***EL CLIENTE*** *podrán ser transferidos de forma local o internacional, de acuerdo con el siguiente detalle:*

Transferencia de Datos Personales a Nivel Nacional. *Para cumplir con la finalidad de indicada,* ***XXXXXXXXXXX*** *debe transferir los datos personales a nivel nacional a las siguientes entidades:*

1.1.1. *Superintendencia de Bancos, Banco Central del Ecuador, Servicio de Rentas Internas.*

1.1.2. *Compañías de Gestión de Call Center.*

1.1.3. *Empresas de gestión de canales electrónicos y ventas de Asistencias.*

1.1.4. *Empresas de verificación de datos.*

1.1.5. *Empresas de gestión documental*

1.1.6. *Transferencia a empresas procesadoras de las tarjetas.*

1.1.7. *Agencias de medios digitales y Agencia de medios tradicionales.*

Cabe señalar que el detalle de estas empresas se encuentra previsto en el aviso de privacidad de XXXXXXXXXX y que podrá ser actualizado en cumplimiento de la obligación contractual.

Transferencia de Datos Personales a Nivel Internacional. EL BANCO cumple con informar a **EL CLIENTE** las siguientes transferencias:

1.2. Estados Unidos: MICROSOFT TEAMS (pendiente nombre completo): [PENDIENTE TAX ID], proveedor de herramientas colaborativas en red.

1.3. Estados Unidos. Microsoft Corp, proveedor de hosting de página web del dominio xxxxxxxxxxxxxxxxxxxx.

Ejercicio de Derechos. Para realizar una solicitud de acceso, rectificación, eliminación, oposición de su información personal o cualquiera de los derechos indicados en los artículos 13 a 19 de la LOPDP, o para obtener información adicional sobre esta declaración de protección de datos personales y para garantizar sus derechos dirigirse a la página web: xxxxxxxxxxxxxxxxxxxxxxxxxxx en la sección, "AVISO DE PRIVACIDAD ", acceso a los derechos y principios de la Ley de Protección de Datos Personales.

Cabe señalar que para garantizar el pleno cumplimiento de los derechos de los clientes y el correcto tratamiento de sus datos personales, se ha realizado un Anexo de protección de Datos Personales a suscribirse con los diferentes proveedores, de conformidad con lo establecido en el Anexo 3. Cabe señalar que en los casos de transferencia de datos a nivel internacional, con compañías tales como Microsoft, entre otras, el Banco se adhiere a las políticas de privacidad.

De esta forma, con las recomendaciones realizadas en el clausulado insertado en el Consentimiento Informado para la protección de Datos Personales, el Banco se encuentra apegado en estricto sentido a lo establecido en el Artículo 12 de La Ley Orgánica de Protección de Datos Personales, en relación al deber de información, por lo tanto, el presente tratamiento de datos personales es legítimo y lícito conforme al numeral 5 del artículo 7 de la misma Ley. Adicional al consentimiento informado, el Banco, se encuentra en constante actualización y mejora de herramientas tecnológicas para garantizar que el tratamiento de los datos personales de clientes cumplirá con las medidas de seguridad necesaria, a fin de evitar cualquier alteración, pérdida, tratamiento no autorizado y/o cualquier riesgo, amenaza o vulnerabilidad.

10. REFERENCIAS

ASAMBLEA NACIONAL DEL ECUADOR. (12 de Septiembre de 2014). CÓDIGO ORGÁNICO MONETARIO Y FINANCIERO. Quito, Ecuador.

Asamblea Nacional del Ecuador. (26 de 05 de 2021). Ley Orgánica de Protección de Datos Personales. Quito, Ecuador. Obtenido de https://total.finder.lexis.com.ec/WebTools/LexisFinder/DocumentVisualizer/DocumentVisualizer.aspx?id=PUBLICO-LEY_ORGANICA_DE_PROTECCION_DE_DATOS_PERSONALES&query=ley%20organica%20de%20protecci%C3%B3n%20de%20datos#I_DXDataRow0

Asociación de Bancos del Ecuador. (01 de Abril de 2022). *Asociación de Bancos del Ecuador*. Obtenido de https://asobanca.org.ec/boletin-macroeconomico/

Asociación de Bancos del Ecuador. (05 de 04 de 2022). *Asociación de Bancos del Ecuador*. Obtenido de https://asobanca.org.ec/evolucion-de-la-banca/

Banco Central del Ecuador. (s.f.). *Banco Central del Ecuador*. Obtenido de https://contenido.bce.fin.ec/home1/economia/tasas/indiceINCFIN.htm

BANCO DE DESARROLLO DE AMÉRICA LATINA. (13 de MAYO de 2021). *BANCO DE DESARROLLO DE AMÉRICA LATINA* . Obtenido de https://www.caf.com/es/actualidad/noticias/2021/05/desigualdad-40-a-cerrar-la-brecha-digital/

Banco Interamericano de Desarrollo (BID). (Junio de 2015). *Banco Interamericano de Desarrollo (BID).* Obtenido de

https://publications.iadb.org/publications/spanish/document/Inclusi%C3%B3n-financiera-en-Am%C3%A9rica-Latina-y-el-Caribe-Coyuntura-actual-y-desaf%C3%ADos-para-los-pr%C3%B3ximos-a%C3%B1os.pdf

XXXXXXXXXXXXXX S.A. (05 de Mayo de 2022). *XXXXXXXXXXXXX*. Recuperado el 05 de Mayo de 2022, de https://www.bancointernacional.com.ec/logros-y-reconocimientos/

Banco Mundial. (07 de abril de 2022). Obtenido de https://www.bancomundial.org/es/country/ecuador/overview#1

Comisión de la Unión Europea. (15 de noviembre de 2022). *Cómo debe solicitarse mi consentimiento*. Obtenido de https://ec.europa.eu/info/law/law-topic/data-protection/reform/rights-citizens/how-my-personal-data-protected/how-should-my-consent-be-requested_es

Iturralde, S. (08 de mayo de 2022). Entorno ambiental de XXXXXXXXXXXXXX S.A. (F. Cobo, Entrevistador)

LEY ORGÁNICA DE PROTECCIÓN DE DATOS PERSONALES. (2020). QUITO.

Moreano, G. (08 de marzo de 2022). Cambio y actualización Core Bancario GIBS XXXXXXXXXXXXXX S.A,. (J. C. Crespo, Entrevistador)

Naciones Unidas. (25 de abril de 2022). *Naciones Unidas*. Obtenido de https://www.un.org/es/un75/impact-digital-technologies#:~:text=Los%20avances%20digitales%20pueden%20apoyar,logro%20de%20la%20alfabetizaci%C3%B3n%20universal.

Pico, L. (20 de abril de 2022). Clientes de XXXXXXXXXXXXXX S.A. (F. Cobo, Entrevistador)

Superintendencia de Bancos. (05 de Agosto de 2022). Obtenido de https://www.superbancos.gob.ec/bancos/wp-content/uploads/downloads/2022/02/L1_IX_cap_V.pdf

11. ANEXOS

Como Anexos se han considerado; Anexo 1. Metodología de implementación de la LODPD, Anexo 2. Condiciones de tratamiento de datos personales de xxxxxxxxxxxxx, Anexo 3. Disclaimer usuarios del sistema financiero (no clientes), Anexo 4. Anexo de protección de datos personales Responsable – Encargado, documentos que han sido aprobados e incluidos en manuales y procedimientos de la entidad financiera objeto de este trabajo de investigación.

Anexo 1. Metodología para la Evaluación de Riesgos Elaborado por la Consultora extranjera

INTRODUCCIÓN

Actualmente la normativa sobre protección de datos personales ha cobrado especial relevancia, no solo a nivel internacional, sino a nivel nacional con la emisión de la Ley Orgánica de Protección de Datos Personales (LOPD).

La LOPD busca "*garantizar el ejercicio del derecho a la protección de datos personales, que incluye el acceso y decisión sobre información y datos de este carácter, así como su correspondiente protección. Para dicho efecto regula, prevé y desarrolla principios, derechos, obligaciones y mecanismos de tutela*"[1].

Las garantías para el ejercicio del derecho a la protección de datos personales se traducen en el establecimiento de mecanismos y procedimientos para permitir que el individuo (titular de los datos personales), ejerza un control y conocimiento sobre los propósitos, necesidades y forma de recopilación y procesamiento de su información personal.

El otorgamiento del ejercicio del derecho a la protección de datos personales implica que las organizaciones establezcan controles internos que les permitan determinar, en principio, las categorías y finalidades del tratamiento de los datos personales; así como el tipo de datos personales que son necesarios para el cumplimiento de las finalidades y objetivos, los cuáles pueden estar determinados en una ley especial o en los objetivos organizacionales de la compañía.

Al respecto, la normativa parte de la necesidad de realizar una recopilación y procesamiento de datos sustentado en el consentimiento del individuo (titular del dato personal), salvo que dicha recopilación y procesamiento se encuentre amparado en un marco legal específico.

Asimismo, el uso de nuevas tecnologías o tecnologías emergentes implican riesgos relacionados a la seguridad y confidencialidad de la información que deben ser conocidos y socializados al interior de la compañía, con la finalidad de minimizarlos o reducirlos.

A través de la presente metodología se establecen los principales conceptos a tener en consideración al momento de determinar la existencia de riesgos en el tratamiento de datos personales, la cual deberá ser complementada y actualizada con los criterios o jurisprudencia que emita la Autoridad de Protección de Datos Personales correspondiente.

ALCANCE

Las disposiciones del presente documento son aplicables a la gestión de riesgos en el tratamiento de datos personales que están contenidos en bases de datos personales de titularidad del XXXXXXXXXXXXX.

[1] Artículo 1 de la Ley Orgánica de Protección de Datos Personales.

OBJETIVO

Establecer la metodología para la identificación, evaluación, tratamiento y riesgos de la recopilación y procesamiento de información personal a la que tenga acceso el XXXXXXXXXXXXX como consecuencia del desarrollo de su objeto social, así como de la persecución de sus finalidades comerciales.

RESPONSABLES.

Las áreas responsables de la aplicación de la presente metodología son:

Áreas Usuarias. Se refiere a todas las áreas establecidas en la estructura organizacional del XXXXXXXXXXXXX, que tienen a su cargo la recopilación y procesamiento de datos personales. Las áreas usuarias deberán solicitar la conformidad del Oficial de Protección de Datos Personales en los casos en que se genere una nueva finalidad de tratamiento de datos personales, o en caso requieran modificar o ampliar las finalidades de tratamiento vigentes a la fecha de la emisión del presente procedimiento.

Delegado de Protección de Datos Personales. Es el funcionario encargado de verificar que la recopilación y procesamiento de datos (entendido como fases del tratamiento de datos personales), se realicen en cumplimiento de los principios de consentimiento, juridicidad, lealtad, transparencia, finalidad, pertinencia y minimización, proporcionalidad, confidencialidad, seguridad, responsabilidad proactiva y demostrada. Asimismo, el Delegado de Protección de Datos es el responsable de informar el grado de las sanciones por infracción normativa establecidos en la LOPD.

Responsable de Seguridad Lógica. Es el funcionario responsable de brindar soporte al Delegado de Protección de Datos Personales en asuntos relacionados al cumplimiento de las medidas de seguridad lógica y física, con la finalidad de resguardar la confidencialidad e integridad de los activos de información que contengan datos personales.

Responsable de Riesgo Operativo. Es el funcionario responsable de coordinar con el Delegado de Protección de Datos la cuantificación final de la exposición al riesgo en determinado tratamiento de datos personales, considerando la metodología de riesgo operativo aplicable a la organización.

GLOSARIO DE TÉRMINOS[2].

[2] Conforme al artículo 4 de la Ley Orgánica de Protección de Datos Personales.

Base de datos o fichero: Conjunto estructurado de datos cualquiera que fuera la forma, modalidad de creación, almacenamiento, organización, tipo de soporte, tratamiento, procesamiento, localización o acceso, centralizado, descentralizado o repartido de forma funcional o geográfica.

Consentimiento: Manifestación de la voluntad libre, específica, informada e inequívoca, por el que el titular de los datos personales autoriza al responsable del tratamiento de los datos personales a tratar los mismos.

Dato personal: Dato que identifica o hace identificable a una persona natural, directa o indirectamente[3].

Encargado del tratamiento de datos personales: Persona natural o jurídica, que solo o juntamente con otros trate datos personales a nombre y por cuenta del XXXXXXXXXXXXXX, en virtud de una relación jurídica que los vincule. Se entiende como encargado de tratamiento a todos los proveedores contratados por el XXXXXXXXXXXXXX que tengan acceso a datos personales contenidos en ficheros de titularidad del XXXXXXXXXXXXXX.

Privacidad desde el diseño y por defecto. Se entiende a la protección de datos desde el diseño como el deber del responsable del tratamiento de tener en cuenta, en las primeras fases de concepción y diseño del proyecto, que determinados tipos de tratamientos de datos personales entrañan una serie de riesgos para los derechos de los titulares en atención al estado de la técnica, naturaleza y fines del tratamiento, para lo cual, implementará las medidas técnicas, organizativas y de cualquier otra índole, con miras a garantizar el cumplimiento de las obligaciones en materia de protección de datos, en los términos del reglamento. La protección de datos por defecto hace referencia a que el responsable debe aplicar las medidas técnicas y organizativas adecuadas con miras a que, por defecto, solo sean objeto de tratamiento los datos personales que sean necesarios para cada uno de los fines del tratamiento, en los términos del reglamento.

Responsable de tratamiento de datos personales: La entidad que decide sobre la finalidad y el tratamiento de datos personales; en este caso toda referencia a “responsable de tratamiento” se entenderá a XXXXXXXXXXXXXX.

Riesgo en el tratamiento de datos personales. El riesgo legal está asociado a la posibilidad de la imposición de una multa por la imputación de una infracción normativa en protección de datos personales, conforme al rango de multas contenido en la LOPD o en sus normas complementarias.

[3] Del concepto general de dato personal se desprenden conceptos específicos que incluyen: datos biométricos, datos genéticos, datos personales crediticios, datos relativos a la salud, datos sensibles. Es necesario remitirse al concepto establecido en la LOPD.

Titular del dato personal: Persona natural cuyos datos son objeto de tratamiento.

Tratamiento de datos personales: Cualquier operación o conjunto de operaciones realizadas sobre datos personales, ya sea por procedimientos técnicos de carácter automatizado, parcialmente automatizado o no automatizado, tales como: la recogida, recopilación, obtención, registro, organización, estructuración, conservación, custodia, adaptación, modificación, eliminación, indexación, extracción, consulta, elaboración, utilización, posesión, aprovechamiento, distribución, cesión, comunicación o transferencia, o cualquier otra forma de habilitación de acceso, cotejo, interconexión, limitación, supresión, destrucción y, en general, cualquier uso de datos personales.

Vulneración de la seguridad de los datos personales: Incidente de seguridad que afecta la confidencialidad, disponibilidad o integridad de los datos personales.

ACTIVIDADES DE TRATAMIENTO DE DATOS PERSONALES.

Las actividades de tratamiento deben reflejar los siguientes aspectos:

Área usuaria que es la responsable directa en el tratamiento de los datos personales, la cual asignará un coordinador que tendrá interacción directa con el Delegado de Protección de Datos Personales.

Denominación de la base de datos o fichero.

Identificación del responsable del tratamiento (XXXXXXXXXXXXXX).

Identificación de los encargados de tratamiento (personas naturales o jurídicas que, por encargo del XXXXXXXXXXXXXX), realizan actividades de tratamiento de datos.

Dirección y correo electrónico de contacto para que el Titular del Dato Personal ejerza sus derechos de acceso, rectificación y actualización, eliminación, oposición y portabilidad en el tratamiento de los datos personales.

Finalidad de tratamiento determinada, específica, lícita y comunicada al Titular del Datos Personal.

Usos previstos.

Datos personales sujetos a tratamiento.

Plazo de conservación de los datos.

Ubicación de la base de datos (en medios físicos o digitales).

Procedimiento de obtención de los datos: fuente, soporte y procedimiento de obtención.

Transferencias nacionales e internacionales.

Especificación de consentimiento o de base legítima de tratamiento de los datos.

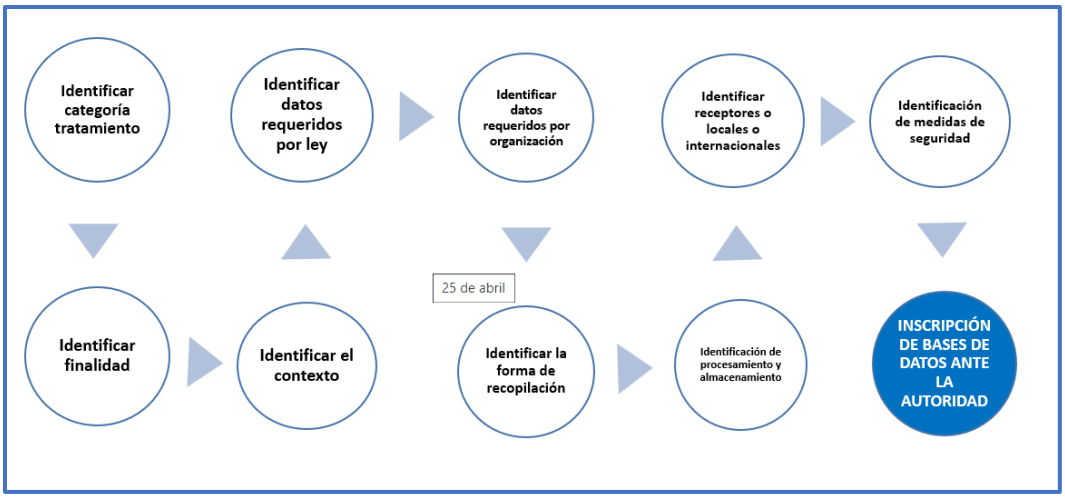
Medidas de seguridad aplicadas.

El Delegado de Protección de Datos Personales tendrá a su cargo el manejo de una "Matriz de Actividades de Tratamiento de Datos Personales" que resuma la información listada en los puntos anteriores y que sirva de soporte para:

Revisión continua de las actividades realizadas por las Áreas Usuarias, que permita actualizar la información en caso de cambios en dichas actividades de tratamiento; y,

Mantener debidamente actualizado los registros de Bases de Datos ante la Autoridad de Protección de Datos Personales.

La "Matriz de Protección de Datos Personales" mapea y resume el siguiente flujo de información:



Cualquier actualización en la "Matriz de Protección de Datos Personales" deberá ser reflejada en los registros de Bases de Datos hechos ante la Autoridad Nacional de Protección de Datos Personales.

Un ejemplo de la "Matriz de Protección de Datos Personales" forma parte de la presente Metodología como "Anexo A".

FINALIDADES DE TRATAMIENTO DE DATOS PERSONALES APROBADAS.

En el curso de las actividades de su objeto social, el XXXXXXXXXXXXXX realiza diversas operaciones de Tratamiento de Datos Personales. En ese sentido, los Datos Personales sujetos a tratamiento deberán someterse únicamente a las finalidades aprobadas; para ello, el XXXXXXXXXXXXXX deberá determinar las finalidades determinadas, específicas y lícitas.

Así, se entiende como finalidades principales a aquellas directamente relacionadas con el negocio, contrato o relación jurídica, mediante la cual se hace necesario contar con los Datos Personales. La falta de dichos Datos Personales ocasionará la imposibilidad de llevar adelante el negocio, contrato o relación jurídica, o de cumplir las obligaciones especificadas en normas, leyes o reglamentos de obligatorio cumplimiento.

Se entiende por finalidades adicionales, a aquellas que no están directamente relacionadas con la celebración de un negocio, contrato o relación jurídica, o que no se encuentra contemplada como una obligación legal en alguna norma legal; o que no se encuentra incluida dentro de las excepciones al consentimiento contenidas en la LOPD.

El Delegado de Protección de Datos Personales tendrá a su cargo el "Procedimiento que regula las Finalidades de Tratamiento de Datos Personales del XXXXXXXXXXXXXX". Este procedimiento forma parte de la presente Metodología como Anexo B.

METODOLOGÍA PARA LA EVALUACIÓN DE RIESGOS EN EL TRATAMIENTO DE DATOS PERSONALES.

Marco metodológico.

El propósito de la gestión de riesgos en el tratamiento de datos personales es identificar y gestionar los riesgos potenciales asociados a una actividad de tratamiento de datos personales.

La presente metodología resume las medidas técnicas, organizacionales y/o legales que sean necesarias para proteger los datos personales de cualquier riesgo, amenaza o vulnerabilidad.

Ciclo de vida del dato.

El ciclo de vida del dato se puede dividir en las siguientes etapas:

Captura de datos: proceso de obtención y almacenamiento de datos para su procesamiento. Las técnicas de captura son diversas (formulario web o papel, encuestas, contratos, etc.).

Clasificación/almacenamiento: establecer categorías para su clasificación y almacenamiento.

Uso y tratamiento: operación o conjunto de operaciones realizadas sobre los datos personales (automatizado o no automatizado).

Cesión de datos a un tercero para su tratamiento: traspaso o comunicación de datos realizada a un tercero, la cesión es muy amplia, dado que alberga la entrega, comunicación, consulta, interconexión, transferencia, difusión o cualquier forma que facilité el acceso.

Destrucción: eliminar los datos que puedan estar contenidos en los sistemas o archivos, de manera que no puedan ser recuperados

Para cada etapa del ciclo de vida se debe identificar todos los elementos involucrados en cada una de las etapas:

Actividades de tratamiento sobre los datos de carácter personal

Es importante describir en detalle todas las actividades u operaciones que se llevan a cabo sobre los datos personales con el objetivo de entender los posibles riesgos. Una actividad y operación puede ser, por ejemplo, la captura de datos mediante formularios web, filtrado de información mediante un

proceso de perfilado, un proceso de cifrado, entre otras actividades que involucren tratamiento o manipulación de datos.

El Delegado de Protección de Datos deberá utilizar la “Matriz de Actividades de Tratamiento de Datos Personales” como punto de partida para la verificación de esta fase.

Datos

Se tiene que identificar los datos personales sujetos a tratamiento siempre que su tratamiento responda a los principios establecidos en la LOPD. Asimismo, establecer su tipología (categoría y grado de importancia) para determinar si es imprescindible o no su inclusión. Cabe señalar que se debe considerar principio de minimización de los datos y asegurar que no existan datos sin utilidad o desproporcionados para la finalidad.

Intervinientes:

Se tiene que identificar las personas naturales y jurídicas que, de manera individual o colectiva, están implicados en el desarrollo del tratamiento; éstas pueden ser: Áreas Usuarias, Proveedores o Terceros. Asimismo, delimitar sus funciones y responsabilidades. Se puede debe incluir al Delegado de Protección de Datos, Coordinadores de las Áreas Usuarias y/o empleados de las organizaciones que intervienen en la actividad de tratamiento.

Tecnología. Se tiene que identificar qué elementos tecnológicos intervienen en las actividades de tratamiento, identificando el hardware y software que sea relevante para el tratamiento, dado que las tecnologías están expuestas a diferentes riesgos. Para esta fase, el Delegado de Protección de Datos debe coordinar directamente con el Responsable de Seguridad Lógica para verificar que se cumplen los más altos estándares en controles de seguridad. El Responsable de Seguridad Lógica sustentará su soporte en la “Metodología de riesgo tecnológico y de seguridad de la información”.

<u>Identificación de riesgos.</u>

Los principales riesgos de probabilidad y gravedad se pueden diferenciar en 2 dimensiones:

Riesgos asociados al cumplimiento de los requisitos regulatorios relacionados con los derechos y libertades de los interesados. Por ejemplo: contar con avisos de privacidad o solicitudes de consentimiento informado conforme a lo establecido en la LOPD, contar con finalidades determinadas, específicas y legales de tratamiento de datos personales, contar con cláusulas de confidencialidad que impongan responsabilidades por el mal uso de los datos personales a los que se tiene acceso, entre otras.

Riesgos asociados a la protección de la información (relacionado con la integridad, disponibilidad y confidencialidad de los datos). Por ejemplo: contar con políticas de seguridad de la información, procedimientos de control de accesos y gestión de privilegios periódicos, entre otros.

Para la identificación de los riesgos asociados a la protección de la información, se deberá tomar como insumo los elementos tecnológicos, hardware y software, que intervienen en las actividades de tratamiento identificados en el ciclo de vida del dato como se mencionó en el numeral 8.2 del presente documento. Los riesgos asociados a la protección de la información sobre estos activos, están relacionados con la afectación de la confidencialidad, integridad y disponibilidad como se muestra a continuación:

Acceso no autorizado a los datos personales (pérdida de confidencialidad).

Modificación no autorizada a los datos personales (pérdida de integridad).

Pérdida, robo o eliminación no autorizada de los datos personales (pérdida de disponibilidad).

Para identificar cuáles de estos riesgos pueden materializarse sobre los elementos tecnológicos identificados, se seguirán los lineamientos definidos en los numerales que se encuentran en la "Metodología de riesgo tecnológico y de seguridad de la información".

Para valorar estos riesgos es importante tener presente que la evaluación del impacto de los riesgos en la protección de datos personales se realiza desde la afectación que represente la materialización de los mismos en el titular de los datos, a diferencia del análisis de los riesgos en la seguridad de la información, el cual se realiza desde el punto de vista del riesgo para la organización.

El Delegado de Protección de Datos dispone de una "Lista de Cumplimiento Normativo", la cual forma parte de la presente Metodología como Anexo C, para poder identificar los riesgos asociados a las actividades de tratamiento.

<u>Identificación de potenciales riesgos asociados a una actividad de tratamiento.</u>

Primero, se debe establecer una descripción detallada del Tratamiento de Datos Personales (contexto y elementos relevantes). Luego, analizar y determinar cuáles son los riesgos que pueden afectar los derechos y libertades de los Titulares de los Datos Personales. Por último, establecer las medidas de seguridad necesarias para garantizar una seguridad y control adecuado.

Asimismo, es necesario una monitorización continua, dado que los riesgos pueden variar con el tiempo, asimismo las actividades de tratamiento también, por lo que es necesaria una revisión y evaluación periódica de efectividad de las medidas de control.

Para estos controles, el Delegado de Protección de Datos llevará un monitoreo programado de la "Matriz de Actividades de Tratamiento de Datos", del "Procedimiento que regula las Finalidades de

Tratamiento de Datos del XXXXXXXXXXXXXX", con el soporte del Responsable de Seguridad Lógica mediante la aplicación de la "Metodología de riesgo tecnológico y de seguridad de la información".

Análisis de los potenciales factores de riesgo del tratamiento de datos personales.

La evaluación de los riesgos consiste en valorar y estimar la probabilidad y el nivel de impacto de que el riesgo asociado a la protección de la información se materialice y genere daños en el Titular de los Datos

Valoración del impacto y la probabilidad.

A continuación, se presenta las escalas para la valoración de la probabilidad e impacto basada en cuatro niveles de acuerdo a los Lineamientos para evaluación de riesgos de la Agencia Española de Protección de Datos.[4]

La probabilidad se determina en base a las posibilidades que existen de que la amenaza se materialice. La escala de valores para el cálculo de la probabilidad es la siguiente:

Improbable: La posibilidad de que un riesgo cause daño o afecte a los derechos y libertades de los titulares de los datos personales es muy bajo.

Baja: La posibilidad de que un riesgo cause daño o afecte a los derechos y libertades de los titulares de los datos personales es bajo.

Alta: La posibilidad de que un riesgo cause daño o afecte a los derechos y libertades de los titulares de los datos personales es alta.

Muy Alta: La posibilidad de que un riesgo cause daño o afecte a los derechos y libertades de los titulares de los datos personales es muy alta.

El impacto se determina con base a los posibles daños que se pueden producir en el titular de los datos si la amenaza se materializa. La escala de valores para el cálculo del impacto es la siguiente:

Muy Limitado: El impacto es muy bajo (por ejemplo, un evento cuyas consecuencias son prácticamente despreciables sin impacto sobre el interesado).

Limitado: El impacto es bajo (por ejemplo, un evento cuyas consecuencias implican un daño menor sin impacto relevante sobre el interesado).

Significativo: El impacto es alto (por ejemplo, un evento cuyas consecuencias implican un daño elevado con impacto sobre el interesado).

[4] Consultar la Guía del riesgo y evaluación de impacto en tratamiento de datos personales.

Máximo: El impacto es muy alto (por ejemplo, un evento cuyas consecuencias implican un daño muy elevado un impacto crítico sobre el interesado).

Si combinamos la probabilidad y el impacto obtenemos la matriz de riesgos, tal como se ilustra a continuación:

Probabilidad	Muy alta	Medio	Alto	Muy alto	Muy alto
	Alta	Bajo	Alto	Muy alto	Muy alto
	Baja	Bajo	Medio	Alto	Muy alto
	Improbable	Bajo	Bajo	Medio	Muy alto
		Muy limitado	Limitado	Significativo	Muy significativo
		Impacto			

Probabilidad x Impacto para determinar el nivel de riesgo

Niveles de impacto y probabilidad aplicables al tratamiento de datos personales.

El nivel de impacto dependerá del daño o afectación que se pueda ocasionar a los titulares de los datos personales, así como a la sociedad en su conjunto; siempre en el ámbito de los derechos y libertades. La probabilidad está asociada a la posible materialización del riesgo.

A continuación, se presentan criterios de niveles de impacto y determinación de probabilidad, sustentados en los lineamientos de la Agencia Española de Protección de Datos.

Criterios para determinar los niveles de impacto[5].

Nivel de Impacto	Descripción	Derechos fundamentales
Muy significativo	Afecta al ejercicio de derechos fundamentales y libertades públicas establecidos en la Constitución, y sus consecuencias son irreversibles y/o Las consecuencias están relacionadas con categorías especiales de datos o relativos a infracciones penales, y es irreversible. y/o	Igualdad No discriminación Vida Integridad física Libertad religiosa Libertad personal Intimidad personal y familiar Propia imagen

[5] Consultar la Guía del riesgo y evaluación de impacto en tratamiento de datos personales.

Muy Significativo	Causa un daño social significativo, como la discriminación, y es irreversible y/o Afecta a interesados en situación de especial vulnerabilidad, en particular niños, y de forma irreversible. y/o Causa perdidas morales o materiales significativas e irreversibles.	Expresión Información Cátedra Reunión Asociación Libre acceso a cargos y funciones públicas en condiciones de igualdad
Significativo	Los casos anteriores cuando los efectos son reversibles. y/o Pérdida de control del interesado sobre sus datos personales, cuando la extensión de los datos sea alta con relación a las categorías de datos o al número de sujetos. y/o Se produce o puede producirse usurpación de la identidad de los interesados y/o Pueden producirse pérdidas financieras significativas a los interesados y/o Pérdida de confidencialidad de datos sujetos al deber de secreto profesional o vulneración del deber de confidencialidad y/o Existe un perjuicio social para los interesados o determinados colectivos de interesados	Tutela judicial efectiva Legalidad penal Educación Libertad de sindicación Derecho de petición

Limitado	Pérdida muy limitada del control de algún dato personal y a interesados puntuales, que no sea categoría especial o relativos a infracciones o condenas penales de carácter irreversible y/o Pérdidas financieras, insignificantes e irreversibles y/o Perdida de confidencialidad de datos sujetos al secreto profesional pero que no sean categorías especiales o sobre infracción penales	
Muy Limitado	En el caso anterior, cuando todos los efectos son reversibles.	

Criterios para determinar la probabilidad del riesgo[6].

Probabilidad	
Muy Alta	Si el factor de riesgo está materializado y no depende de la probabilidad. Por ejemplo: se identifica el uso de una tecnología como un riesgo y está presente en el tratamiento. y/o Si hay constancia de diversas materializaciones de dicho riesgo en el último año en distintas entidades. y/o Si hay constancia de una materialización de dicho riesgo en el último año en la misma entidad. y/o Existen auditorías/estudios que identifican importantes vulnerabilidades en los procedimientos

[6] Consultar la Guía del riesgo y evaluación de impacto en tratamiento de datos personales.

	organizativos o medios técnicos vinculados con dicho riesgo.
Alta	Si hay constancia de una materialización de dicho riesgo en el último año en alguna entidad. y/o Existen estudios que determinan que la probabilidad podría ser alta. y/o Existen auditorías/estudios que identifican posibles vulnerabilidades en los procedimientos organizativos o medios técnicos vinculados con dicho riesgo. y/o Los elementos vinculados con los factores de riesgo se han implementado con tecnologías o procedimientos organizativos no maduros, sin seguir normas de calidad, sin estar certificados por terceros independientes
Baja	Si hay constancia de una materialización de dicho riesgo en los últimos 10 años en alguna entidad.
Improbable	Si no hay constancia de materialización de dicho riesgo en ningún caso.

Lista de Factores de Riesgo.

Se debe tener en cuenta todos los factores ya identificados en la normativa sobre protección de datos personales, así como en la normativa especial, y determinar si estos afectan, o son susceptibles de afectar, al tratamiento.

Las categorías son las siguientes:

Operaciones relacionadas con los fines de tratamiento	Factores de riesgo que se derivan del fin declarado del tratamiento y otros fines vinculados al propósito principal.
Tipos de datos utilizados	Factores de riesgo relacionados con el ámbito del tratamiento que se derivan de los datos recogidos, procesados o inferidos en el tratamiento.

Extensión y alcance del tratamiento	Factores de riesgo relacionados con el ámbito del tratamiento relativos al número de sujetos afectados, la diversidad de datos o aspectos tratados, la duración en el tiempo, el volumen de datos, la extensión geográfica, la exhaustividad sobre la persona, la frecuencia de recogida, etc.
Categorías de interesados	Factores de riesgo relacionados con el ámbito del tratamiento relativos a la categoría de interesados, como empleados, menores, mayores, personas en situación de vulnerabilidad, víctimas, discapacitados, etc.
Factores técnicos del tratamiento	Factores de riesgo que se derivan de la naturaleza del tratamiento al implementarse con determinadas características técnicas o tecnologías.
Recogida y generación de datos	Factores de riesgo que se derivan de la naturaleza del tratamiento al recogerse o generarse datos de forma específica.
Efectos colaterales del tratamiento	Factores de riesgo que se derivan del contexto del tratamiento al poder generarse consecuencias no contempladas en los propósitos originales previstos del tratamiento.
Categoría del responsable/encargado	Factores de riesgo que se derivan del contexto específico del sector de actividad, modelo de negocio o tipo de entidad.
Comunicaciones de datos	Factores de riesgo que se derivan del contexto en el que se realizan las comunicaciones de datos a terceros en el marco del tratamiento.
Brechas de seguridad	Factores de riesgo que se derivan de la posible materialización de brechas de seguridad sobre los datos personales.

Asimismo, los factores de riesgo en el tratamiento de datos se ejemplarizan en el “Listado de Factores de Riesgo” que forma parte de la presente Metodología como Anexo D.

Niveles de riesgo al nivel de cumplimiento regulatorio.

Los niveles de riesgo en el tratamiento de datos personales están determinados tanto por el uso de tecnologías que puedan afectar la seguridad y confidencialidad de los datos, como por las infracciones y multas detalladas en la LOPD. En ese sentido, se debe tener en consideración lo siguiente:

Niveles de riesgo legal en el tratamiento de datos personales		Volumen de negocio (VN) Ejercicio Fiscal 2022
Infracciones leves	En el caso de la comisión de estas infracciones, el riesgo legal y económico asociado es una multa económica entre el 0.1% y 0.7% calculada sobre el volumen de negocio[7] correspondiente al ejercicio económico inmediatamente anterior al de la imposición de la multa.	[Por favor incluir el monto correspondiente]: Multa mínima: 0.1% VN = [*] Monto máximo: 0.7% VN = [*]
Infracciones graves	En el caso de la comisión de estas infracciones, el riesgo legal y económico asociado es una multa económica entre el 0.7% y el 1% calculada sobre el volumen de negocios, correspondiente al ejercicio económico inmediatamente anterior al de la imposición de la multa.	[Por favor incluir el monto correspondiente] Multa mínima: 0.7% VN = [*] Monto máximo: 1% VN = [*]

Riesgos asociados al nivel de cumplimiento regulatorio y medidas de control.

Riesgos asociados al nivel de cumplimiento regulatorio y medidas de control			
Posible infracción	Actividad que gatilla el riesgo	Multa Potencial	Medida de control
Leve	No tramitar, tramitar fuera del término previsto o negar injustificadamente las peticiones o	Multa económica entre el 0.1% y 0.7% calculada sobre el volumen de	Establecer un procedimiento de atención a los derechos de los titulares de los datos personales, aplicable a todas las categorías de

[7] Conforme al artículo 73 de la LOPD, se entiende por volumen de negocio a la cuantía resultante de la venta de productos y de la prestación de servicios realizados por operadores económicos, durante el último ejercicio que corresponda a sus actividades, previa deducción del Impuesto al Valor Agregado y de otros impuestos directamente relacionados con la operación económica.

	quejas realizadas por el titular.	negocio[8] correspondiente al ejercicio económico inmediatamente anterior al de la imposición de la multa. Multa económica entre el 0.1% y 0.7% calculada sobre el volumen de negocio[9] correspondiente al ejercicio económico inmediatamente anterior al de la imposición de la multa.	tratamiento de datos personales.
Leve	No implementar protección de datos desde el diseño y por defecto.		Mantener actualizado el registro de actividades de tratamiento, con especial énfasis en la determinación de las finalidades determinadas, específicas y legales, antes del inicio de una nueva actividad de tratamiento. Aplicar el principio de minimización de
Leve	No mantener disponibles políticas de protección de datos personales afines al tratamiento de datos personales.		Aprobar las políticas de privacidad adecuadas a las finalidades de tratamiento detalladas en el registro de actividades de tratamiento.
Leve	Elegir un encargado del tratamiento de datos personales que no ofrezca garantías suficientes para hacer efectivo el ejercicio del derecho a la protección de datos personales.		Incorporar cláusulas de protección de datos personales con los encargados de tratamiento para asegurar: (i) el uso de los datos personales únicamente para las finalidades establecidos en el encargo, (ii) confidencialidad de los datos personales requiriendo medidas de seguridad organizativas, técnicas y legales.
Grave	No implementar medidas administrativas, técnicas y físicas, organizativas y jurídicas, a fin de	Multa económica entre el 0.7% y el 1% calculada sobre el volumen de	Aprobar y mantener actualizadas (i) Política institucional de protección de datos personales, (ii) Política de retención de datos personales, (iii)

[8] Conforme al artículo 73 de la LOPD, se entiende por volumen de negocio a la cuantía resultante de la venta de productos y de la prestación de servicios realizados por operadores económicos, durante el último ejercicio que corresponda a sus actividades, previa deducción del Impuesto al Valor Agregado y de otros impuestos directamente relacionados con la operación económica.
[9] Conforme al artículo 73 de la LOPD, se entiende por volumen de negocio a la cuantía resultante de al venta de productos y de la prestación de servicios realizados por operadores económicos, durante el último ejercicio que corresponda a sus actividades, previa deducción del Impuesto al Valor Agregado y de otros impuestos directamente relacionados con la operación económica.

	garantizar el tratamiento de datos personales que realice conforme la LOPD y normas complementarias que sean emitidas.	negocios, correspondiente al ejercicio económico inmediatamente anterior al de la imposición de la multa.	procedimientos de aprobación de finalidades de tratamiento, (iv) el registro de actividades de tratamiento.
Grave	Utilizar información o datos para fines distintos a los declarados.		Aprobar y mantener actualizado: (i) el registro de actividades de tratamiento; (ii) el procedimiento de aprobación de finalidades de tratamiento, aplicando los principios de consentimiento, finalidad, proporcionalidad, minimización de datos, calidad, seguridad y confidencialidad.
Grave	Ceder o comunicar datos personales sin cumplir con los requisitos y procedimientos establecidos en la LOPD.		Mantener debidamente monitoreados a los encargados de tratamiento, así como a los receptores de datos personales a nivel nacional o internacional, identificando la finalidad de transferencia de los datos.
Grave	No utilizar metodologías de análisis y gestión de riesgos adaptadas a la naturaleza de los datos personales las particularidades del tratamiento y de las partes involucradas.	Multa económica entre el 0.7% y el 1% calculada sobre el volumen de negocios, correspondiente al ejercicio económico inmediatamente anterior al de la imposición de la multa.	Mantener actualizada la metodología para la evaluación de riesgos en función de las actividades de tratamiento, y aplicar el Estudio de Impacto en Protección de Datos cuando corresponda.
Grave	No realizar evaluaciones de impacto al tratamiento de datos en los casos		Aplicar la metodología indicada en los casos en los que la LOPD requiera la realización de un Estudio

	en que era necesario realizarlas.		de Impacto en Protección de Datos Personales.
Grave	No implementar medidas técnicas organizativas o de cualquier índole, necesarias para prevenir, impedir, reducir, mitigar y controlar los riesgos y las vulneraciones a la seguridad de datos personales que hayan sido identificadas.		Aprobar, aplicar y mantener actualizadas políticas institucionales de protección de datos personales, políticas de seguridad de la información, política de control de accesos y gestión periódica de privilegios asignados, procedimientos técnicos que garanticen la anonimización o seudonimización de los datos personales. Tal y como la privacidad desde el diseño y por defecto.
Grave	No notificar a la Autoridad de Protección de Datos Personales y al titular, de vulneraciones a la seguridad y protección de datos personales, cuando afecte los derechos fundamentales y libertades individuales de los titulares.		Aprobar y mantener actualizadas las políticas institucionales de protección de datos personales que mantengan un procedimiento de notificación de vulneración a la seguridad y protección de datos personales.
Grave	No suscribir contratos que incluyan cláusulas de confidencialidad y tratamiento	Multa económica entre el 0.7% y el 1% calculada sobre el volumen de	Aprobar y aplicar cláusulas de confidencialidad en los contratos con los encargados de tratamiento de datos personales, incluyendo las

	adecuado de datos personales con el encargado y el personal a cargo del tratamiento de datos personales o que tenga conocimiento de los datos personales.	negocios, correspondiente al ejercicio económico inmediatamente anterior al de la imposición de la multa.	cláusulas de confidencialidad de colaboradores y terceros.
Grave	No mantener actualizado el Registro Nacional de protección de datos.		Aprobar y mantener actualizado el registro de actividades de tratamiento de datos personales y el procedimiento de aprobación de finalidades de tratamiento de datos personales.
Grave	No consignar en el Registro Nacional de Protección de Datos Personales lo dispuesto en la LOPD y normas complementarias.		Aprobar y mantener actualizado el registro de actividades de tratamiento de datos personales y el procedimiento de aprobación de finalidades de tratamiento de datos personales.
Grave	No designar al delegado de protección de datos personales cuando corresponda.		Aprobar la designación del Delegado de Protección de Datos Personales y establecer los mecanismos para la comunicación ante la Autoridad Nacional de Protección de Datos Personales.
Grave	No permitir y no contribuir a la realización de auditorías o inspecciones por parte del auditor acreditado por la Autoridad de Protección de Datos Personales.		Colaborar y brindar la información solicitada por la Autoridad Nacional de Protección de Datos Personales, en los casos de auditorías.

Grave	Incumplir las medidas correctivas ordenadas por la Autoridad Nacional de Protección de Datos Personales.	Multa económica entre el 0.7% y el 1% calculada sobre el volumen de negocios, correspondiente al ejercicio económico inmediatamente anterior al de la imposición de la multa.	Monitorear de manera constante cualquier actividad de fiscalización iniciada por la Autoridad y coordinar las acciones necesarias para el cumplimiento cabal de las órdenes correctivas impuestas por la autoridad.

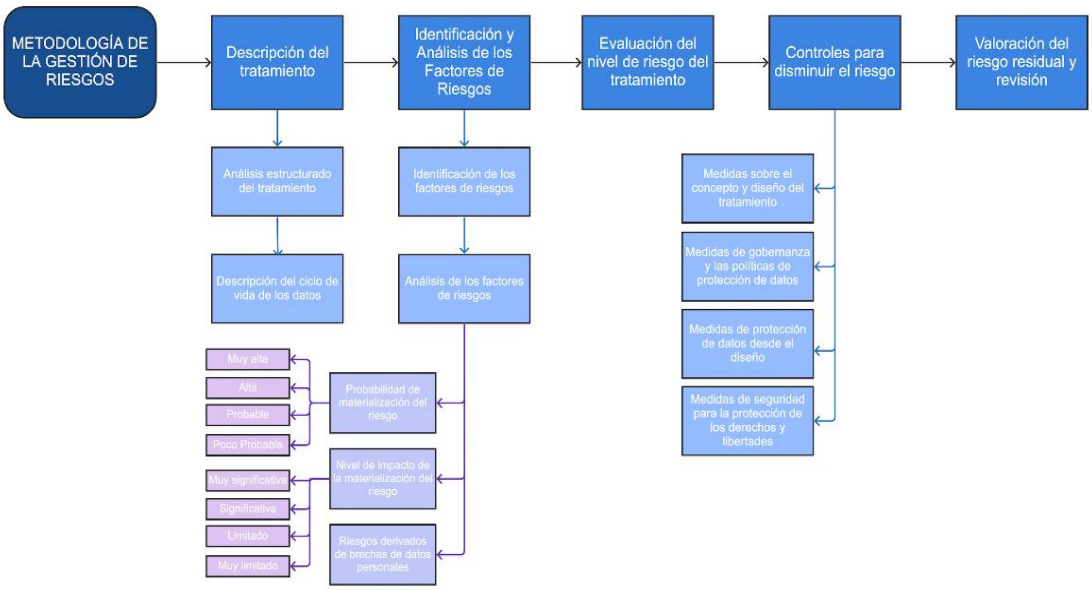
Medidas de seguridad como control para disminuir riesgos.

Estas medidas deben entenderse en sentido amplio, entonces, deben cubrir tanto aspectos relativos (por ejemplo, accesos no autorizados) y posibles amenazas, como los accidentes naturales o producto de errores humanos, etc.

Por lo tanto, se deben establecer medidas preventivas y correctivas, y a la par, evaluar el impacto que tendría un incidente (intrusiones, ataques, etc.) en los derechos y libertades de las personas físicas, esta evaluación debe considerar tantos incidentes accidentales (tecnológicos y humanos) como de eventos naturales. Además, establecer cómo se va a gestionar los posibles errores o fallos de las medidas técnicas y organizativas implementadas. Por último, gestionar los errores técnicos producto de la implementación de las medidas de seguridad.

Flujograma de la metodología de la gestión de riesgos.

La presente metodología de gestión de riesgos se resume en las acciones establecidas en el siguiente flujograma:



ESTUDIO DE IMPACTO EN PROTECCIÓN DE DATOS

¿Qué es una evaluación de impacto en protección de datos?

Es la evaluación que debe hacer el Responsable del Tratamiento desde el inicio, en la fase de diseño, las acciones preventivas suficientes para poder identificar, evaluar y tratar los riesgos asociados de datos personales con el objetivo de garantizar los derechos y libertades de las personas físicas.

Asimismo, según las Directrices WP 248[10], la evaluación de impacto debe entenderse como un proceso donde se describe el tratamiento de los datos personales, al cual se le realiza una evaluación de necesidad y proporcionalidad con la finalidad de evaluar si es recomendable o no el tratamiento de datos personales.

Es importante señalar que esta evaluación es un complemento a la gestión de riesgos, por lo tanto, se encuentra dentro de esta, y le añade un grado de dedicación y complejidad a la hora de su elaboración, dado que le incorpora elementos como: análisis de necesidad y proporcionalidad; realizar la evaluación de impacto antes del inicio de las actividades de tratamiento; exige un asesoramiento del Delegado de Protección de Datos; si es necesario, recabar la opinión de interesados o representantes de los datos en tratamiento; entre otros.

En consecuencia, el resultado de la evaluación determina la viabilidad del tratamiento, por lo tanto, es una herramienta para fundamentar la toma de decisiones por parte del Responsable del Tratamiento de Datos Personales.

[10] Grupo de Trabajo de "Protección de Datos" del Artículo 29. Directrices sobre la Evaluación de Impacto relativa a la Protección de Datos. Este grupo de trabajo se creó de conformidad con el artículo 29 de la Directiva 95/46/CE. Se trata de un órgano consultivo independiente de la UE en materia de protección de datos y privacidad. Sus funciones se describen en el artículo 30 de la Directiva 95/46/CE y en el artículo 15 de la Directiva 2002/58/CE.

La evaluación de impacto deberá efectuarse previo al inicio del tratamiento de datos personales.

¿Cuándo es obligatorio realizar un EIPD?

Si bien la obligación de realizar una evaluación de impacto depende de la legislación de cada país, en el caso ecuatoriano, la obligatoriedad de realizarla se da en los siguientes casos[11]:

Evaluación sistemática y exhaustiva de aspectos personales de personas físicas que se base en un tratamiento automatizado, como la elaboración de perfiles, y sobre cuya base se tomen decisiones que produzcan efectos jurídicos para las personas naturales;

Tratamiento a gran escala de las categorías especiales de datos, o de los datos personales relativos a condenas e infracciones penales, u

Observación sistemática a gran escala de una zona de acceso público. La Autoridad de Protección de Datos Personales establecerá otros tipos de operaciones de tratamiento que requieran una evaluación de impacto relativa a la protección de datos.

Cabe resaltar que esta lista no es taxativa, por lo tanto, el Responsable del Tratamiento que no esté obligado a realizar la evaluación de impacto puede realizarla en aras de ser más diligente al momento de realizar el tratamiento de los datos personales.

Asimismo, la Autoridad de Protección de Datos Personales podrá emitir listas específicas de tratamientos de datos sujetos a EIPD de forma obligatoria.

¿Quién debe realizar la evaluación de impacto?

Si bien es el responsable del tratamiento quien responde por la elaboración de la evaluación de impacto, es el DPD (Delegado de Protección de Datos) quien debe asesorar la realización la mencionada evaluación[12].

¿Qué debe incluir?

Una descripción sistemática de la actividad de tratamiento previstas.

Una evaluación de la necesidad y proporcionalidad del tratamiento respecto a su finalidad.

[11] Artículo 42 de la Ley Orgánica de Protección de Datos Personales.
[12] Numeral 3, Artículo 49° de la Ley Orgánica de Protección de Datos Personales.

Una evaluación de los riesgos.

Las medidas previstas para afrontar riesgos (incluidas garantías, medidas de seguridad y mecanismos que garanticen la protección de datos personales.

Es importante señalar la información contenida en la evaluación de impacto debe ser documentada de la manera más eficiente, sea positivo o negativo el resultado de la evaluación.

(MARSH Y ESTUDIO OILOCHEA, 2022)

ANEXO 2. **CONDICIONES DEL TRATAMIENTO DE DATOS PERSONALES DE CLIENTES**
DE XXXXXXXXXXXXX

De conformidad con lo dispuesto en el artículo 12 de la Ley Orgánica de Protección de Datos Personales, el **XXXXXXXXXXXXX,** identificado con RUC No. 1790098354001, con domicilio en la ciudad de Quito - Av. Patria E 4-21 y Av. 9 De Octubre**,** cumple con el deber de informar relacionado al tratamiento de los datos personales de sus **clientes**. En ese sentido, en base a la Ley Orgánica de Protección de Datos Personales, promulgada en el Registro Oficial Suplemento No. 459 de 26 de mayo de 2021, (en adelante, la "LOPDP") **EL CLIENTE** declara haber sido apropiadamente informado respecto del tratamiento de los datos personales, en los términos siguientes:

Base de Datos. El XXXXXXXXXXXXX S.A. es titular de la base de datos denominada "CLIENTES" y "MARKETING Y DESARROLLO DE NEGOCIOS", las cuales serán oportunamente registradas ante la Autoridad de Protección de Datos Personales. Las bases de datos son manejadas directamente desde el domicilio de XXXXXXXXXXXXX S.A., ubicado en la ciudad de Quito - Av. Patria E 4-21 y Av. 9 De Octubre.

2. **Datos Personales Obligatorios para cumplimiento de relación contractual que el cliente mantenga con XXXXXXXXXXXXX S.A.. EL CLIENTE** tiene conocimiento que los datos proporcionados al **XXXXXXXXXXXXX,** que se otorgan son obligatorios con motivo de la preparación, suscripción y/o ejecución de una relación contractual mediante la cual **EL CLIENTE** adquiere productos o servicios bancarios. Los datos personales requeridos son: Identificación; Nombre y Apellido; Barrio/Distrito de nacimiento; Dirección de domicilio; Celular, correo personal; Teléfono de trabajo; Fecha de nacimiento; Nacionalidad; Género; Estado Civil; Cónyuge; sociedad conyugal; Nivel de educación; teléfono móvil para interacción con banca móvil; Datos crediticios; Persona Expuesta Políticamente, Relación Laboral; Dirección de trabajo; Información tributaria (impuestos en el exterior); Actividad Económica, Fuente de ingresos; Activos, Pasivos, Patrimonio; Dirección de tributación en exterior, ingresos y egresos mensuales; además de cualquier otra información necesaria para la relación contractual, por lo tanto **XXXXXXXXXXXXX** tiene una necesidad legítima de acceder y procesar los datos para los fines anteriormente indicados**.**

2.1.Finalidad: Los datos personales serán utilizados para cumplir con las siguientes finalidades:

(xii)Cumplir con la norma Conozca a su Cliente.

(xiii) Prestación de servicios o productos financieros, como apertura de cuentas bancarias de ahorros, cuenta corriente, cuenta de ahorro programado, cuenta de ahorro rentable, entre otras, emisión de tarjetas de crédito y débito, entre otros, certificados de depósito, créditos vehiculares, hipotecarios y de consumo, entre otros productos, así como lo referente al contrato de vinculación.

(xiv) Transferencia de los datos del cliente a las empresas procesadoras y emisoras de tarjetas de crédito.

(xv) Velar porque el proceso y calidad de los datos sean correctos y actualizados.

(xvi) Mejorar el uso de los datos, definir los procesos que serán ejecutados por el área comercial.

(xvii) Verificación de la información proporcionada por el cliente mediante fuentes públicas y privadas para cumplimiento de normas de prevención de lavado de activos y financiamiento de terrorismo, previo al otorgamiento de servicios o productos bancarios.

(xviii) Recopilación de datos del equipo móvil, para procesos de autenticación de banca móvil.

(xix) Envío de SMS para autenticación de uso de contraseñas o movimientos en cuentas o productos relacionados con el Banco.

(xx) Prestación de servicios de banca online y móvil como servicios auto gestionables por parte del cliente para bloqueos de cuenta.

(xxi) Verificación de transacciones mediante uso de cajeros automáticos (retiro o depósito, pago servicios).

(xxii) Coordinación de entrega o envío de información o comunicaciones relacionadas a los productos contratados con el Banco, envío de plásticos de tarjetas de crédito o débito, comunicaciones de seguimiento respecto de los productos o servicios solicitados por el Cliente.

3. <u>Datos Personales con para tratamiento de datos con fines de marketing.-</u>

3.1.<u>Datos Personales con fines de Marketing</u>. Los datos requeridos de los usuarios en la interacción con las distintas plataformas (digital, redes sociales y telefónica) del **XXXXXXXXXXXXX** son los siguientes:

(v) **Datos de carácter identificativo:** Nombres y apellidos, número de cédula (sólo en página), correo electrónico, dirección, teléfono.
(vi) **Datos de características personales:** edad, estado civil, sexo, relación laboral
(vii) **Datos de carácter social:** hábitos de navegación y tipo de transacciones.
(viii) **Datos de carácter económico y financiero:** ingreso mensual (dependiente/independiente), actividades económicas.

3.2.Finalidad y Usos. El Usuario tiene conocimiento que los datos proporcionados al **XXXXXXXXXXXXX** se otorgan con el fin de cumplir con las siguientes finalidades:

(xii) Desarrollo de productos, servicio al cliente e inteligencia de negocios.

(xiii) Desarrollo de marca (comunicación externa, comunicación digital, relaciones públicas, y sostenibilidad).

(xiv) Manejo de comunicación externa, digital, relaciones públicas y sostenibilidad. Se incluye página web y mail marketing, redes sociales.

(xv) Desarrollo de productos, relacionados a activo, pasivo, banca seguros y transporte de valores, factoring y confirming.

(xvi) Oferta de valor para nuevos segmentos.

(xvii) Servicio al cliente. Revisión de la llamada de servicio al cliente.

(xviii) Inteligencia de negocios. Generar conocimiento a través de la información de los clientes, generación de campañas comerciales, paneles de visualización.

(xix) Aplicación de modelos de ciencia de datos (machine learning) para modelos de segmentación de clientes, modelos de retención, modelos para realización de ventas cruzada, uso de y evaluación de métricas de precisión, modelo para evaluar el perfil digital del cliente.

(xx) Campañas en la web pública y los mensajes de inbox de redes sociales, en relación a potenciales clientes para captación de nuevos productos.

(xxi) Impulso de ventas a través de canales de contact center, mediante canales de comunicación de nuevos productos o servicios.

(xxii) Fortalecer el uso de aplicaciones móviles del banco.

En cumplimiento de la LOPDP, el Usuario acepta el tratamiento de sus datos personales, y al hacer "clic" en la sección "Otorgo mi consentimiento", otorga su consentimiento libre, previo, expreso, informado e inequívoco para que sus datos personales, sean incorporados en sus bases de datos personales y sean tratados con todas las medidas de seguridad y confidencialidad establecidas en el marco legal aplicable

○ Sí otorgo mi consentimiento. ○ No otorgo mi consentimiento	Tratamiento de mis datos personales para finalidades asociadas a marketing, publicidad o perfilamiento.

4. **<u>Plazo</u>.** El plazo de conservación de los datos se sujeta al plazo de vigencia del Contrato, y serán conservados por los plazos establecidos en el Código Orgánico Monetario y Financiero y demás normas conexas o hasta que usted ejercite el derecho de revocación o cancelación

conforme a la LOPD, sin embargo, el **BANCO** se reservará el derecho de retener los datos en caso que la cancelación no sea posible por mandato legal o motivo debidamente fundamentado.

5. **Transferencia de Datos Personales.** Para cumplir con los fines indicados en el punto 3, los datos personales de **EL CLIENTE** podrán ser transferidos de forma local o internacional, de acuerdo con el siguiente detalle:

5.1. Transferencia de Datos Personales a Nivel Nacional. Para cumplir con la finalidad de indicada, **XXXXXXXXXXXXX** debe transferir los datos personales a nivel nacional a las siguientes entidades:

5.1.1. Superintendencia de Bancos, Banco Central del Ecuador, Servicio de Rentas Internas.
5.1.2. Compañías de gestión con Call Center
5.1.3. Compañías de Gestión de canales electrónicos y ventas de Asistencias.
5.1.4. Empresas de verificación de datos.
5.1.5. Empresas de gestión documental.
5.1.6. Transferencia a empresas procesadoras de las tarjetas.
5.1.7. Agencias de medios digitales y Agencia de medios tradicionales.

6. **Transferencia de Datos Personales a Nivel Internacional. LA EMPRESA** cumple con informar a **EL CLIENTE** las siguientes transferencias internacionales, con el fin de garantizar la obligación contractual a generarse:

6.1. Proveedor de herramientas colaborativas en red.
6.2. Estados Unidos. Microsoft Corp, proveedor de hosting de página web del dominio xxxxxxxxxxxxxxxxxxxx.

7. **Ejercicio de Derechos.** Para realizar una solicitud de acceso, rectificación, eliminación (cancelación), oposición de su información personal o cualquiera de los derechos indicados en los artículos 13 a 19 de la LOPDP, o para obtener información adicional sobre esta declaración de protección de datos personales y para garantizar sus derechos dirigirse a la página web: xxxxxxxxxxxxxxxxxxxxxx en la sección, "POLITICA DE PRIVACIDAD Y DE SEGURIDAD", acceso a los derechos y principios de la Ley de Protección de Datos Personales.

8. **Garantía. EL CLIENTE** tiene conocimiento que **XXXXXXXXXXXXX** garantiza que el tratamiento de sus datos personales cumplirá con las medidas de seguridad necesarias a fin de evitar cualquier alteración, pérdida, tratamiento no autorizado y/o cualquier riesgo, amenaza o vulnerabilidad.

9. **Derecho/Deber de Información.** Por medio de la presente, **EL CLIENTE** declara haber recibido la información relativa al tratamiento de sus datos personales, conoce que el tratamiento de sus datos personales se utiliza para la preparación, celebración y ejecución de una relación contractual, para cumplir con las finalidades indicadas en el punto uno del presente ANEXO, por lo tanto, el presente tratamiento de datos personales es legítimo y lícito

conforme al numeral 5 del artículo 7 de la LOPDP, encontrándose exceptuada de consentimiento conforme a lo establecido en el numeral 2 del artículo 36 de la LOPDP.

Nombres y Apellidos: _____

Documento de identidad N°: _____

Correo electrónico: _____

Firma: _____

ANEXO 3. **Disclaimer usuarios del sistema financiero no clientes.**

Disclaimer de entrega de la información: Estimado usuario, al llenar los datos y dar *click* en la opción "Continuar", que se realiza en virtud del servicio o producto a contratarse, usted autoriza expresamente a XXXXXXXXXXXXXX S.A. para el tratamiento de datos personales, los cuales han sido entregados, y de los cuales el Banco protegerá su privacidad de conformidad con lo establecido en la Ley Orgánica de Protección de Datos Personales. El usuario declara que la información proporcionada, es veraz, íntegra, precisa y verdadera. En caso de que lo anterior fuese falso, XXXXXXXXXXXXXX. no asumirá ninguna responsabilidad y estará en capacidad de negar el producto o servicio solicitado.

Además, el usuario autoriza expresamente a XXXXXXXXXXXXX para que pueda obtener datos de fuentes de información y crediticias válidas, con el fin único de valorar la conducta crediticia y capacidad de pago del usuario financiero. EL BANCO almacenará sus datos personales mientras dure la fase pre-contractual. Sus datos podrán ser transferidos a nivel nacional e internacional, conforme al detalle que estará contenido en el Consentimiento informado de Protección de Datos de Personales de Clientes.

En caso de duda sobre el alcance del tratamiento y/o almacenamiento de sus datos personales, por favor dirigirse a la página web:

xxxxxxxxxxxxxxxxxx/ en la sección, "POLITICA DE PROTECCIÓN DE DATOS Y DE SEGURIDAD"

ANEXO 4. PROTECCIÓN DE DATOS PERSONALES

De conformidad con lo dispuesto en el artículo 12 de la Ley Orgánica de Protección de Datos Personales, las Partes suscriben el presente **Anexo de Protección de Datos Personales**, de ahora en adelante ***"Anexo",*** vigente a partir del _____ ahora en adelante ***"Fecha de Vigencia"***, por y entre **XXXXXXXXXXXXX S.A.** representado por el _____ en calidad de _____ y como tal debidamente para suscribir este tipo de actos y contratos en nombre del BANCO, parte a la de ahora en adelante se denominará *"**Parte Responsable del tratamiento de datos Personales***" y/o ***"El Banco",*** con oficina matriz en Av. Patria E4-21 y 9 de Octubre, Quito, Ecuador, y _____, en su calidad de _____, y con domicilio en _____parte a la que para efectos de este convenio se denominará la *"**Parte Encargada del Tratamiento de Datos Personales"*** y/o ***"El Proveedor"***, con dirección en la ciudad de Quito, ambos llamados colectivamente *"**Las Partes"***.

Las *Partes* de manera libre y voluntaria y por los derechos que representan, han convenido en suscribir el presente ***ANEXO*** para establecer los términos que regirán para la "Protección de datos Personales" en relación a información de clientes, accionistas y personal, que proporcionada por XXXXXXXXXXXXX S.A. a ***"El Proveedor"*** con el propósito de cumplir con los servicios contratados por el BANCO, a través del Contrato _____, del que forma parte, de ahora en adelante "Propósito autorizado".

PRIMERA: OBJETO DEL ENCARGO DEL TRATAMIENTO.-

El objeto del presente ***Anexo*** es habilitar a ***"El Proveedor",*** en su calidad de "Encargado del tratamiento de datos personales", para tratar por cuenta de XXXXXXXXXXXXX S.A., los datos de carácter personal que este proporcione para el cumplimiento del objeto del Contrato _____.

A los efectos del presente Anexo, se entenderá por "tratamiento" cualquier operación o conjunto de operaciones que se realicen sobre los Datos Personales del Cliente, ya sea por medios automáticos o no, tales como la recogida, recopilación, intención, registro, organización, estructuración, almacenamiento, adaptación o alteración, recuperación, consulta, utilización, divulgación por transmisión, difusión o puesta a disposición de otra forma, alineación o combinación, bloqueo, borrado o destrucción, según la información personal que sea entregada por el BANCO a ***"El Proveedor"*** para el cumplimiento del objeto del contrato de _____.

SEGUNDA: DATOS PERSONALES.-

"Dato o Información personal" significará la información personal que hace identificable a un individuo relacionada a clientes, colaboradores y accionistas proporcionada por o en nombre del Banco a "El Proveedor", en relación con la prestación de los Servicios de _____, que de conformidad con la legislación en materia de protección de datos personales, se relaciona con un individuo vivo identificado o identificable; siempre y cuando, la Información Personal del Cliente no incluya información de tarjetas de presentación o sea de conocimiento público. La Información Personal que proporcione el BANCO a "El Proveedor", en relación con la prestación

de los Servicios se establece según la naturaleza del servicio a ser prestado por "El Proveedor", por lo que se entregará información que sea estrictamente necesaria para el cumplimiento cabal del objeto del Contrato.

Información Personal proporcionada por el Banco no incluirá ninguna información que haya sido anonimizada o seudonimizada de manera que los datos ya no se relacionen con una persona viva identificada o identificable.

TERCERA: RESPONSABILIDADES.-

3.1. RESPONSABILIDADES DEL ENCARGADO DE PROTECCIÓN DE DATOS PERSONALES.-

3.1.1. Dar a los datos personales a los que tenga acceso, un tratamiento acorde con el objeto del contrato, respetando la normativa sobre protección de datos personales.

3.1.2. Utilizar los datos personales objeto de tratamiento, o los que recoja para su inclusión, sólo para la finalidad objeto de este encargo. En ningún caso podrá utilizar los datos para fines propios.

3.1.3. No utilizar bases de datos que hayan sido obtenidas utilizando medios fraudulentos, desleales o ilícitos.

3.1.4. Será el único responsable de cuantas sanciones, multas o reclamos por daños se derivaren del incumplimiento de lo estipulado en esta Cláusula; y resarcirá a ***"el Banco"*** de los importes que por tales motivos hubiera tenido que abonar; ello, con inclusión de los gastos derivados de servicios jurídicos o de las costas y gastos de su defensa en cualquier juicio o procedimiento administrativo o judicial que se ocasionare. El incumplimiento al que aquí se alude, será considerado causal de resolución; y dará lugar a las indemnizaciones y reparaciones del caso a favor del perjudicado.

3.1.5. Cumplir y hacer cumplir todas las obligaciones y responsabilidades asumidas en el presente contrato a sus empleados, contratados y subcontratados y deberá:

3.1.5.1. Proteger y guardar la confidencialidad de los Datos Personales a los que tenga acceso y que formen parte, o estén destinados a ser parte de una base de datos de titularidad del ***"Banco".***

3.1.5.2. Procesar la información sólo en base a las instrucciones escritas del ***"Banco"*** o con la previa autorización escrita de éste.

3.1.5.3. Utilizar los datos personales otorgados por ***"el Banco"*** única y exclusivamente para los fines establecidos en el presente Contrato, y a guardar secreto profesional respecto a todos los datos de carácter personal que conozca y a los que tenga acceso.

3.1.5.4. Implementar medidas de seguridad, técnicas, físicas, organizacionales y legales apropiadas a los fines de proteger los datos personales contra cualquier destrucción accidental o ilícita, pérdida accidental, alteración, divulgación o accesos no autorizados o contra cualquier otro medio ilegal de tratamiento de estos.

3.1.5.5. No revelar los Datos Personales por ningún medio a ninguna persona fuera de los casos permitidos por el presente Contrato y/o sin el consentimiento previo y por escrito del titular de dichos datos o del titular de la base de datos personales. En

caso de ser intimada o requerida, por cualquier regulación, mandamiento judicial, notificación, citación o cualquier otro proceso legal y/o judicial válido, previo a cualquier divulgación deberá notificar por escrito a ***"El Banco"***.

3.1.5.6. Informar sobre cualquier tipo de evento o incidente que pudiera tener un impacto negativo sobre los datos personales al ***"El Banco"*** y prestar la asistencia necesaria para resolver el evento o incidente. La referencia a evento o incidente incluirá los escenarios de incidentes o brechas de seguridad o ciberataques. Para cumplir con esta obligación, ***"El Proveedor"*** deberá notificar de inmediato el evento o incidente a ***"El Banco",*** brindando la mayor información posible, así como un detalle de las primeras medidas de seguridad adoptadas para revertir el hecho, así como un detalle de las primeras acciones y recomendaciones que se deberán adoptar con la finalidad de proteger la información personal.

3.1.5.7. Proveer a ***"El Banco"*** de toda la información técnica, organizativa y jurídica relacionada con el tratamiento de datos personales que hubieran sido encargados para su tratamiento.

3.1.6. A solicitud escrita del ***"Banco"***, a la terminación o vencimiento del Contrato, "***El Proveedor"*** deberá, destruir de manera pronta, segura y confirmar dicha destrucción segura de toda la Información Personal del ***"Banco"*** en su posesión o control (incluyendo, sin limitación, todas las copias electrónicas tales como en discos duros, cintas de respaldo, dispositivos portátiles, medios de almacenamiento ópticos, magnéticos o de otro tipo, así como todas las copias impresas) o, si el BANCO lo solicita, devolver dicha Información Personal del BANCO.

3.2. RESPONSABILIDADES DEL RESPONSABLE DE PROTECCIÓN DE DATOS PERSONALES.-

3.2.1. Entregar al encargado los datos que fuesen necesarios para el cumplimiento del objeto del Contrato.

3.2.2. Verificar el cumplimiento de la normativa de Protección de datos personales durante todo el tratamiento.

3.2.3. ***"El Banco"*** declara que cumplirá con las Leyes de Protección de Datos Aplicables y manifiesta que cualquier instrucción que le proporcione a "El Proveedor" relacionada con el manejo y procesamiento de los Datos Personales del banco, sus clientes o colocadores, en relación con los Servicios que se prestarán, no hará que ***"el Proveedor"*** incumpla las Leyes de Protección de Datos Aplicables.

CUARTA: VIGENCIA.-

El presente acuerdo tiene una duración de _____. Una vez finalice el presente contrato, el encargado del tratamiento debe suprimir/devolver al responsable/devolver a otro encargado que designe el responsable (indicar la opción que proceda) los datos personales y suprimir cualquier copia que esté en su poder.