FACULTAD DE POSTGRADOS

MAESTRÍA EN DERECHO DIGITAL E INNOVACIÓN

TÍTULO DE LA INVESTIGACIÓN

PROPUESTA DE UN PLAN DE CUMPLIMIENTO DEL DELEGADO DE PROTECCIÓN DE DATOS PERSONALES EN UNA EMPRESA ECUATORIANA DE TELECOMUNICACIONES, 2022.

Profesor

Lorena Naranjo

Autores

Marco Vinicio Guerra Naranjo

Alex Santiago Navarrete Mora

2023

Tabla de contenido

RESUMEN

Las tecnologías de la información permiten conocer datos sobre los hábitos, consumos, e intereses de sus usuarios. Hoy en día, esta data se ha posicionado como la materia prima más importante en la economía de la información. Es decir, los datos personales se traducen en activos que fundamentan, o refutan, las decisiones para el desarrollo e implementación de nuevos negocios y productos.

Es así que, mientras las sociedades se encaminan paulatinamente a una mayor digitalización, se generan cada vez más contingentes relacionados al tratamiento de esos datos personales. Ante ello, el Derecho como ciencia ha buscado la manera de enmarcarlo en una normativa que propenda a la protección de los datos personales en la cual, en resumen, el dato es la persona misma; por lo tanto, se entiende a la protección a este derecho como un Derecho Humano.

Una de las herramientas que ha encontrado el Derecho para la implementación de la protección de datos, es la incorporación en la normativa de la figura del Delegado de Protección Datos. Este participante o actor en el sistema de protección cuya función es la de ejercer como asesor del encargado del tratamiento de estos datos, advierte sobre sus obligaciones legales y supervisa su cumplimiento normativo como se constituye en el nexo con la Autoridad de Protección de Datos Personales. También tiene como deber el generar, como parte del sistema de gestión de protección de datos personales, un Plan de Cumplimiento de las funciones o actividades que la Ley prevé para los fines que en ella se establecen.

Es así que, dentro de este estudio, se han identificado los procesos generales a los que el Delegado de Protección de Datos se ve abocado bajo la Ley Orgánica de Protección de

Datos Personales (LOPDP) para poder establecer un programa de cumplimiento de estas actividades sistemáticas que deben realizarse de manera continua en el tiempo.

Esta propuesta de Plan de Cumplimiento se basa en la necesidad de que el Delegado de Protección de Datos Personales pueda contar con una herramienta de carácter administrativo con la que guiar sus actividades. El propósito es reducir los riesgos propios del tratamiento de datos personales y dar seguimiento a la implementación de medidas de mitigación. Es decir, gestionar todo el sistema de protección de datos personales para el pleno cumplimiento de la normativa en estudio por parte de la Empresa de Telecomunicaciones, evitar las sanciones atinentes a la responsabilidad del Delegado de Protección de Datos en el ámbito civil, administrativo y penal en caso de omitir sus obligaciones.

INTRODUCCIÓN

Contexto del entorno interno y macro de la Organización

La Empresa de Telecomunicaciones, cuya razón social será omitida por motivos de confidencialidad en esta investigación, se constituyó en el país a principios de los años 90 como una compañía con capital ecuatoriano cuyo nicho era la prestación de servicios de comunicaciones celulares. Posteriormente, esta fue adquirida por una organización extranjera que buscó la expansión local y, actualmente forma parte de una corporación transnacional con operaciones en tres continentes, y con una fuerte presencia regional enfocada en el segmento corporativo y empresarial. Por ello, se puede considerar a la empresa como pionera de negocios digitales en el Ecuador.

La misión de esta organización es ofrecer conexiones que unen a las personas, y que las inviten a ser ellas mismas, a expresarse y a compartir.

Su visión es poner al alcance de las personas las posibilidades que ofrece la tecnología, y de esta forma, generar una mejor convivencia. Para hacer realidad esta visión, su estrategia es acercar lo mejor de la tecnología a sus clientes, a través de sus marcas comerciales.[1]

Sus principales servicios son las comunicaciones inalámbricas, a través de la prestación del Servicio Móvil Avanzado en modalidad postpago o prepago. Así mismo y, conforme los retos de la tecnología, los servicios de acceso a internet fijo y soluciones digitales para empresas, incluyendo el alojamiento o almacenamiento de información en la nube o servidores de la empresa.

[1] Se hace hincapié en la necesidad de mantener la confidencialidad evitando citar la fuente

Los clientes de la Empresa de Telecomunicaciones son personas naturales y jurídicas en busca de soluciones de telecomunicación inalámbrica que permitan la comunicación móvil con altos estándares de calidad, a través de las modalidades prepago (recargas) y planes pospago. Estos servicios los presta de conformidad con el título habilitante otorgado en su momento bajo la figura de concesión por la ahora Agencia de Regulación y Control de las Telecomunicaciones (ARCOTEL), de acuerdo con lo establecido en el numeral 1 del Art. 37 de la Ley Orgánica de Telecomunicaciones (LOT). Son los clientes identificados como personas naturales y sus datos aquellos que deben revestir una mayor importancia en el momento del análisis del tratamiento de datos personales.

Por experiencia, se conoce que, en el sector de telecomunicaciones los principales proveedores de la empresa son compañías que suministran bienes y servicios relacionados a la conectividad. Es decir: antenas, tarjetas electrónicas y licenciamiento de software; así como la integración entre las distintas estaciones base y el mantenimiento de infraestructuras para la interacción de los equipos. El soporte informático también cuenta con proveedores que son, al mismo tiempo, encargados del tratamiento de datos. Cabe indicar que la Empresa de Telecomunicaciones actúa en calidad de encargada del tratamiento de datos cuando interviene como revendedora, subcontratista o distribuidora de servicios prestados por terceros para sus clientes, tales como: *hosting*, *cloud* y seguros.

Por conocimiento del sector, en el Ecuador están perfectamente identificados los competidores de la Empresa de Telecomunicaciones, pues el mercado ecuatoriano es pequeño y poco atractivo para la entrada de muchos actores dentro del nicho. En la actualidad, el mercado de telecomunicaciones inalámbricas está compuesto por tres operadores, uno de ellos es la Empresa de Telecomunicaciones.

Las tecnologías de información y comunicación (TIC) juegan un papel importante en el desarrollo de las actividades que lleva a cabo la Empresa de Telecomunicaciones frente a las actuales formas de consumo y producción. La utilización de abundantes cantidades de información que cruzan por las redes y sistemas de la empresa, incluidos naturalmente datos personales, se constituye como la base para la estructuración de los servicios tradicionales de la industria, así como de nuevos servicios basados en el comportamiento de los clientes. Sin perjuicio de esto, en todos los entornos en donde se utilicen datos personales como parte de una economía de datos, se debe buscar el balance entre el derecho a la protección de datos personales y el progreso de las industrias.

La Empresa de Telecomunicaciones, en su calidad de responsable y encargada del tratamiento de datos personales, y como parte de los actores del sistema de protección de datos, requiere adecuarse a los nuevos contextos y realidades de los mercados internacionales, en donde la protección de datos personales tiene ya una larga tradición. Es importante tomar en cuenta que este activo se verá multiplicado exponencialmente en los próximos años.

Es indispensable que, para la innovación y desarrollo de actividades enmarcadas bajo esta protección, la Empresa de Telecomunicaciones otorgue al cliente la calidad de valor agregado bajo la premisa de que la utilización legítima de los datos personales es uno de sus pilares en sus relaciones comerciales, fomentando la confianza en las mismas y, por ende, maximizando los beneficios para la empresa. Adicionalmente, deberá adecuarse a lo señalado por el *Libro Blanco de la Sociedad de la Información y del Conocimiento* (2018) donde la protección de datos personales forma parte de los ejes estratégicos de la sociedad de la Información y del conocimiento en el Ecuador.

Buscando hacer una concreción de lo que de manera general la Empresa de Telecomunicaciones requiere en torno a cumplir con sus obligaciones derivadas de la LOPDP con relación al ciclo de vida del dato. Esta deberá llevar a todos sus procesos, bases y sistemas a cumplir con los principios establecidos en la norma, que son: juridicidad, lealtad, transparencia, finalidad, pertinencia, minimización de datos personales, proporcionalidad, confidencialidad, calidad, exactitud, conservación, seguridad de datos personales, responsabilidad proactiva y demostrada, aplicación favorable al titular e independencia del control. Así también, deberá propender a la promoción de los derechos de información, acceso, rectificación, actualización, eliminación, oposición, portabilidad, suspensión, y a no ser objeto de una decisión basada única o parcialmente en valoraciones automatizadas igualmente descritas en nuestra legislación.

Contexto del entorno externo de la organización.

Según el Banco Central del Ecuador (2022): "La economía ecuatoriana creció 3.8% durante el primer trimestre de 2022 en comparación con el mismo período de 2021 (…) El comportamiento del consumo de los hogares del primer trimestre de 2022 respondió al incremento de remesas, importaciones y créditos de consumo". Estos indicadores marcan un crecimiento sostenido en nuestra economía que provocará un incremento en el consumo de bienes y servicios, entre ellos, el servicio público de telecomunicaciones inalámbricas, como lo corroboran los índices estadísticos de inmersión a internet fijo y móvil determinados en la Política para la Transformación Digital del Ecuador 2022-2025 emitido mediante Acuerdo N° MINTEL-MINTEL-2022-0031 del Ministerio de Telecomunicaciones y de la Sociedad de la Información del 2 de noviembre de 2022.

Luego del paro nacional encabezado por el movimiento indígena en el mes de junio de 2022, haciendo un análisis retrospectivo, César Ulloa, en su artículo publicado en la *Revista Digital Latinoamérica 21* (2022, párr 7) menciona que este se produjo en un contexto donde: "En un año, el Ejecutivo había perdido 50% de apoyo pese al exitoso plan de vacunación, a haber logrado la estabilidad macroeconómica y a estar exento de acusaciones de corrupción", por lo que el escenario político se configuró, incluyendo nuevos objetivos a ser tratados en forma prioritaria. El Gobierno estableció una nueva agenda bajo las expectativas de soluciones a los problemas de los sectores desprotegidos, las cuales fueron tratadas por las mesas de diálogo conformadas de forma heterogénea.

Nuestro país, a diferencia de otros de la región, cuenta con un gran grupo de concentración poblacional urbana, que llega aproximadamente al 64,3% (de un total de 17.77 millones de habitantes aproximadamente). Por lo que la población rural es del 35,7%, y de ella solo el 16% cuenta con acceso a internet (Alvino, C. 2021). Los anteriores indicadores muestran aún un margen importante de sectores de telecomunicaciones que debe ser cubierto, con la aplicación de políticas estatales a través de planes y programas determinados para cumplir con el acceso y la universalización de las telecomunicaciones.

En el 2018, en *El Libro Blanco de la Sociedad de la Información y del Conocimiento* (Mintel, 2017, Pág. 57) publicado por el Ministerio de Telecomunicaciones y Sociedad de la Información (MINTEL) se estableció como prioridad la mejora e inmersión de tecnologías digitales a través de la universalización de las telecomunicaciones en la población que aún no cuenta con un servicio adecuado, siendo, en este punto, las empresas concesionarias actores importantes en la mejora de la prestación del servicio público de telecomunicaciones. Complementariamente, mediante Acuerdo Ministerial N°11-2017 de 20 de marzo de 2017, el MINTEL como organismo rector del sector de telecomunicaciones en Ecuador, en el

ejercicio de sus competencias para determinar las políticas aplicables al país, las materializó a través de la expedición de las Políticas Públicas del Sector de las Telecomunicaciones y de la Sociedad de la Información para los años 2017-2021.

Los desafíos ambientales de Ecuador en 2022 son, a su vez, una verdadera transición ecológica que busca implementar los acuerdos de Escazú y mayores recursos para las áreas protegidas (Montaño D, 2022, párr. 1, 2). El sector de telecomunicaciones en el entorno ambiental, a pesar de contribuir con un impacto positivo con relación a la propagación del servicio público de telecomunicaciones constitucionalmente reconocido, presenta aspectos sensibles con relación a la infraestructura, principalmente con el impacto visual en zonas rurales y patrimoniales en las ciudades y las zonas protegidas, siendo una materia de principal atención por esta industria.

Capítulo I

1.1 ¿Quién es el Delegado de Protección de Datos?

La Ley Orgánica de Protección de Datos Personales (LOPDP) cuenta en su estructura normativa con la concepción regulatoria y doctrinal del respeto a la protección de datos personales proveniente de la Unión Europea, encontrándose la primera referencia conocida de un delegado de protección en el Reglamento N° 45/2001 del Parlamento Europeo y del Consejo, de fecha 18 de diciembre de 2000.

Salvador Tomás (2017, Págs. 173,174), menciona que el aparecimiento del Delegado de Protección de Datos (DPD) se limitaba al tratamiento de datos personales efectuada por las instituciones y organismos comunitarios, debiendo estas entidades nombrar un responsable de protección de datos con funciones similares a las que se encuentran en la actualidad.

Una definición que engloba los roles y relaciones que tiene un DPD con el responsable o encargado del tratamiento de datos se encuentra en el *Libro Blanco de DPD* (2019), el cual lo determina como:

> El enlace entre la alta dirección y el sistema de gestión de protección de datos. A nivel de gobierno, si bien su ruta de escalado suele ser la alta dirección, debe comunicarse y coordinarse con todas las partes interesadas de las diferentes Áreas de Negocio. (Pág. 39)

Nuestra LOPDP, ha definido al DPD en su Art. 4 como:

> Persona natural encargada de informar al responsable o al encargado del tratamiento sobre sus obligaciones legales en materia de protección de datos, así como de velar o supervisar el cumplimiento normativo al respecto, y de cooperar con la Autoridad de Protección de Datos Personales, sirviendo como

punto de contacto entre esta y la entidad responsable del tratamiento de datos.

(Asamblea Nacional, 2021)

De la definición se puede deducir que solo una persona natural puede ser designada como DPD, a diferencia de la normativa europea que permite que pueda ser también una persona jurídica; adicionalmente, en la definición se detallan algunas de sus obligaciones, las cuales pueden ser divididas en las siguientes:

a) Informar y asesorar al responsable o al encargado del tratamiento sobre sus obligaciones.

b) Velar o supervisar el cumplimiento normativo.

c) Cooperar con la Autoridad de Datos Personales, sirviendo de nexo o canal de comunicación entre la autoridad y el responsable o encargado de datos.

Según el *Libro Blanco del DPD* (2019, Pág. 41), entre las obligaciones principales del DPD se encuentra la de dar a conocer a todos los miembros de la organización, la cultura de protección de datos. Dado el principio de responsabilidad proactiva y demostrada, debe demostrarse el cumplimiento de la norma a través de la evaluación y revisión de mecanismos en forma continua y constante. Esto implica que el DPD debe encontrarse en planificación sostenida de los ciclos de capacitación del personal, sobre todo de las áreas que tienen injerencia directa en el tratamiento de datos personales que la organización administra.

1.2 ¿Cuándo se encuentra obligada la organización a su nombramiento?

La LOPDP en su Art. 48 determina cuándo se debe contar obligatoriamente con la designación de un DPD, estableciendo cuatro tipos de actividades, las cuales no son taxativas, pues la Autoridad de Protección de Datos, como autoridad de la materia, puede establecer mediante normativa derivada, nuevas condiciones. A continuación, enunciamos

brevemente los casos que ameritan la designación obligatoria de un DPD conforme la norma actual:

> Art. 48.- Delegado de protección de datos personales. - Se designará un delegado de protección de datos personales en los siguientes casos:
> 1) Cuando el tratamiento se efectúa en el sector público entendido como entidades establecidas en el artículo 225 de la Constitución;
> 2) Cuando las actividades del responsable o encargado del tratamiento de datos personales requieran un control permanente y sistematizado por su volumen, naturaleza, alcance o finalidades del tratamiento, conforme se establezca en la norma o en disposiciones de la autoridad;
> 3) Cuando se refiera al tratamiento a gran escala de categorías especiales de datos, de conformidad con la norma; y,
> 4) Cuando el tratamiento no se refiera a datos relacionados con la seguridad nacional y defensa del Estado que adolezcan de reserva ni fuesen secretos, de conformidad con lo establecido en la normativa especializada. (Asamblea Nacional, 2021)

1.3 Funciones del Delegado de Protección de Datos

Las funciones del DPD se encuentran establecidas en el Art. 49 de la LOPDP, sin que el listado sea taxativo, pues tanto la Autoridad de Protección de Datos Personales como la interna de cada organización, pueden determinarse más atribuciones, por lo que la norma establece un mínimo de funciones, entre las que se encuentran las siguientes:

1) Asesorar al responsable, al personal del responsable y al encargado del tratamiento de datos personales, sobre las disposiciones contenidas en la

ley, el reglamento, las directrices, lineamientos y demás regulaciones emitidas por la Autoridad de Protección de Datos Personales.

2) Supervisar el cumplimiento de las disposiciones contenidas en la ley, el reglamento, las directrices, lineamientos y demás regulaciones emitidas por la Autoridad de Protección de Datos Personales.
3) Asesorar en el análisis de riesgo, evaluación de impacto y evaluación de medidas de seguridad, y supervisar su aplicación.
4) Cooperar con la Autoridad de Protección de Datos Personales y actuar como punto de contacto con dicha entidad, con relación a las cuestiones referentes al tratamiento de datos personales.
5) Las demás que llegase a establecer la Autoridad de Protección de Datos Personales con ocasión de las categorías especiales de datos personales. (Asamblea Nacional, 2021)

Dentro de las funciones anotadas con anterioridad, se podría incluir las determinadas en el Art. 51 de la LOPDP que corresponden al reporte y mantenimiento actualizado de la información ante la Autoridad de Protección de Datos Personales, teniendo en cuenta que, entre el DPD y la autoridad, existirá una relación de cooperación y punto de contacto, como lo ha definido la norma. Esta función incluiría la Empresa de Telecomunicaciones dentro de las funciones propias del DPD, toda vez que sería el principal contacto con la autoridad reguladora.

Aunque la LOPDP no ha determinado una obligación de reportar el nombramiento del DPD a la Autoridad de Protección de Datos Personales, no se descarta que la autoridad regule y determine aquello, teniendo en cuenta que existe un enlace entre la autoridad y el DPD como la misma definición en la norma lo ha dispuesto.

Dentro del Art. 50 de la LOPDP se establecen consideraciones especiales para el DPD, entre las cuales constan mandatos que deberán respetar tanto el responsable como el encargado de tratamiento de datos personales, tales como: garantizar en forma oportuna la participación del DPD en todas las cuestiones relativas a la protección de datos personales; facilitar su acceso a los datos personales de las operaciones de tratamiento dotándolo de recursos que sean necesarios; actualizar y capacitar respecto a la normativa técnica de protección de datos; no ser destituido por causa del cumplimiento de su cargo; mantener reporte directo con la dirección o representación más alta del responsable o encargado de datos.

El titular de los datos puede contactar al DPD con relación al tratamiento de los datos para hacer efectivo sus derechos, y mantener la más estricta confidencialidad respecto a la ejecución de sus funciones. El último inciso del Art. 50 de la LOPDP, establece un criterio adicional del perfil del DPD relacionado con la neutralidad de sus funciones para evitar el conflicto de intereses, disponiéndose que:

> Siempre que no exista conflicto con las responsabilidades establecidas (…) podrá desempeñar otras funciones dispuestas por el responsable o el encargado del tratamiento de datos personales. (Asamblea Nacional, 2021)

La disposición antes referida tiene una relación práctica con el ejercicio de sus funciones, pues el DPD no puede tener la suerte de juez y parte en la elaboración de cualquiera de las herramientas administrativas, técnicas, físicas, organizativas y jurídicas implementadas para garantizar la seguridad y protección de datos personales; ni posteriormente controlar y dar seguimiento a las herramientas implementadas o propuestas por este.

También se deberá evitar un conflicto de intereses que ocurra en la toma de las decisiones, por lo que el DPD, en caso de ser un colaborador en relación de dependencia de la organización, no deberá estar a cargo de la determinación de los fines y medios del tratamiento de datos, tampoco deberá encontrarse involucrado en dependencia con áreas directamente relacionadas en el tratamiento de datos, como por ejemplo áreas de Tecnología de la Información; sin embargo, podría ser excusado de esta responsabilidad cuando se trata de DPD externo a la organización, con una relación de prestación de servicios profesionales de naturaleza civil.

Salvador Tomás (2017) menciona que el conflicto de intereses se produce con mayor frecuencia cuando se desarrolla a medio tiempo el trabajo de DPD, pues en organizaciones de gran tamaño la dedicación a sus funciones determina que se aparte de otras que podrían conllevarle un conflicto, aclarando que:

> Sin embargo, cuando la organización es de menor dimensión, lo habitual será que el delegado realice su cometido a tiempo parcial, compaginando actividades de distinta naturaleza. Es en estos supuestos en los que es preciso evitar que se produzcan conflictos de intereses entre las distintas ocupaciones. (Pág. 181)

1.4 Características del Delegado de Protección de Datos

Actualmente, con relación al nombramiento de un DPD, se ha determinado que debe ser designado en virtud de sus características o cualidades profesionales, conocimientos especializados de la legislación y las prácticas en materia de protección de datos. Pero en Ecuador, hasta el momento, sin un reglamento a la LOPDP que especifique esta temática, se

deberá designar a un DPD entendiendo sus competencias y aspectos organizacionales que formarán parte de su perfil.

La experiencia europea ha podido determinar los atributos o características con las que debería contar el DPD, entre las cuales Salvador Tomás (2017) detalla algunas de relevancia:

a) Conocimiento legal de la normativa especializada o titulación en derecho.
b) Formación práctica en protección de datos.
c) Conocimiento del entorno empresarial privado o público al que se va a integrar el DPD. (Pág. 178)

Dentro de este aspecto, es deseable que conozca sobre las operaciones del tratamiento de datos, sistemas de información y seguridad en la protección de datos. Dentro de las habilidades de tipo personal, se encuentran las habilidades denominadas blandas, que son consideradas atributos innatos de la persona por su temperamento y carácter, tales como: comunicación y escucha activa, liderazgo, planificación y gestión del tiempo, flexibilidad, orientación a resultados y negociación.

Aun así, la mayoría de los expertos sostiene que estas pueden ser habilidades adquiridas, mejoradas o entrenadas. Carlos Ortega (2017) llega a definirlas como:

> Las habilidades blandas son un conjunto de destrezas que permiten desempeñarse mejor en las relaciones laborales y personales. Especialistas en educación coinciden en que las habilidades técnicas se pueden enseñar mucho más fácilmente que las habilidades blandas. (Pág. 7)

Estas habilidades blandas deben ser parte de las características del DPD, pues está dentro de sus funciones el trabajar con distintas áreas y personas a cargo de procesos en los cuales se efectúa tratamiento de datos personales y se establecen sus controles, demandando

información y el cumplimiento de políticas, procedimientos, manuales o instructivos de la organización.

1.5 Responsabilidades del Delegado de Protección de Datos

El Art. 49 de la LOPDP, determina una responsabilidad administrativa, civil y penal del DPD en caso de incumplimiento a sus funciones. Dentro de los tres tipos de responsabilidad, se revisará la responsabilidad que involucra al DPD.

La responsabilidad del DPD en materia civil puede vincularse en atención al sujeto, pudiendo ser responsable directo o solidario. En el caso del DPD, en principio, sería responsable directamente de sus funciones siempre que no sean compartidas con alguna persona adicional, en cuyo caso implicaría una responsabilidad solidaria.

En el caso de la responsabilidad civil atribuible al DPD, se buscará que sea condenado al pago de los daños y perjuicios que ocasione su accionar o incluso, al tratarse de un funcionario público designado como DPD en la institución pública, podrá ser condenado con la omisión de sus funciones conforme reza del Art. 52 de la Ley Orgánica de la Contraloría General del Estado. Este accionar u omisión de las funciones del DPD pueden nacer tanto del contrato, como de las funciones determinadas en la LOPDP.

En cuanto a la responsabilidad administrativa, se enmarca exclusivamente la relación pública del DPD. Es decir, cuando se enviste en la calidad de funcionario público, por lo que estará sujeto a la entidad pública, y con ello regulado por el marco disciplinario administrativo y por el marco sancionatorio determinado por la Contraloría General del Estado. Dentro de los procesos administrativos que la Contraloría pueda levantar en contra de un DPD de una institución pública, debe probarse predeterminación o responsabilidad civil culposa y tendrá como consecuencia las órdenes de reintegro correspondientes a los daños producidos.

La normativa constitucional constante en el Art. 233 determina que los funcionarios públicos no están exentos de responsabilidad por las acciones y omisiones de sus funciones siendo responsables en el ámbito civil, administrativo y penal.

Finalmente, con relación a la responsabilidad penal, el DPD responderá por los hechos dolosos que se encuentren tipificados en el Código Integral Penal, los cuales pueden ser de diversa índole. Especialmente, se toma en cuenta conductas aplicables a la interacción del DPD con la confidencialidad de la información que maneja y el actuar amplio que brinda las funciones que ostenta, tal como lo establecen los artículos 179, 180, 229, entre otros referentes a la revelación ilegal de información restringida y de base de datos, respectivamente.

En este punto, a pesar de que el DPD no se encuentra inmerso en las infracciones y sanciones de la LOPDP, su responsabilidad administrativa se debe entender como aquella que nace del vínculo con la función pública, entendiéndose aplicable el ámbito sancionador disciplinario cuando sean funcionarios públicos a cargo de responsabilidad de DPD, conforme el numeral 1 del Art. 48 de la LOPDP.

En cuanto a las excusas sancionatorias o de destitución del DPD, nuestra legislación determina en el numeral 4 del Art. 50 de la LOPDP (2021): “No podrá destituir o sancionar al delegado de protección de datos personales por el correcto desempeño de sus funciones”. Con relación a este punto, es necesario precisar que según Sierra Benítez E. (2018, Pág. 256), al referirse al caso al Reglamento 2016/679, que trata esta disposición en forma analógica a nuestra norma, puede considerarse nulo el despido que tenga como consecuencia el desempeño de sus funciones; sin embargo, esta disposición en nuestra normativa puede entrar en conflicto con la figura de despido ineficaz contenida en los artículos del 195.1 al 195.3 del Código de Trabajo, pues no se encuentra incluido dentro de sus casos, es decir, se

entiende como un despido inexistente con los efectos contemplados en la norma laboral ecuatoriana.

Aunque no se ha determinado la reforma explícita del Código de Trabajo, por el principio de jerarquía normativa determinada en el Art. 425 de la Constitución, se deberá entender que la LOPDP se encuentra en aplicación implícita del despido ineficaz dentro de las prohibiciones del empleador con relación al DPD que cumple con sus funciones.

Con relación a la vinculación laboral, exclusivamente entre el responsable o encargado del tratamiento de datos y su DPD, deberá entenderse que la prohibición de su despido por el cumplimiento de sus funciones se enmarca en el correcto desempeño de estas, por lo que el régimen disciplinario sí puede ser aplicable en casos de incumplimiento del Reglamento Interno de la organización mediante la interposición de un visto bueno.

Capítulo II

Plan de Cumplimiento del Delegado de Protección de Datos

2.1 ¿Qué es un Plan de Cumplimiento?

Si bien no se ha encontrado una definición de plan o programa de cumplimiento de protección de datos personales del DPD en la literatura especializada consultada, de acuerdo con lo que establece el *Diccionario de Real Academia de la Lengua Española*, se entiende por *plan* al "modelo sistemático de una actuación pública o privada, que se elabora anticipadamente para dirigirla o encausarla".

Por su parte, la norma ISO 9000 2015 con relación a un plan de calidad, en la sección correspondiente a fundamentos y vocabulario, lo define como: "Una especificación de los procedimientos y recursos asociados a aplicar, cuándo deben aplicarse y quién tiene que aplicarlos a un objeto específico". Así mismo, la *Guía de riesgo y evaluación de impacto en tratamiento de datos personales* (2021), al tratar sobre cómo se desarrolla la gestión del riesgo señala que:

> La gestión de riesgo está formada por un conjunto de acciones ordenadas y sistematizadas con el propósito de controlar las posibles (probabilidad) consecuencias (impactos) que una actividad puede tener sobre un conjunto de bienes o elementos (activos) que han de ser protegidos. (Pág. 12)

En tal sentido, la definición de Plan de Cumplimiento con relación a la protección de datos personales se entiende como el conjunto sistematizado de acciones, recursos y procedimientos interrelacionados con el fin de monitorear, revisar, mantener y mejorar el tratamiento de los derechos y las libertades de los titulares de datos personales, así como el cumplimiento de los principios, deberes y obligaciones previstos en el Art. 49 de la LOPDP.

Se hace hincapié en que estas acciones o procedimientos son continuos en el tratamiento de datos personales. Es decir, que no se agotan con la primera implementación, sino que se mantienen vigentes durante la vida de los datos personales que se tratan por parte de los responsables o encargados con el fin señalado. Esto es, por lo tanto, la búsqueda del mejoramiento del tratamiento de los derechos y libertades de los titulares de los datos.

2.2 Herramientas administrativas, técnicas, físicas, organizativas y jurídicas implementadas en el cumplimiento de protección de datos personales

Para el caso de las operadoras de telecomunicaciones, como lo es la empresa en estudio, una de las obligaciones establecidas en el numeral 14 del Art. 24 de la Ley Orgánica de Telecomunicaciones es: "Adoptar las medidas necesarias para la protección de los datos personales de sus usuarios y abonados, de conformidad con esta Ley, su Reglamento General y las normas técnicas y regulaciones respectivas" (Asamblea Nacional, 2015).

Así mismo, a lo largo de toda la LOPDP se hace referencia a las medidas que deben tomar tanto el responsable como el encargado del tratamiento de datos personales, con el fin de precautelar los derechos y libertades de los titulares de los datos personales que administran. De manera particular, de conformidad con el numeral 7 del Art. 47 de la LOPDP relativo a las obligaciones del responsable y encargado del tratamiento de datos personales, este expresa que el responsable está obligado a: "Tomar las medidas tecnológicas, físicas, administrativas, organizativas y jurídicas necesarias para prevenir, impedir, reducir, mitigar y controlar los riesgos y las vulneraciones identificadas" (Asamblea Nacional, 2021). En tal sentido, de acuerdo con Fernandez, M., Lerdo de Tejada M., y Murga J. Palma (2018, Pág. 111 - 120) se identifican cinco principales medidas que el responsable y encargado deben

tomar para la aplicación de la LOPDP, así: jurídicas, administrativas, organizativas, técnicas y físicas.

En cuanto a las medidas jurídicas, estas están circunscritas a la instrumentación de documentos de contenido legal, como, por ejemplo: contratos con proveedores, distribuidores o encargados; acuerdos de confidencialidad interna (empleados o colaboradores) y externa (clientes, proveedores, encargados); documentos de cesión de cartera y lo que se denomina "acuerdo de procesamiento de datos". Por su parte, las medidas administrativas van encaminadas hacia el gobierno de datos personales: elección del DPD, creación de comités de seguridad, establecimiento de roles, manejo documental, entre otros.

Las organizativas tienen por objetivo la elaboración de políticas, procedimientos o manuales, como la política de protección de datos, manejo documental, eliminación segura, uso de equipos, restricción de accesos a bases, matriz de análisis de riesgos y la de evaluación de impacto del tratamiento de datos personales. Con relación a las técnicas y físicas, estas medidas se relacionan con la seguridad de la información, a sus reportes de eventos y prevención, seguridad física de infraestructura, matrices de análisis de riesgos de seguridad de la información, principios de ciberseguridad y clasificación de datos, entre otros.

Ahora bien, actualmente la Empresa de Telecomunicaciones cuenta como parte de las medidas para la protección de datos personales con la Política de Privacidad Global, emitida por la casa matriz para sus operaciones donde el grupo empresarial tiene presencia. Esta política deviene de la aplicación del Reglamento General de Protección de Datos Personales de la Unión Europea, a la que se ve directamente sometida.

Por temas de confidencialidad, esta política no puede ser divulgada en este estudio, sin perjuicio de lo cual, tiene como objetivo macro el compromiso de respetar la privacidad de los usuarios y el secreto y seguridad de los datos personales, de conformidad con lo

establecido en la normativa de protección de datos aplicable bajo principios de transparencia, control y seguridad. Asimismo, esta política muestra, bajo la legislación por la que se rige, quién es y dónde está el responsable de la protección de datos de la matriz, indicando, además, la instauración del delegado de protección de datos.

Adicionalmente, esta política es presentada al cliente de una forma sencilla, planteando preguntas como: "¿Qué datos se tratan?", estructuradas con relación a la finalidad del tratamiento. Así se comprende dentro de las interrogantes: atención a consultas, gestión del canal de negocio; envío de boletines informativos; gestión de la relación con usuarios a través de redes sociales de la empresa matriz; gestión de datos para el análisis y valoración de la marca bajo la cual se comercializa el servicio; mantenimiento y gestión de la web de titularidad de la marca, su seguridad y acciones de los usuarios. Por cada una de estas finalidades se despliegan las preguntas con sus respectivas respuestas a: "¿Para qué?", cuyos fines están relacionados con los principios de negocio responsable; "¿por qué?", con respecto a la base legal aplicable; "¿qué datos?", sobre la tipología de datos; "¿de dónde se han obtenido?", con respecto a su procedencia; "¿a quién pertenecen?", sobre las categorías de interesados; "¿durante cuánto tiempo se tratan?", con respecto a los plazos de conservación.

Dicha Política denominada de Privacidad, habla también de las transferencias de datos a fin de ejecutar varias de las finalidades de los tratamientos, como la utilización por parte de subcontratistas autorizados en calidad de encargados, como, por ejemplo, proveedores de internet, de correo electrónico, de alojamiento de datos, etc; y, de ser el caso, la compartición de datos a empresas o entidades pertenecientes o vinculadas al grupo empresarial al que pertenece la Empresa de Telecomunicaciones. De la misma manera, la política señala los derechos y libertades que poseen los clientes como titulares de datos, y los resume de manera concreta.

Adicionalmente, también como parte de las medidas organizativas y administrativas, la Empresa de Telecomunicaciones cuenta con una herramienta para el registro general de actividades de tratamiento de datos, sus posibles brechas y el nivel de impacto y riesgos que generan. Por temas de confidencialidad, se reserva la denominación de la plataforma.

Por conocimiento directo de la Empresa de Telecomunicaciones, luego de la primera auditoría legal realizada para conocer el estado de la aplicación de la LOPDP se han encontrado algunas debilidades en las medidas de protección de datos, por ejemplo: una limitada regularización de relaciones con proveedores, destinatarios y terceros; falta de mecanismos que permitan la trazabilidad de los fines del tratamiento; ausencia de procesos actualizados que reflejen las actividades ejecutadas por la organización; dificultad en la identificación de personas responsables, entre otras.

Como consecuencia de esto, la Empresa de Telecomunicaciones ha tomado algunas decisiones iniciales desde la alta dirección para promover la protección de datos, como la generación de un proyecto completo para el efecto, estableciendo roles de los actores internos que tienen relación directa con la protección de las libertades de los titulares de los datos, incluyendo los que corresponden al DPD.

Como parte de este proyecto y como una medida organizativa importante, está la implantación de una Política local de protección de datos personales, la cual deberá seguir de manera general el formato de la Política de Privacidad Global del grupo empresarial. Esta política establece, en sus postulados, lo que para el efecto busca la legislación local. Es decir, la determinación de los principios que rigen la protección de datos, derechos de los usuarios titulares sobre los datos personales confiados a la Empresa de Telecomunicaciones, finalidades del tratamiento de los datos, obligaciones de la operadora, normativa aplicable, así como la información de los contactos en la empresa con relación al tema de privacidad.

De la entrevista con una de las personas que forman parte del área de protección de datos de la Empresa de Telecomunicaciones, ya se cuenta con un primer borrador sujeto a revisión por parte del Área Legal de la empresa.

2.3 Autorregulación y códigos de conducta

La LOPDP, en la letra k del Art. 10 relativo a los principios que rigen a la Ley, señala que, para una adecuada protección de los derechos y libertades de los titulares de datos, los responsables deberán poder acreditar la implementación de mecanismos para la protección de datos personales, para lo cual, no solo bastaría el cumplimento de lo que establece la Ley en sí misma, sino que deberá incorporar estándares, mejores prácticas, esquemas de autorregulación, códigos de protección, sistemas de certificación, sellos de protección de datos personales o cualquier otro mecanismo que se determine adecuado a los fines, la naturaleza del dato personal o el riesgo del tratamiento.

A este principio o mecanismo se lo conoce como responsabilidad proactiva o demostrada, o también como *accountability*. De acuerdo con Alejandro Alday (2019, Pág. 811) en el *Diccionario de Protección de Datos Personales*, en los conceptos fundamentales establece que "un responsable de los datos personales debe poder demostrar su cumplimiento de las medidas que habiliten el cumplimiento de los demás principios del esquema". En concordancia con esta definición, la Agencia Española de Protección de Datos Personales en su *Guía para la Gestión de Riesgo y Evaluación de Impacto en Tratamientos de Datos Personales* (2021, Pág. 20) indica que: "La gestión del riesgo no se debe reducir a la mera gestión de las consecuencias que se han producido sobre el interesado, como en el caso de que exista una brecha de datos personales. La gestión del riesgo ha de incluir el enfoque preventivo".

En tal sentido, la Empresa de Telecomunicaciones, con el fin de incluir este enfoque preventivo y demostrar el cumplimiento de la legislación de protección de datos, podrá establecer o acogerse a estándares internacionales sobre protección de datos y en especial podrá fomentar la administración de los datos personales bajo un gobierno de la privacidad.

En consecuencia, en el *Libro Blanco del DPO* Fernández, A., Mora, et al. (2019) mencionan que, en su atribución de auto regulación, la organización podrá elaborar una Política de Protección de Datos en una suerte de código de conducta interna. La misma que deberá ser aprobada por la alta dirección de la Empresa de Telecomunicaciones, donde se desplieguen los objetivos del sistema de gestión, así como los corporativos en la cual se recogerán, según el mentado *Libro Blanco del DPO*, los siguientes puntos en calidad de compromisos: Transparencia, minimización, legitimación, exactitud, inventario de actividades de procesamiento, retención, derechos de los interesados, seguridad de datos, transferencias internacionales, identificación de partes interesadas, roles y responsabilidades internas, revisiones y auditorías.

2.4 Inexistencia del Plan de Cumplimiento para el Delegado de Protección de Datos Personales

Actualmente, la Empresa de Telecomunicaciones no ha adoptado ni diseñado localmente un Plan de Cumplimiento para el DPD, cuyas directrices generales deberán ser proporcionadas por el grupo corporativo transnacional al cual pertenece formal y naturalmente con base en la legislación ecuatoriana. En tal sentido, la alta dirección de la empresa, por conocimiento directo de esta, ha demostrado tener la predisposición para el cumplimiento de la norma local, para lo cual ha destinado recursos económicos y humanos con este fin.

El incumplimiento a la normativa de protección de datos en la Empresa de Telecomunicaciones puede darse no solo por el desconocimiento interno de la empresa y de sus líneas de negocio que interactúan con el tratamiento de datos personales, sino por la ausencia del Plan de Cumplimiento del DPD instaurado a través de la Oficina de Protección de Datos de la corporación de la que forma parte la Empresa de Telecomunicaciones como parte de las políticas o medidas organizativas.

La creación del plan contribuirá para evidenciar en forma continua el control, seguimiento y reporte, así como advertir a la alta dirección el correcto cumplimiento de la legislación; o en su defecto, del incumplimiento de esta, con el correspondiente levantamiento de las oportunidades de mejora y la evaluación del impacto del tratamiento de datos. Adicionalmente, el cumplimiento de la norma a través de la ejecución del plan del DPD, evitará las sanciones a la organización y la complementaria responsabilidad civil, administrativa y penal del DPD.

El DPD requiere de una guía o plan para el cumplimiento de sus funciones y obligaciones que se determinan actualmente en la LOPDP y posteriormente en su respectivo Reglamento o política interna de protección de datos personales.

Este plan adquiere vital importancia en la vigilancia y cumplimiento normativo, porque su ejecución demostrará a la alta dirección de la empresa y a la autoridad competente de datos personales, el sometimiento de la compañía a la LOPDP y normativa derivada, evitando así la imposición de multas y sanciones tanto a la empresa como al mismo DPD por el ejercicio de sus funciones y obligaciones.

El adecuamiento a la norma y el seguimiento que debe realizar el DPD, tomando como base el Plan de Cumplimiento para la Empresa de Telecomunicaciones, tiene como objetivo generar valor agregado a la compañía frente a sus *stakeholders* (terceros

interesados), demostrando transparencia en el tratamiento de datos personales en sus actividades empresariales e incrementando su valor reputacional. Asimismo, por experiencia en el sector de telecomunicaciones, la compañía disminuirá el riesgo existente en el tratamiento de datos personales dado el volumen y sensibilidad de los datos que administra por motivo de la operación, y por la cantidad de abonados de los servicios que presta a través del contrato de concesión otorgado por el Estado.

Capítulo III

Diseño del Plan de Cumplimiento del Delegado de Protección de Datos Personales

3.1 Perfil del Delegado de Protección de Datos Personales en una Empresa de Telecomunicaciones

El perfil del DPD no se encuentra determinado en la LOPDP; por consiguiente, podría incluirse en el reglamento a la Ley. Tampoco se ha determinado ningún organismo para acreditación de un DPD; sin embargo, es algo que en un futuro podría llegar a concretarse a través de las disposiciones que regula la autoridad de control de datos.

En este punto, Salvador Tomás (2018, Pág. 179) menciona que, con la finalidad de proporcionar seguridad en la formación de estos especialistas, hay un esquema de certificación para DPD en la Agencia Española de Protección de Datos en el cual se evalúan las competencias, aplicando los criterios de la norma internacional ISO/IEC 17024:2012. La Entidad Nacional de Acreditación -ENAC- puede acreditar a Entidades de Certificación que refrenden que los DPD reúnen una capacidad profesional y de conocimientos. Aunque la acreditación no es obligatoria para ejercer el cargo, es una buena idea en busca de preparar a los profesionales que se encargarán de esta función.

La obligatoriedad de las empresas o entidades que deben contar con un DPD según el Art. 48 de la LOPDP, conlleva realizar una valoración interna de cada organización, para lo cual será indispensable incluir en ella la evaluación de riesgo en el tratamiento de datos.

Es de tener en cuenta que, conforme lo dispone el último inciso del Art. 48 de la norma referida, la Autoridad de Protección de Datos Personales, conforme a la emisión del reglamento a la Ley o de resoluciones, podría definir nuevas condiciones en las que deba designarse un DPD.

En el caso de la Empresa de Telecomunicaciones, esta se encuentra sin duda obligada a designar un DPD, ya que dependiendo de la oferta de sus servicios, sea como responsable o encargado del tratamiento de datos, maneja una gran cantidad de datos personales de sus clientes, por lo que requiere de un control permanente y sistematizado. Asimismo, la empresa mantiene una amplia cantidad de detalle de información de cada cliente, lo que puede conllevar un riesgo de afectación a los derechos y libertades del titular de los datos.

Con la finalidad de determinar el perfil con que debe contar el DPD en la Empresa de Telecomunicaciones, este es sometido a análisis desde dos aspectos:

a) Determinación del perfil del DPD por el tipo de organización o modelos organizacionales.
b) Determinación del perfil del DPD por las cualidades propias o intrínsecas que debe tener el DPD.

Para el primer punto, el Modelo Organizativo y Relacional determinado por el *Libro Blanco del DPD* (2019, Pág. 16) es de gran impacto para delinear el cumplimiento de sus funciones en forma adecuada. Ante ello, y dada la especialidad de los servicios que brinda la Empresa de Telecomunicaciones en el Ecuador, es necesario que el DPD conozca de las líneas de negocio, aspectos técnicos además de los legales de la empresa y de la normativa ligada a la regulación de las telecomunicaciones. Por lo mencionado, es importante que el DPD en la Empresa de Telecomunicaciones sea interno, con conocimiento y formación legal de las líneas de negocio.

La Empresa de Telecomunicaciones no forma parte de un grupo societario, empresarial o *holding* que involucre tener varios DPD o entrar en el análisis de la necesidad de contar con un DPD por el grupo societario o empresarial, por lo que se debe contar con una sola delegación por la empresa. En cuanto a la compatibilidad de su cargo, en capítulos

anteriores se ha enunciado la normativa ecuatoriana que prevé que el DPD puede realizar otras funciones, siempre que no entre en conflicto con sus responsabilidades o conflicto de interés, como lo menciona el *Libro Blanco del DPO* (2019):

> Aunque los DPD pueden tener otras funciones, solamente se les podrá confiar otras tareas y cometidos si estas no dan lugar a conflictos de intereses. Esto supone, en especial, que el DPD no puede ocupar un cargo en la organización que le lleve a determinar los fines y medios del tratamiento de datos personales. (Pág. 14)

La Empresa de Telecomunicaciones, en función de la cantidad o volumen de datos utilizados en el tratamiento y en atención a los distintos servicios de carácter masivos que presta, requiere de un DPD que dedique todo su esfuerzo y tiempo a cumplir con sus funciones determinadas por la ley y por la organización, los mismos que tendrán relación estrictamente a su cargo.

En lo que respecta al conocimiento de orden técnico, el DPD en la empresa en análisis debe conocer no solamente de aspectos tecnológicos que utiliza e involucra el accionar de la Empresa de Telecomunicaciones en la prestación de sus servicios, sino también de seguridad de la información o ciberseguridad.

Aunque muchas empresas determinan que la designación del DPD debe ser parte de las funciones complementarias del personal responsable de velar por la ciberseguridad de una empresa CISO (*Chief Information Security Officer*), como lo menciona el *Libro Blanco del Delegado de Protección de Datos* (2019, Pág. 21), en el presente caso, al ser una empresa de tecnología enfocada en telecomunicaciones, cuenta con áreas propias y especializadas para el control tecnológico, de seguridad y prevención de fraudes, por lo que las funciones

del DPD serán propias sin tener que compartir funciones con las áreas de tecnología y seguridad.

Es sugerible que exista una separación entre el responsable de seguridad y el DPD, según lo ha mencionado la Agencia Española de Protección de Datos Personales, determinando que siempre se realice un análisis de caso por caso, al tratarse de organizaciones que por su tamaño y recursos no pudiesen contar con un DPD a tiempo completo.

Adicionalmente, en la Empresa de Telecomunicaciones, aunque el componente tecnológico y el tratamiento de los datos es principalmente digital y se hace mediante bases de datos y ficheros, existen amenazas de ciberseguridad. Sin embargo, el principal riesgo a la vulneración de los derechos de los titulares de los datos se encuentra en los procesos de consentimiento informado, en el sistema de confidencialidad del personal y la delegación de responsabilidad contractual con proveedores estratégicos. Por lo tanto, los servicios que ejecutan los encargados del tratamiento de datos, lo que implica que el DPD no debería tener conocimientos técnicos intrínsecos ni ser un CISO en la Empresa de Telecomunicaciones.

Otro modelo organizativo posible es el de confluir las funciones del DPD con el denominado Oficial de Cumplimiento Normativo. Sin perjuicio de esto, la Empresa de Telecomunicaciones, pese a contar con un puesto determinado para el control del cumplimiento legal por instrucciones de la organización internacional a la cual se debe, recalca la cantidad importante de responsabilidades que tendrá el DPD, y se determina que su cargo no involucre otras actividades ajenas que lo distraigan de sus funciones. Sin embargo, por directo conocimiento de la Empresa de Telecomunicaciones, en la organización, desde la matriz, confluyen la Oficina de Cumplimiento con la de Protección

de Datos personales, por lo que se ha trasladado esta forma de organización a la empresa ecuatoriana.

El *Libro Blanco del DPD*, dentro de la medida organizativa posible, determina la posibilidad de que el DPD provenga del área jurídica, siendo otro modelo la creación de un área independiente de protección de datos, por lo que la Empresa de Telecomunicaciones deberá idealmente escoger el perfil del DPD dentro del ámbito legal, pero llegando a ser independiente de dicha área.

Es indudable la experticia legal que debe tener el DPD por el conocimiento especializado en la protección de los derechos y libertades del titular de datos, que servirá para enfocar el ejercicio de sus funciones de una manera eficiente. Más aún cuando los aspectos regulatorios del sector de las telecomunicaciones requieren que el DPD de la organización tenga la habilidad de conocer la norma y aplicarla en forma proactiva.

En este punto, la Empresa de Telecomunicaciones no caerá en el riesgo de conflicto de intereses, pues el DPD no reportará a la Gerencia Legal, sino directamente al Comité Ejecutivo de la compañía como órgano colegiado máximo de la empresa, sin que ejerza el DPD funciones de abogado, representante o patrocinador de causas con contenido legal que se presenten contra la empresa como responsable o encargado de protección de datos. Así también, tendrá reporte con el DPO Corporativo de la organización multinacional. Finalmente, aunque la carencia de conocimientos técnicos podría ser una limitación del DPD, esta puede ser suplida con la inclusión en los comités de seguridad de la empresa y una capacitación interna de las áreas tecnológicas y de seguridad de la información.

Dentro de este primer análisis del perfil del DPD, se sintetiza que para la Empresa de Telecomunicaciones se requerirá que sea: un delegado único de la organización, empleado interno de la compañía, que cuente con funciones compartidas con otros cargos como el área

de cumplimiento normativo, proveniente del área legal pero independiente, con un cargo de reporte directo a la alta dirección.

En cuanto a la determinación del perfil del DPD por las cualidades propias o intrínsecas que debe tener el DPD, dentro de esta categoría se encuentran algunos atributos referidos en el *Libro Blanco del DPD* (2019, Pág. 50) que es importante tener en cuenta en el establecimiento del perfil del DPD para la Empresa de Telecomunicaciones:

- Cualificación: Dentro de las cualidades profesionales, el DPD debe atender a su formación, por lo que deberá incorporar conocimientos especializados del Derecho del sector de telecomunicaciones y del negocio de la organización.
- Experiencia profesional: Dada la novedad de la LOPDP, solicitar experiencia profesional como DPD en Ecuador sería una exigencia ineficaz. Sin embargo, será un requisito indispensable dentro de al menos los dos años posteriores al 26 de mayo del 2023, fecha en la que la moratoria de la aplicación del ámbito sancionatorio de la norma finalizará.

Adicionalmente, la experiencia profesional deberá incluir el conocimiento de la norma de telecomunicaciones ecuatoriana, protección de datos, tecnología de la información y comunicación, procesos informáticos, sistemas de organización, identificación de riesgos y su evaluación, gestión de procesos, sistemas de gestión y procedimientos de auditoría de procesos.

El DPD debe tener habilidades blandas, e incorporar en estas habilidades personales a la ética profesional, sin que se cuente con referencias de sanciones que hayan involucrado actos contrarios a las prácticas empresariales honestas, ni haber mantenido sanciones relacionadas con el deber de secreto.

3.2 Actividades del Delegado de Protección de Datos Personales en la Empresa de Telecomunicaciones

El Art. 51 de la LOPDP, determina la obligatoriedad de remitir a la autoridad de datos correspondiente un registro de tratamiento de datos, junto con otra información propia de la organización con relación al tratamiento que realiza. La normativa referida, además, dispone reportar y mantener actualizada la información.

El registro de tratamiento de datos tiene por finalidad que la autoridad competente conozca la gestión de los riesgos, que puede representar para los derechos y libertades del titular de datos, el tratamiento que se haga de sus datos y la mitigación que se haya gestionado, con la finalidad de controlar los riesgos asociados. Para ello, es necesario analizar y detallar el tipo de tratamiento, la naturaleza, finalidad, identificar a los destinatarios, el modo de interrelacionar la información, el cumplimiento de principios, derechos y obligaciones, las herramientas empleadas para garantizar la seguridad y protección de datos y el tiempo de conservación.

Dentro de las funciones y actividades del DPD en la Empresa de Telecomunicaciones, tiene especial relevancia la gestión de riesgo, análisis, amenazas y vulnerabilidades; así también, la evaluación de impacto del tratamiento de datos personales y demás actividades específicas.

3.2.1 Gestión del Riesgo, Análisis, Amenazas y Vulnerabilidades

El riesgo es definido por la guía ISO 31000, enfocada en la gestión de riesgos, como: "El efecto de la incertidumbre sobre la consecución de objetivos". Ese efecto puede ser cualquier cambio sobre lo que se haya previsto en un comienzo.

La Agencia Española de Protección de Datos (AEPD), al inicio de su herramienta EVALÚA_RIESGO RGPD v1, que fue creada con el propósito de ayudar a los responsables y encargados a identificar los factores de riesgo para los derechos y libertades de los titulares de datos, menciona la importancia de una evaluación de riesgo, determinando que:

> Tiene como objeto identificar los factores de riesgo para los derechos y libertades de los interesados o titulares de datos personales, cuyos datos están presentes en el tratamiento, hacer una primera evaluación del riesgo intrínseco y estimar el riesgo residual si se utilizan medidas y garantías para mitigar los factores de riesgos específicos. (AEPD, 2021)

Para los responsables y encargados del tratamiento de datos es necesario efectuar una gestión del riesgo que parte con la evaluación interna, encaminada a identificar factores de riesgo principales, mínimos y específicos del tratamiento que se efectúa. El propósito coadyuvante de la gestión de riesgo es tomar las decisiones que se deben materializar en hechos concretos, los cuales permiten controlar los posibles impactos que una actividad de tratamiento de datos puede producir en los derechos y libertades de los titulares conforme lo determinado en la Constitución Política y en la LOPDP. Los impactos deben ser minimizados aun cuando el riesgo no se pueda disipar y permanezca un riesgo residual o remanente.

La gestión del riesgo es algo continuo que permanece en la organización y debe ser actualizado cada vez que subsista un nuevo riesgo, cuando las medidas de mitigación no hayan sido efectivas o cuando existan proyectos nuevos que entrañen tratamiento de datos, por lo que deberán ser evaluados previamente.

La valoración del nivel de riesgo para cada factor y el cálculo final de nivel de riesgo debe ser realizada a medida de cada organización, siendo perfectible con el tiempo a través de la continua revisión de la misma, conforme la dinámica en la Empresa de

Telecomunicaciones y en la tecnología implementada. En el presente caso de estudio, la Empresa de Telecomunicaciones deberá valorar en cada nuevo proyecto el dinamismo que trae su sector a través de la distribución masiva de sus canales de venta.

La Agencia Española de Protección de Datos, en *Gestión del Riesgo y Evaluación de Impacto en Tratamiento de Datos Personales* (2021), al referirse a la importancia de identificar el tipo de tratamiento de datos que efectúa una organización, menciona lo siguiente:

> Analizar supone examinar detalladamente, separando y considerando de forma independiente cada una de sus partes, para conocer sus características, cualidades, restricciones y limitaciones, y así poder extraer conclusiones. (Pág. 30)

El Art. 40 de la LOPDP, dispone que se realice un análisis de riesgos, amenazas y vulnerabilidades, para lo cual debe utilizar una metodología que considere, entre otros aspectos, los siguientes:

1) Las particularidades del tratamiento.

2) Las particularidades de las partes involucradas.

3) Las categorías y el volumen de datos personales objeto de tratamiento.

Como se ha mencionado con anterioridad, el numeral tercero del Art. 39 de la antedicha norma establece como funciones del DPD el asesorar en el análisis de riesgo, evaluación de impacto y evaluación de medidas de seguridad, y supervisar su aplicación; por lo que su conocimiento y experiencia serán en este punto de mucha importancia para el responsable o encargado del tratamiento de datos.

La gestión del riesgo, amenazas y vulnerabilidades en el tratamiento de datos de una organización podría enfocarse en tres actividades que se resumen en el proceso, los cuales según la Agencia Española de Protección de Datos AEPD (2021) son:

- Identificar los factores de riesgos o amenazas para los derechos y habilidades.
- Analizar los mismos en su impacto y probabilidad, para poder llevar a cabo la evaluación del nivel del riesgo inherente que se deriva de cada uno de los factores de riesgo.
- Evaluar el nivel global del tratamiento para los derechos y libertades del tratamiento. (Pág, 32)

Las medidas para mitigar el riesgo, amenazas y vulnerabilidades en el tratamiento de datos se encuentran enunciadas también en las obligaciones del responsable y encargado del tratamiento de datos, que de conformidad con el numeral 7 del Art. 47 de la LOPDP se plasman en algunas categorías:

> 7) Tomar medidas tecnológicas, físicas, administrativas, organizativas y jurídicas necesarias para prevenir, impedir, reducir, mitigar y controlar los riesgos y las vulneraciones identificadas.

El proceso de evaluación del riesgo significa tener, al final del resultado, un nivel de riesgo asociado al tratamiento de datos del responsable o encargado, lo cual servirá para determinar la obligatoriedad o no de realizar la evaluación de impacto en el tratamiento de datos, de conformidad con lo dispuesto en el Art. 42 de la LOPDP, siendo obligatorio cuando el riesgo global o final es alto o cuando la autoridad así lo requiera.

Así también, es destacable la aclaración que se efectúa en el último inciso de la norma antes referida, determinando que tanto el responsable como el encargado del tratamiento de datos personales deberán tomar las medidas adecuadas y necesarias, de forma permanente y

continua, para evaluar, prevenir, impedir, reducir, mitigar y controlar los riesgos, amenazas y vulnerabilidades, incluidas las que conlleven un alto riesgo para los derechos y libertades del titular, de conformidad con la normativa que emita la Autoridad de Protección de Datos Personales. En la disposición anotada se vuelve a incluir la aplicación de medidas de mitigación en función del alto riesgo que implica a los derechos y libertades del titular.

En el caso de la Empresa de Telecomunicaciones, por el tipo de tratamiento de datos, perfilamiento y volumen de los mismos, luego de haber efectuado el análisis de la matriz de riesgo, teniendo como herramienta a EVALÚA_RIESGO RGPD v1, elaborada para uso público por La Agencia Española de Protección de Datos (AEPD), se ha determinado que la probabilidad del tratamiento global que realiza para la prestación de los servicios de telecomunicaciones y de soporte informático, por su naturaleza, contexto o fines, es un alto riesgo para los derechos y libertades del titular. Como Anexo 1 se encuentran los aspectos sometidos a la matriz de evaluación del riesgo que se ha efectuado.

3.2.2 Evaluación de Impacto del Tratamiento de Datos Personales

La LOPDP no ha definido en forma explícita lo que significa la Evaluación de Impacto del Tratamiento de Datos Personales (conocido en Europa como Evaluación de Impacto de Protección de Datos – EIPD); sin embargo, el Comité Europeo de Protección de Datos (CEPD) (2017) estableció un concepto, el cual se encuentra en las Directrices WP248 rev.01, mencionando:

> Una EIPD es un proceso concebido para describir el tratamiento, evaluar su necesidad y proporcionalidad y ayudar a gestionar los riesgos para los derechos y libertades de las personas físicas derivados del tratamiento de datos personales, evaluándolos y determinando las medidas para abordarlos. Las

> EIPD son instrumentos importantes para la rendición de cuentas, ya que ayudan a los responsables no solo a cumplir los requisitos del RGPD, sino también a demostrar que se han tomado medidas adecuadas para garantizar el cumplimiento del Reglamento (…) En otras palabras, una EIPD es un proceso utilizado para reforzar y demostrar el cumplimiento. (Pág. 4)

La AEPD (2021, Pág. 25-28), ha determinado una serie de características de la EIPD, mismas que ayudan a comprender el alcance de este proceso y que, parafraseando, se tratan a continuación:

1. No es un proceso aislado ni puntual, es un sistema continuo mientras dura el tratamiento de los datos, que sirve para demostrar el cumplimiento de la normativa y el respeto a los derechos y libertades de los titulares de los datos.
2. Debe tener documentos que reflejen el cumplimiento, en forma similar a cualquier auditoría de seguimiento de procesos de gestión integrada, evidenciándose la conformidad con la norma.
3. Se evalúa el riesgo, es decir, los niveles o dimensión de este, pero al mismo tiempo se acompaña de los mecanismos para mitigarlo, por lo que se integran ambos aspectos en la gestión del riesgo. En este punto, la AEPD (2021) menciona específicamente que:

   > La EIPD obliga al responsable a actuar y tiene una dimensión mayor que un mero formalismo plasmado en un documento sobre el que se pueden realizar cambios mínimos para adaptarlo a cualquier tratamiento. (Pág. 25)

4. Es exigible un EIPD cuando el riesgo en el tratamiento global de una organización es alto.
5. Es una obligación del responsable de datos, aplicable conforme el Art. 42 LOPDP.

6. Se debe analizar la necesidad y la proporción del tratamiento, así como sus fines.
7. Se debe realizar antes del inicio de las actividades del tratamiento.
8. El DPD asesora en la creación del EIDP, esto guarda relación con el numeral 3 del Art. 49 de la LOPDP.
9. Implica recabar la opinión de las partes interesadas de la organización, siendo importante para determinar los riesgos y medidas de mitigación.
10. Se toma en cuenta la existencia de códigos de conducta. En el caso de corporaciones o empresas multinacionales, como la Empresa de Telecomunicaciones del presente estudio, su norma corporativa de conducta y política de respeto al tratamiento de datos deberá ser adecuada al Ecuador.
11. Tener en cuenta las certificaciones que pueda obtener la organización, pues aquello demanda la existencia de una proactividad y orden en el manejo de la gestión integrada del riesgo.
12. La herramienta puede servir para establecer la viabilidad o inviabilidad del tratamiento o modificar el tratamiento en ciertos alcances. De allí la necesidad de analizar cada nuevo proyecto sobre la base del proceso de una EIPD.

Como se ha determinado con anterioridad, con relación a la evaluación de impacto del tratamiento de datos personales, el Art. 42 de la LOPDP ha determinado que es una obligación del responsable cuando el riesgo del tratamiento de datos es alto con relación a los derechos y libertades del titular o cuando la Autoridad de Protección de Datos Personales así lo determine o lo requiera.

Sin embargo, la norma referida llega a enumerar circunstancias en las cuales es obligatorio efectuar el EIPD, siendo las siguientes:

a) 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;
b) Tratamiento a gran escala de las categorías especiales de datos, o de los datos personales relativos a condenas e infracciones penales.
c) 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. La evaluación de impacto deberá efectuarse previo al inicio del tratamiento de datos personales. (Asamblea Nacional, 2021)

Finalmente, es relevante destacar que el EIDP es también una herramienta para evidenciar el cumplimiento de sujeción a la norma de protección de datos personales, pues en dichos procesos se materializa el seguimiento, control y adecuación de todas las medidas que el responsable o encargado del tratamiento de datos deben tomar para mitigar el riesgo del tratamiento. Estas medidas, como lo menciona el Art. 41 de la LOPDP y en relación con el último inciso del Art. 37, deben ser:

> …adecuadas y necesarias, de forma permanente y continua, para evaluar, prevenir, impedir, reducir, mitigar y controlar los riesgos, amenazas y vulnerabilidades, incluidas las que conlleven un alto riesgo para los derechos y libertades del titular, de conformidad con la normativa que emita la Autoridad de Protección de Datos Personales. (Asamblea Nacional, 2021)

En el caso de la Empresa de Telecomunicaciones, habiéndose determinado qué servicios de telecomunicaciones y de soporte informático tienen un alto riesgo para los

derechos y libertades del titular, en atención a lo dispuesto por la LOPDP, es necesario que cuente con una evaluación global de impacto al tratamiento de datos personales, independientemente de que en nuevos proyectos se deba incluir un proceso específico de EIPD.

Con miras a materializar el proceso de elaboración de un EIPD, en un documento que demuestre la trazabilidad, el levantamiento de riesgos y medidas de mitigación, que contribuya a evidenciar el cumplimiento de la normativa y el respeto a los derechos y libertades de los titulares de los datos, se ha creado la matriz de "EVALUACIÓN DE IMPACTO AL TRATAMIENTO DE DATOS PERSONALES", cuyo modelo referencial consta como Anexo 2 de la presente investigación.

3.2.3. Actividades específicas del Delegado de Protección de Datos Personales en la Empresa de Telecomunicaciones

Cabe mencionar que, en este apartado, la fuente de información proviene directamente de las entrevistas mantenidas con los funcionarios responsables de protección de datos personales de la Empresa de Telecomunicaciones. En tal sentido, teniendo en cuenta el entorno interno y externo de la Empresa de Telecomunicaciones, así como el perfil del DPD aplicable a la compañía, como actividades específicas del DPD adicionales a las determinadas de conformidad con la LOPDP, se encuentran las siguientes:

- Identificar las responsabilidades legales y éticas de la Empresa, dentro de las funciones del oficial de cumplimiento o *Compliance Officer* que forman parte del cargo que comparte adicionalmente funciones de DPD.
- Integrar y dirigir el Comité de Gestión de Datos Personales cuyas actividades, entre otras, son: la creación del sistema de gestión de protección de datos personales

(estructura, seguimiento y controles); el levantamiento del procedimiento para el desarrollo del registro de actividades de tratamiento, su actualización y su respectivo monitoreo; la definición de directrices, políticas y procesos del sistema de gestión de protección de datos personales (roles, responsabilidades por áreas, registro de actividades de tratamiento, gestión de riesgos, evaluación de impacto medidas de control, medidas de seguimiento); la identificación de áreas de riesgo; el diseño del programa de sensibilización, concienciación y formación permanente; la diferenciación en la estructura interna de la Empresa de Telecomunicaciones, la independencia de la oficina de DPD y Compliance; y la elaboración de guías orientadas a trabajadores, según sus roles específicos.

- Integrar el Comité de Seguridad de la Información, a través del cual el DPD realizará las siguientes actividades: a) Seguimiento de los cambios significativos de los riesgos que afectan a los recursos de información frente a las amenazas más importantes; b) Tomar conocimiento y supervisar la investigación y monitoreo de los incidentes relativos a la seguridad de la información, con nivel de impacto alto; c) Coordinar la implementación de controles específicos de seguridad de la información para nuevos sistemas o servicios; entre otros.
- Formar parte integrante del comité denominado “Gobierno del Dato”, el cual está conformado por representantes de las áreas que mayor impacto tienen en el tratamiento de datos de la organización, teniendo en cuenta que en sus funciones están el monitorear y garantizar la correcta utilización de los datos, cumpliendo con el principio de finalidad de los datos, así como monitorear y aplicar medidas de mitigación sobre la gestión de los activos de datos.

- Al ser la Empresa de Telecomunicaciones una corporación multinacional con divisiones internacionales por regiones de Sudamérica, existe la oficina de DPD en la matriz de la corporación, que determina lineamientos propios de esta, existiendo reportes del DPD de la Empresa de Telecomunicaciones a la oficina corporativa como queda anotado.
- Finalmente, la Empresa de Telecomunicaciones cuenta con una instancia organizacional de la más alta jerarquía, denominada "Comité Ejecutivo", la cual es un organismo colegiado, integrado por cada uno de los más altos directores de todas las áreas de la empresa. Este comité es presidido por su Presidente Ejecutivo, bajo cuyo cargo se ejerce la representación legal de la compañía. En tal sentido, el DPD efectuará un reporte directo de su gestión en forma constante al Comité Ejecutivo de la Empresa de Telecomunicaciones, en cumplimiento con el numeral 5 del Art. 50 de la LOPDP.

3.3 Estructuración del Plan de Cumplimiento

Dentro del Plan de Cumplimiento del DPD se deben tener en cuenta dos tipos macro de actividades:

a) Preventivas: Las que corresponden a un seguimiento continuo o permanente del cumplimiento normativo; y, verificación de las medidas de mitigación del riesgo levantado dentro de la evaluación del impacto del tratamiento de datos global o específico de la Empresa de Telecomunicaciones al tratarse de proyectos individuales, lo que conlleva a evitar la materialización de vulneraciones a los derechos y libertades de los titulares de datos personales. Dentro de las actividades

preventivas que tiene la Empresa de Telecomunicaciones, se pueden enumerar las siguientes:

- Documentar y formalizar la estructura de gestión de datos, políticas, roles y responsabilidades.
- Acompañar y capacitar al equipo de protección de datos personales a lo largo de la implementación.
- Definir estándares de protección de datos personales en el ciclo de vida del dato.
- Definir el procedimiento para la anonimización y borrado seguro de los datos personales.
- Incluir avisos de protección de datos personales y repositorios que permitan recopilar el consentimiento informado de los titulares de los datos.
- Diseñar e implementar canales informativos, de comunicación y consulta de los titulares de los datos personales para que estos los conozcan y puedan ejercer sus derechos y libertades.
- Realizar campañas de concienciación y formación del personal implicado en las operaciones de tratamiento de datos personales y en la definición o concepción de nuevos tratamientos.
- Implementación de planes de auditorías internas o externas que evalúen el cumplimento de las políticas de protección de datos.
- Diseñar e implementar un procedimiento de notificación de violaciones de protección de datos personales para la Superintendencia de Protección de Datos y/o para los clientes en caso de vulneraciones.

- Diseñar e implementar un instructivo que los encargados de tratamiento deben cumplir para notificar a la organización de los eventos, incidentes, vulnerabilidades y violaciones de protección de datos personales.
- Diseñar y elaborar un procedimiento para la notificación de riesgos, amenazas, vulnerabilidades y violaciones de datos personales.

b) Correctivas: Referentes a la coordinación e implementación de nuevas medidas de mitigación de riesgos que devienen de observaciones realizadas en el proceso de seguimiento. También se relaciona con el levantamiento de oportunidades de mejora de la vigilancia efectuada, conforme las actividades del literal precedente o, en su defecto, por no haber incorporado riesgos en el tratamiento de datos en cualquiera de sus ámbitos y no haber determinado las medidas adecuadas y suficientes para mitigar los riesgos. Dentro de las actividades correctivas, enunciamos algunas que se adaptan a la Empresa de Telecomunicaciones:

- Implementación de *web services* con los aplicativos para la recopilación del consentimiento.
- Generar roles de acceso y actualizar convenios de confidencialidad en concordancia con la LOPDP.
- Modificación del proceso de calificación de proveedores que tratan datos personales directa o indirectamente para clasificarlos y adecuar sus obligaciones y responsabilidades como encargados dentro de los contratos y documentos que obligatoriamente suscriben.
- Reformas a los modelos contractuales de los contratos con proveedores para incluir cláusulas con validez jurídica aplicables en las relaciones responsable-encargado.

3.4 Esquema de ejecución y seguimiento del Plan de Cumplimiento

Dentro de las macro actividades tanto preventivas como correctivas que se estructuran en el Plan de Cumplimiento del DPD de la Empresa de Telecomunicaciones, se debe contemplar un cronograma que atienda a dos tipos de necesidades:

a) El seguimiento de actividades globales de control, levantadas en el estudio de impacto en tratamiento de datos y sus medidas de mitigación de carácter preventivo.
b) Un cronograma de actividades cuando se realicen acciones de índole correctiva que devienen de un control del DPD y que deriven en el registro de nuevos riesgos en el tratamiento de datos y el levantamiento de nuevas medidas de mitigación.

Todo ello dentro de un proceso continuo de seguimiento y control por parte del DPD que permitirá, en unos casos, eliminar el riesgo inherente y, en otros, mitigarlo. Esto, teniendo en consideración que existirán riesgos residuales o latentes que no dejarán de existir, por la propia naturaleza del dato en la Empresa de Telecomunicaciones.

A continuación, se presenta la estructura que ejecutará el DPD en cumplimiento de sus obligaciones y funciones en la Empresa de Telecomunicaciones.

Fase preventiva

a) Realizar el seguimiento para verificar la correcta implementación y cumplimiento de las medidas de mitigación establecidas en la Empresa de Telecomunicaciones.
b) Evaluar, luego de implementada la medida de mitigación, si esta fue eficiente y efectiva; es decir, si se han cumplido los fines para los cuales fue establecida.
c) Establecer oportunidades de mejora; esto es, identificar si las medidas de seguridad de información requieren ser actualizadas y optimizadas.

d) Incorporar las mejores prácticas de la corporación a la cual pertenece la Empresa de Telecomunicaciones, permitiendo fortalecer las medidas de seguridad adoptadas.
e) Actualizar el sistema de gestión integrado, políticas, manuales e instructivos ligados al tratamiento de datos personales.

Fase correctiva

a) Seleccionar las medidas de mitigación y seguridad tecnológicas, físicas, administrativas, organizativas y jurídicas, para el tratamiento de riesgos y cierres de posibles brechas o inconformidades con la LOPDP;
b) Analizar las medidas seleccionadas, límites técnicos, compatibilidad y riesgo residual.
c) Establecer las actividades requeridas para la implementación de las medidas de mitigación seleccionadas.
d) Definir al personal que será responsable de la implementación.
e) Determinar los tiempos necesarios para la implementación de las medidas.

Esta estructura del Plan de Cumplimiento debe tener un cronograma de ejecución anual, para lo cual el DPD deberá levantar un informe de cumplimiento dirigido al comité ejecutivo con el fin de dar a conocer a este cuerpo colegiado, las actividades de implementación de medidas y seguimiento de estas bajo la LOPDP. Un esquema de esta estructura se adjunta como Anexo 3 del presente estudio. Asimismo, se adjunta como Anexo 4 la propuesta del Plan de Cumplimiento para el Delegado de Protección de Datos Personales.

CONCLUSIONES Y RECOMENDACIONES

Conclusiones

A modo de conclusión, se ha visto la necesidad de construir la definición del Plan de Cumplimiento para el DPD, a falta de una en la literatura especializada, para lo cual se ha tomado como base varios conceptos sobre planes, cumplimento y riesgos relativos a la protección de datos personales, vinculados a las obligaciones, funciones, características y responsabilidades del DPD.

Sustentado en la definición de Plan de Cumplimiento para el DPD elaborada en este estudio, se desprende que la Empresa de Telecomunicaciones tiene dos tipos de macro actividades: una preventiva y una correctiva, tomando en cuenta que la primera forma parte de la implementación que se encuentra vigente a partir de la publicación de la LOPDP; y la segunda macro actividad corresponde a las acciones y procedimientos continuos que no se agotan con la primera implementación, sino que, por la dinámica de los datos, obligan a un seguimiento sostenido en el tiempo.

Por otra parte, teniendo en cuenta la actividad que realiza la Empresa de Telecomunicaciones, el volumen de datos personales que trata, así como la naturaleza propia de estos y sus fines, se ha determinado que el riesgo de vulnerabilidad de los derechos y libertades de los datos personales que trata es alto; por consiguiente, el DPD deberá contribuir a la definición de directrices, políticas y procesos del sistema de gestión de protección de datos personales, así como precisar las actividades de las áreas involucradas, sus responsabilidades, el registro de actividades de tratamiento, la evaluación de impacto del tratamiento de datos personales, la gestión de riesgos, las medidas de control y de seguimiento, entre otros. En forma complementaria, la Empresa de Telecomunicaciones, como responsable del tratamiento de datos, deberá implementar como parte del Sistema de

Gestión de Protección de Datos Personales, sin que la enumeración sea exhaustiva: la identificación de áreas de riesgo (Atención al cliente, Negocios, Inteligencia de Negocio, *Business to Client, Business to Business*, etc.); la determinación de perfiles de puesto con asignación de nuevas funciones; el diseño del programa de sensibilización, concienciación y formación permanente para empleados y proveedores; la creación en la estructura interna de la independencia de la oficina de DPO y *Compliance*; la elaboración de las guías orientadas a trabajadores, según sus roles específicos; y la inclusión en las distintas políticas de mecanismos de recopilación de lecciones aprendidas respecto de la revisión y auditorías implementadas.

Con todas estas determinaciones expuestas, se desprende que es indispensable la elaboración de un Plan de Cumplimiento para el DPD en la Empresa de Telecomunicaciones, que se constituirá en una guía para la prevención y corrección de las actividades encaminadas a evitar las vulneraciones de los derechos y libertades de los titulares de los datos personales por efecto del tratamiento estos; en particular, del control de la implementación de las medidas organizativas, jurídicas, administrativas, técnicas y físicas; así como el monitoreo continuo de estas medidas de mitigación.

Asimismo, el DPD deberá establecer, como parte del control preventivo, las observaciones y oportunidades de mejora cuando las medidas no hayan sido determinadas y suficientes para mitigar el riesgo en el tratamiento de los datos, en cuyo efecto, en el momento de la evaluación preventiva se sugerirá la adaptación de nuevas medidas que permitan el cumplimiento de la LOPDP, evitando la vulneración de los derechos y libertades del titular de los datos y la imposición de multas o sanciones por parte de los organismos o autoridades de control.

Recomendaciones

Se recomienda que en la designación del DPD, la Empresa de Telecomunicaciones incorpore como parte del perfil de su DPD el modelo señalado en el *Libro Blanco del DPD* correspondiente a las funciones compartidas entre el Delegado de Protección de Datos Personales y el Oficial de Cumplimiento o *Compliance Officer*. No existe incompatibilidad en sus funciones, pues sus puestos se complementan y no existe conflicto de intereses, debido a que ambos cargos aseguran el cumplimiento de normas legales dentro de la Empresa de Telecomunicaciones.

Es de anotar que cuando se expida el Reglamento a la LOPDP, así como las disposiciones del organismo regulador, el DPD, en seguimiento del Plan de Cumplimiento, solicitará a la Empresa de Telecomunicaciones, en calidad de responsable del tratamiento de datos, que efectúe una revisión detallada de las medidas de mitigación de riesgos y de las herramientas de evaluación de impacto al tratamiento de datos, a fin de generar y adaptar los reportes que requerirá la Superintendencia de Protección de Datos.

De la misma manera, cuando se convaliden las certificaciones internacionales en materia de protección de datos personales por parte de la Superintendencia de Protección Datos, a través de entidades certificadoras, la Empresa de Telecomunicaciones deberá someterse a una auditoría a fin de obtener estos sellos de protección de datos personales, los que le permitirán acreditar el haber implementado las mejores prácticas en el tratamiento de datos en sus procesos, promoviendo la confianza del titular de los datos, en cumplimiento del principio de responsabilidad proactiva y demostrada.

En relación con la observancia del esquema de ejecución al Plan de Cumplimiento del DPD y teniendo en cuenta que la LOPDP ha contemplado una moratoria de dos años en la aplicación del régimen sancionatorio, estableciendo una suerte de *vacatio legis,* obligará

al responsable del tratamiento, la Empresa de Telecomunicaciones, al estricto cumplimiento de las medidas de mitigación levantadas en la(s) auditoría(s) y en el estudio de impacto del tratamiento de datos, evitando así las sanciones establecidas en la norma.

Referencias Bibliográficas

Alvino, C. (2021). *Estadísticas de la situación digital de Ecuador en el 2020-2021*. *Branch.* https://branch.com.co/marketing-digital/estadisticas-de-la-situacion-digital-de-ecuador-en-el-2020-2021/

Asamblea Nacional del Ecuador. *Constitución de la República del Ecuador*. Registro Oficial N° 449, 20 de octubre de 2008.

Asamblea Nacional del Ecuador. *Código Orgánico Integral Penal*. Registro Oficial Suplemento N° 180, 10 de febrero de 2014.

Asamblea Nacional del Ecuador. *Ley Orgánica de Telecomunicaciones*. Registro Oficial Suplemento No. 439, 18 de febrero de 2015.

Asamblea Nacional del Ecuador. *Ley Orgánica de Protección de Datos Personales*. Registro Oficial Suplemento No. 459, 26 de mayo de 2021.

Asociación Española de Protección de Datos (2019). *Esquema de certificación de delegados de protección de datos de la Agencia Española de Protección de Datos (Esquema AEPD-DPD).*

Asociación Española de Protección de Datos. (2021). *Guía de riesgo y evaluación de impacto en tratamiento de datos personales.*

Asociación Española de Protección de Datos. (sf) *Protección de Datos y Administración local, Guías sectoriales AEPD.*

Banco Central del Ecuador. (junio, 2022). *Ecuador Registró un Crecimiento Interanual de 3.8% en el Primer Trimestre de 2022*. https://www.bce.fin.ec/index.php/boletines-de-prensa-archivo/item/1514-ecuador-registro-un-crecimiento-interanual-de-3-8-en-el-primer-trimestre-de-2022

Congreso Nacional. *Ley Orgánica de la Contraloría General del Estado.* Registro Oficial Suplemento N° 595, 12 de junio de 2002.

Congreso Nacional. *Código del Trabajo*. Registro Oficial Suplemento N°167, 16 de diciembre de 2005.

Davara, I. (2019). *Diccionario de Protección de Datos Personales, conceptos fundamentales.* Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales INAI, México.

De Miguel, J. (2018). *Economist Jurist* s/e

Durán, B. (2019). *El Delegado de Protección de Datos en el RGPD y la Nueva LOPDGDD*. Wolters Kluwer España. https://elibro.net/es/ereader/udla/118188?page=1

Fernández, M., Lerdo de Tejada, M., Lorenzo, S., Murga, J., Palma, A. (2018). *Protección de datos, responsabilidad activa y técnicas de garantía. Curso de "Delegado de la Protección de Datos*" , Reus S.A.

Grupo "Protección de datos" del Art. 29 (2017). Directrices WP248 rev.01. *Directrices sobre la evaluación de impacto relativa a la protección de datos (EIPD) y para determinar si el tratamiento «entraña probablemente un alto riesgo» a efectos del Reglamento (UE) 2016/679*

La Agencia Española de Protección de Datos (AEPD). (2021). *"EVALÚA_RIESGO RGPD v1*

Ministerio de Telecomunicaciones y Sociedad de la Información. (2017). *Libro Blanco de la Sociedad de la Información y del Conocimiento.* Mintel.

Ministerio de Telecomunicaciones y Sociedad de la Información. Acuerdo Ministerial N°11-2017. *Políticas Públicas del Sector de las Telecomunicaciones y de la Sociedad de la Información 2017-20121*. Registro Oficial No. 15, 15 de junio del 2017.

Montaño, D. (11 de enero de 2022) *Los desafíos ambientales de Ecuador en 2022: una verdadera transición ecológica, implementar Escazú y mayores recursos para las áreas protegidas*. https://es.mongabay.com/2022/01/desafios-ambientales-de-ecuador-en-2022/

Norma Internacional ISO 9000. (2015). *Sistema de Gestión de la Calidad – Fundamentos y Vocabulario*. Obtenido de la Norma Internacional ISO 9000: http://www.umc.edu.ve/pdf

Norma Internacional ISO 31000. (2018). *Gestión de Riesgos.* Obtenido de la Norma Internacional ISO 31000 https://www.iso.org/obp/ui#iso:std:iso:31000:ed-2:v1:es

Ortega C. (2017) *Desarrollo de habilidades blandas desde edades tempranas* Universidad Ecotec

Parlamento Europeo y del Consejo. (2016). *Reglamento (UE) 2016/679*.

Real Academia Española. (s.f.). Norma. *Diccionario de la lengua española*. Recuperado el 9 de agosto, 2022, de https://dle.rae.es/norma

Saiz, C., Balanzátegui, B. (2019) *El Libro Blanco del DPO.* Asociación Española para el Fomento de la Seguridad de la Información, ISMS Forum Spain

Salvador, T. (2017). en *Curso de "Delegado de Protección de Datos*"

Sierra Benítez, E. (2018). *Revista Internacional y comparada de Relaciones Laborales y Derecho del Empleo.* El delegado de protección de datos en la industria 4.0: funciones, competencias y las garantías esenciales de su estatuto jurídico, ADAPDT

Simón Castellano, P. y Bacaria Martrus, J. (2020). *Las Funciones del Delegado de Protección de Datos en los Distintos Sectores de Actividad.* Wolters Kluwer España. https://elibro.net/es/ereader/udla/136388?page=1

Ulloa, C. (2022). *Ecuador: entre el estallido y el diálogo.* Latinoamérica21. https://latinoamerica21.com/es/ecuador-entre-el-estallido-y-el-dialogo/

ANEXO 1

VERSION 1.0

Limpiar datos | Comenzar

Evaluación de Impacto relativa a la Protección de Datos (EIPD) Art. 42 LEY ORGANICA DE PROTECCIÓN DE DATOS PERSONALES

Las celdas que requieren entrada están marcadas en color:

El Art. 42 de la LODPDP dispone: "Evaluación de impacto del tratamiento de datos personales.- El responsable realizará una evaluación de impacto del tratamiento de datos personales cuando se haya identificado la probabilidad de que dicho tratamiento, por su naturaleza, contexto o fines, conlleve un alto riesgo para los derechos y libertades del titular o cuando la Autoridad de Protección de Datos Personales lo requiera".

La Evaluación de Impacto en la Protección de Datos Personales (EIPD) es una herramienta que permite evaluar de manera anticipada cuáles son los potenciales riesgos a los que están expuestos los datos personales en función de las actividades de tratamiento que se llevan a cabo con los mismos. El análisis de riesgos para un determinado tratamiento permite identificar los riesgos que se ciernen sobre los datos de los interesados y establecer una respuesta adoptando las salvaguardas necesarias para reducirlos hasta un nivel de riesgo aceptable.

La EIPD es una herramienta con carácter preventivo que debe realizar el responsable del tratamiento para poder identificar, evaluar y gestionar los riesgos a los que están expuestas sus actividades de tratamiento con el objetivo de garantizar los derechos y libertades de las personas físicas. En la práctica, la EIPD permite determinar el nivel de riesgo que entraña un tratamiento, con el objetivo de establecer las medidas de control más adecuadas para reducir el mismo hasta un nivel considerado aceptable.

Instrucciones:

1. Pulse "Comenzar" para iniciar el análisis.
2. Determine, en un primer ciclo de análisis, la aplicabilidad de los diferentes factores de riesgo al tratamiento de datos personales para calcular el riesgo intrínseco. Seleccionando el cuadro de aplicabilidad de cada factor de riesgo se desplegará (en muchos casos) una descripción con algunos ejemplos, además de permitir seleccionar “Aplica” o “No aplica”.
3. Pulse "Siguiente" para recorrer las distintas categorías de factores de riesgo. Seleccionando las pestañas se puede acceder directamente a las distintas categorías de factores de riesgo, aunque se recomienda que en un primer análisis se realice un recorrido secuencial.
4. Repita los apartados 2, 3 y 4 para cada una de las categorías de factores de riesgo considerados en la herramienta.
5. En la pestaña "Resultado" obtendrá el nivel de riesgo intrínseco y la valoración sobre la necesidad de realizar un EIPD.
6. En la pestaña "Resultado" pulse el botón "Informe" para generar un resumen de la información consignada.
7. Una vez realizada la evaluación del riesgo intrínseco, vuelva al inicio e indique el nivel de mitigación que introducen las medidas y garantías que hayan adoptado para cada factor de riesgo: “No mitigado”, “Limitadamente mitigado”, “Significativamente mitigado", “Mitigado”.
8. Siga los pasos anteriores para determinar finalmente el riesgo residual.
9. Si lo desea, imprima el informe resultante pulsando el botón imprimir en la hoja "Resultados".

Reiniciar Atras Siguiente

Factores de riesgo que se derivan del fin declarado del tratamiento y otros fines vinculados al propósito principal.

OPERACIONES RELACIONADAS CON LOS FINES DE TRATAMIENTO

	Aplicabilidad del riesgo	Mitigación
Perfilado	Aplica	Significativamente mitigado
Evaluación de sujetos	No aplica	
Predicción	Aplica	Significativamente mitigado
Control del empleado	Aplica	Significativamente mitigado
Control de acceso a internet	Aplica	Significativamente mitigado
Observación	Aplica	Significativamente mitigado
Monitorización	No aplica	
Supervisión	No aplica	
Rastreo de contactos	No aplica	
Control físico de acceso	Aplica	Significativamente mitigado
Localización	No aplica	
Identificación unívoca	No aplica	
Decisiones Automatizadas sin intervención humana	No aplica	
Tratamiento automatizado para soporte a toma de decisiones	No aplica	
Decidir sobre, o impedir, el ejercicio de derechos fundamentales	No aplica	
Decidir sobre el control del interesado de sus datos personales	No aplica	
Decidir sobre el acceso a un servicio	No aplica	
Decidir sobre la realización o ejecución de un contrato	No aplica	
Decidir sobre el accesos a servicios financieros	No aplica	
Efectos jurídicos sobre las personas	No aplica	
Evaluación y/o predicción de enfermedad/salud genéticamente	Aplica	Significativamente mitigado
Conservación con fines de archivo	Aplica	Significativamente mitigado

Reiniciar | Atras | Siguiente

Factores de riesgo relacionados con el ámbito del tratamiento que se derivan de los datos recogidos, procesados o inferidos en el tratamiento.

TIPOS DE DATOS UTILIZADOS

	Aplicabilidad del riesgo	Mitigación
Documentos personales	Aplica	Significativamente mitigado
Información de aplicaciones de registro de actividades vitales	No aplica	
Aspectos personales	No aplica	
Preferencias de consumo, gustos, hábitos (no categorias especiales)	No aplica	
Rendimiento laboral	Aplica	Significativamente mitigado
Situación económica	Aplica	Significativamente mitigado
Estado financiero	No aplica	
Medios de pago	No aplica	
Datos de comportamiento	Aplica	Significativamente mitigado
Datos de localización	No aplica	
Datos sanitarios	Aplica	Significativamente mitigado
Datos biométricos	Aplica	Significativamente mitigado
Datos genéticos	No aplica	
Categorías especiales de datos o que permitan inferirlos	No aplica	
Categorías especiales de datos seudonimizados	No aplica	
Datos personales relativos a condenas e infracciones penales (o administrativas)	No aplica	
Metadatos	No aplica	
Identificadores únicos	Aplica	Significativamente mitigado
Datos y metadatos de la comunicaciones electrónicas	Aplica	Significativamente mitigado
Datos de navegación web	Aplica	Significativamente mitigado

Reiniciar

Atras Siguiente

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.

EXTENSIÓN Y ALCANCE DEL TRATAMIENTO

	Aplicabilidad del riesgo	Mitigación
Sistemático	Aplica	Limitadamente mitigado
Exhaustivo sobre las personas	No aplica	
Involucra gran número de sujetos	No aplica	
El volumen de datos tratado es muy elevado	No aplica	
Duración del tratamiento elevada	Aplica	Limitadamente mitigado
Actividad del tratamiento de gran alcance geográfico	No aplica	
Tratamiento a gran escala	No aplica	
Recopilación excesiva de datos con relación al fin del tratamiento	No aplica	

Reiniciar Atras Siguiente

interesados, como empleados, menores, mayores, personas en situación de vulnerabilidad, víctimas, discapacitados, etc.

CATEGORIAS DE INTERESADOS

	Aplicabilidad del riesgo	Mitigación
Menores de 14 años	No aplica	
Víctimas de violencia de género	No aplica	
Menores dependientes de sujetos vulnerables	No aplica	
Persona bajo guardia y custodia de víctimas de violencia de género	No aplica	
Mayores con discapacidad	No aplica	
Personas mayores	No aplica	
Personas con enfermedades mentales	No aplica	
Discapacitados	No aplica	
Personas que acceden a servicios sociales	No aplica	
Sujetos en riesgo de exclusión social	No aplica	
Empleados	Aplica	Significativamente mitigado
Solicitantes de asilo	No aplica	
Pacientes/Examenes ocupacionales	Aplica	Significativamente mitigado
Sujetos vulnerables	No aplica	

Reiniciar Atras Siguiente

Factores de riesgo que se derivan de la naturaleza del tratamiento al implementarse con determinadas características técnicas o tecnologías.

FACTORES TÉCNICOS DEL TRATAMIENTO

	Aplicabilidad del riesgo	Mitigación
Sistema de información hospitalaria	No aplica	
TV interactiva	No aplica	
Servicios web	Aplica	Significativamente mitigado
Aplicaciones móviles	No aplica	
Sistemas de registro de localización	No aplica	
Reconocimiento facial	No aplica	
Huella dactilar/datos biométricos	Aplica	Significativamente mitigado
IoT (Internet de las Cosas)	No aplica	
Uso innovador o nuevas soluciones organizativas	No aplica	
Uso innovador de tecnologías consolidadas	No aplica	
Tecnologías combinadas con otras	No aplica	
Nuevas tecnologías	No aplica	
Alto grado de fragmentación de los actores que intervienen en el desarrollo e implementación de los productos/servicios que implementan el tratamiento	No aplica	Significativamente mitigado
Tratamientos automatizados	No aplica	
Sistema inteligente	No aplica	
Videovigilancia	Aplica	Limitadamente mitigado

Reiniciar Atras Siguiente

Factores de riesgo que se derivan de la naturaleza del tratamiento al recogerse o generarse datos de forma específica.

RECOGIDA Y GENERACIÓN DE DATOS

	Aplicabilidad del riesgo	Mitigación
Acceso a bases de datos de referencia de crédito	Aplica	Significativamente mitigado
Acceso a bases de datos sobre fraude	No aplica	
Acceso a bases de datos sobre blanqueo de capitales o financiación del terrorismo	No aplica	
Datos personales obtenidos en zonas de acceso público	No aplica	
Recogida de datos de los medios sociales públicos	Aplica	Significativamente mitigado
Recogida de datos de redes de comunicaciones	No aplica	
Recogida de datos de aplicaciones	No aplica	
Datos procedentes de dos o mas tratamientos con finalidades diferentes	No aplica	
Datos procedentes de dos o mas responsables distintos	No aplica	
Asociación de conjuntos de datos	No aplica	
Combinación de conjuntos de datos	No aplica	
Enlaces de registros de base de datos de dos o mas tratamientos con finalidades o responsables diferentes	No aplica	
Recogida de datos por un responsable distinto al que trata y aplica excepción de información	Aplica	Significativamente mitigado
Falta de transparencia del momento preciso de la recogida de datos	No aplica	
Nuevas formas de recogida de datos con riegos para derechos y libertades	No aplica	

Reiniciar Atras Siguiente

Factores de riesgo que se derivan del contexto del tratamiento al poder generarse consecuencias no contempladas en los propósitos originales previstos del tratamiento. En este caso, no se ha evaluado el nivel de riesgo, sino solo el impacto que podría tener. El responsable tendrá que evaluar la probabilidad de que estas amenazas se materialicen en su tratamiento, por lo que se deja la columna "Probabilidad" vacía. Una vez completada, podrá determinar el nivel de riesgo empleando, por ejemplo, la matriz de riesgo "probabilidad x impacto" de la Guía.

EFECTOS COLATERALES DEL TRATAMIENTO

	Aplicabilidad del riesgo	Probabilidad	Mitigación
Excede las expectativas del interesado	No aplica		
Posible reversión no autorizada de la seudonimización	No aplica		
Posible pérdida de control por el responsable de los datos procesados por el encargado del tratamiento	No aplica		
Riesgo de reidentificación de usuarios	No aplica		
Podría determinar la situación financiera	Aplica	Muy alta	Significativamente mitigado
Podría determinar la solvencia patrimonial	Aplica	Muy alta	Significativamente mitigado
Podría deducir información relacionada con categorías especiales de datos	Aplica	Muy alta	Significativamente mitigado
Pudiera privar a los afectados de sus derechos y libertades	No aplica		
Pudiera impedir el control sobre sus datos personales	No aplica		
Puede provocar exclusión	No aplica		
Puede provocar o genera discriminación	No aplica		
Posible usurpación de identidad	No aplica		
Posible fraude	No aplica		
Posible daño reputacional	No aplica		
Posible perjuicio económico significativo	No aplica		
Posible perjuicio moral significativo	No aplica		
Posible perjuicio social significativo	No aplica		
Posible pérdida de confidencialidad de datos sujetos al secreto profesional	Aplica	Baja	Significativamente mitigado
Podría impedir el ejercicio de un derecho	No aplica		
Podría impedir el acceso a un servicio	No aplica		
Podría impedir el acceso a un contrato	No aplica		
Podría recoger datos personales distintos de los usuarios de servicio	No aplica		
Posible manipulación de las personas	No aplica		
Posibilidad de autocensura	No aplica		
Posibilidad de provocar un cambio cultural para claudicar derechos y libertades	No aplica		
Usos imprevistos o no deseados que pudieran afectar a derechos fundamentales	No aplica		

Reiniciar Atras Siguiente

Factores de riesgo que se derivan del contexto específico del sector de actividad, modelo de negocio o tipo de entidad.
En este caso, entendido generalmente para tratamientos que no forman parte de los procesos de soporte de la entidad.

CATEGORÍA DEL RESPONSABLE / ENCARGADO

	Aplicabilidad del riesgo	Mitigación
Sociedad de la información	No aplica	
Empresa de biotecnología	No aplica	
Mercadotecnia	Aplica	Significativamente mitigado
Hospitales	No aplica	
Investigadores privados	No aplica	
Entidad de evaluación de información crediticia	No aplica	
Entidad de evaluación de fraude	No aplica	
Entidad financiera	No aplica	
Empleador	Aplica	Significativamente mitigado
Proyectos de investigación	No aplica	
Ensayos clínicos	No aplica	

Reiniciar | Atras | Siguiente

Factores de riesgo que se derivan del contexto en el que se realizan las comunicaciones de datos a terceros en el marco del tratamiento.

COMUNICACIONES DE DATOS

	Aplicabilidad del riesgo	Mitigación
Transferencia habitual a estados u organizaciones en otros países sin un adecuado nivel de protección	No aplica	
Falta de transparencia de los actores involucrados en el tratamiento	No aplica	

Reiniciar Atras Siguiente

Es necesario estudiar las peculiaridades del tratamiento para identificar factores de riesgo para los derechos y libertades que no estén identificados explícitamente en el RGPD o en su desarrollo. El responsable de llevar a cabo el análisis de riesgos ha de realizar un análisis crítico de su tratamiento para señalar aquellas situaciones singulares que podrían tener afectación desde el punto de vista de los riesgos introducidos.

En particular, los identificados en los códigos de conducta a los que se está

	Aplicabilidad del riesgo	Probabilidad	Impacto	Mitigación
Pérdida de información en archivos físicos o digitales	Aplica	Baja	Limitado	Significativamente mitigado
Prolongado almacenamiento de archivos físicos o digitales	Aplica	Baja	Limitado	Significativamente mitigado
Introduce breve descripción del factor de riesgo				
Introduce breve descripción del factor de riesgo				
Introduce breve descripción del factor de riesgo				
Introduce breve descripción del factor de riesgo				
Introduce breve descripción del factor de riesgo				
Introduce breve descripción del factor de riesgo				
Introduce breve descripción del factor de riesgo				
Introduce breve descripción del factor de riesgo				

Reiniciar | Atras | Siguiente

SEGURIDAD EN LOS TRATAMIENTOS

Factores de riesgo que se derivan de la posible materialización de brechas de seguridad sobre los datos personales.

	Aplicabilidad del riesgo	Probabilidad	Impacto	Mitigación
Pérdida de confidencialidad	Aplica	Baja	Limitado	Significativamente mitigado
Pérdida de integridad	Aplica	Baja	Limitado	Significativamente mitigado
Pérdida de disponibilidad	Aplica	Baja	Significativo	Significativamente mitigado
Pérdida de trazabilidad	Aplica	Baja	Limitado	Significativamente mitigado
Pérdida de autenticidad	No aplica			
Deficiencias en resiliencia	No aplica			
Fallos en medidas y garantías técnicas de protección de datos	Aplica	Baja	Limitado	Significativamente mitigado
Errores en las operaciones técnicas de tratamiento	Aplica	Baja	Limitado	Significativamente mitigado

VALORACIÓN RIESGO INTRÍNSECO	VALORACIÓN RIESGO
ALTO	ALTO

INFORME

El resultado de valoración de riesgo intrínseco es:	**ALTO**
El resultado de valoración de riesgo residual es:	**ALTO**

LISTADO DE FUENTES DE RIESGO POR CATEGORÍAS:

CATEGORÍA: OPERACIONES RELACIONADAS CON LOS FINES DE TRATAMIENTO:
- Perfilado, Mitigación: Significativamente mitigado
- Predicción, Mitigación: Significativamente mitigado
- Control del empleado, Mitigación: Significativamente mitigado
- Control de acceso a internet, Mitigación: Significativamente mitigado
- Observación, Mitigación: Significativamente mitigado
- Control físico de acceso, Mitigación: Significativamente mitigado
- Evaluación y/o predicción de enfermedad/salud genéticamente, Mitigación: Significativamente mitigado
- Conservación con fines de archivo, Mitigación: Significativamente mitigado

CATEGORÍA: TIPOS DE DATOS UTILIZADOS:
- Documentos personales, Mitigación: Significativamente mitigado
- Rendimiento laboral, Mitigación: Significativamente mitigado
- Situación económica, Mitigación: Significativamente mitigado
- Datos de comportamiento, Mitigación: Significativamente mitigado
- Datos sanitarios, Mitigación: Significativamente mitigado
- Datos biométricos, Mitigación: Significativamente mitigado
- Identificadores únicos, Mitigación: Significativamente mitigado
- Datos y metadatos de la comunicaciones electrónicas, Mitigación: Significativamente mitigado
- Datos de navegación web, Mitigación: Significativamente mitigado

CATEGORÍA: EXTENSIÓN Y ALCANCE DEL TRATAMIENTO:
- Sistemático, Mitigación: Limitadamente mitigado
- Duración del tratamiento elevada, Mitigación: Limitadamente mitigado

CATEGORÍA: CATEGORIAS DE INTERESADOS:
- Empleados, Mitigación: Significativamente mitigado
- Pacientes, Mitigación: Significativamente mitigado

CATEGORÍA: FACTORES TÉCNICOS DEL TRATAMIENTO:
- Servicios web, Mitigación: Significativamente mitigado
- Huella dactilar, Mitigación: Significativamente mitigado
- Videovigilancia, Mitigación: Limitadamente mitigado

CATEGORÍA: RECOGIDA Y GENERACIÓN DE DATOS:
- Acceso a bases de datos de referencia de crédito, Mitigación: Significativamente mitigado
- Recogida de datos de los medios sociales públicos, Mitigación: Significativamente mitigado
- Recogida de datos por un responsable distinto al que trata y aplica excepción de información, Mitigación: Significativamente mitigado

CATEGORÍA: EFECTOS COLATERALES DEL TRATAMIENTO:
- Podría determinar la situación financiera, Probabilidad: Muy alta, Mitigación: Significativamente mitigado
- Podría determinar la solvencia patrimonial, Probabilidad: Muy alta, Mitigación: Significativamente mitigado
- Podría deducir información relacionada con categorías especiales de datos, Probabilidad: Muy alta, Mitigación: Significativamente mitigado
- Posible pérdida de confidencialidad de datos sujetos al secreto profesional, Probabilidad: Baja, Mitigación: Significativamente mitigado

CATEGORÍA: CATEGORÍA DEL RESPONSABLE / ENCARGADO:
- Mercadotecnia, Mitigación: Significativamente mitigado
- Empleador, Mitigación: Significativamente mitigado

CATEGORÍA: COMUNICACIONES DE DATOS:
- El usuario no ha configurado ningún factor en esta categoría.

CATEGORÍA: OTROS FACTORES DE RIESGO ESPECÍFICOS DEL TRATAMIENTO:
- Pérdida de información en archivos físicos o digitales, Probabilidad: Baja, Impacto: Limitado, Mitigación: Significativamente mitigado
- Prolongado almacenamiento de archivos físicos o digitales, Probabilidad: Baja, Impacto: Limitado, Mitigación: Significativamente mitigado

CATEGORÍA: SEGURIDAD EN LOS TRATAMIENTOS:
- Pérdida de confidencialidad, Probabilidad: Baja, Impacto: Limitado, Mitigación: Significativamente mitigado
- Pérdida de integridad, Probabilidad: Baja, Impacto: Limitado, Mitigación: Significativamente mitigado

VALORACIÓN RIESGO INTRÍNSECO	VALORACIÓN RIESGO
ALTO	ALTO

- Pérdida de disponibilidad, Probabilidad: Baja, Impacto: Significativo, Mitigación: Significativamente mitigado
- Pérdida de trazabilidad, Probabilidad: Baja, Impacto: Limitado, Mitigación: Significativamente mitigado
- Fallos en medidas y garantías técnicas de protección de datos, Probabilidad: Baja, Impacto: Limitado, Mitigación: Significativamente mitigado
- Errores en las operaciones técnicas de tratamiento, Probabilidad: Baja, Impacto: Limitado, Mitigación: Significativamente mitigado

Este informe tiene carácter de documento de soporte a la realización de la gestión del riesgo, y en ningún caso la sustituye, ni reemplaza a las obligaciones de responsables y encargados. La utilización de herramientas no puede reducir el cumplimiento de la responsabilidad proactiva a una cuestión meramente formal, o una limitación en la capacidad de decisión a la hora de evaluar el riesgo. Ninguna herramienta, en sí misma, toma decisiones que corresponden al responsable sobre los fines y medios del tratamiento, no sustituye las obligaciones y principios que son aplicables a un tratamiento en función de su naturaleza, ámbito, fines y contexto, ni implementa las políticas de protección de datos y las medidas y garantías para la gestión del riesgo para los derechos y libertades.
En todo caso, a la hora de utilizar los resultados de esta herramienta, se aconseja añadir referencias y comentarios (documentos, enlaces, notas, informes, etc.) sobre cada una de las valoraciones de riesgo realizadas.

ANEXO 2

VERSION 1.0

Limpiar datos | Comenzar

Evaluación de Impacto relativa a la Protección de Datos (EIPD) Art. 42 LEY ORGANICA DE PROTECCIÓN DE DATOS PERSONALES

Las celdas que requieren entrada están marcadas en color:

El Art. 42 de la LODPDP dispone: "Evaluación de impacto del tratamiento de datos personales.- El responsable realizará una evaluación de impacto del tratamiento de datos personales cuando se haya identificado la probabilidad de que dicho tratamiento, por su naturaleza, contexto o fines, conlleve un alto riesgo para los derechos y libertades del titular o cuando la Autoridad de Protección de Datos Personales lo requiera".

La Evaluación de Impacto en la Protección de Datos Personales (EIPD) es una herramienta que permite evaluar de manera anticipada cuáles son los potenciales riesgos a los que están expuestos los datos personales en función de las actividades de tratamiento que se llevan a cabo con los mismos. El análisis de riesgos para un determinado tratamiento permite identificar los riesgos que se ciernen sobre los datos de los interesados y establecer una respuesta adoptando las salvaguardas necesarias para reducirlos hasta un nivel de riesgo aceptable.

La EIPD es una herramienta con carácter preventivo que debe realizar el responsable del tratamiento para poder identificar, evaluar y gestionar los riesgos a los que están expuestas sus actividades de tratamiento con el objetivo de garantizar los derechos y libertades de las personas físicas. En la práctica, la EIPD permite determinar el nivel de riesgo que entraña un tratamiento, con el objetivo de establecer las medidas de control más adecuadas para reducir el mismo hasta un nivel considerado aceptable.

Instrucciones:

1. Pulse "Comenzar" para iniciar el análisis.
2. Determine, en un primer ciclo de análisis, la aplicabilidad de los diferentes factores de riesgo al tratamiento de datos personales para calcular el riesgo intrínseco. Seleccionando el cuadro de aplicabilidad de cada factor de riesgo se desplegará (en muchos casos) una descripción con algunos ejemplos, además de permitir seleccionar “Aplica” o “No aplica”.
3. Pulse "Siguiente" para recorrer las distintas categorías de factores de riesgo. Seleccionando las pestañas se puede acceder directamente a las distintas categorías de factores de riesgo, aunque se recomienda que en un primer análisis se realice un recorrido secuencial.
4. Repita los apartados 2, 3 y 4 para cada una de las categorías de factores de riesgo considerados en la herramienta.
5. En la pestaña "Resultado" obtendrá el nivel de riesgo intrínseco y la valoración sobre la necesidad de realizar un EIPD.
6. En la pestaña "Resultado" pulse el botón "Informe" para generar un resumen de la información consignada.
7. Una vez realizada la evaluación del riesgo intrínseco, vuelva al inicio e indique el nivel de mitigación que introducen las medidas y garantías que hayan adoptado para cada factor de riesgo: “No mitigado”, “Limitadamente mitigado”, “Significativamente mitigado", “Mitigado”.
8. Siga los pasos anteriores para determinar finalmente el riesgo residual.
9. Si lo desea, imprima el informe resultante pulsando el botón imprimir en la hoja "Resultados".

Reiniciar Atras Siguiente

Factores de riesgo que se derivan del fin declarado del tratamiento y otros fines vinculados al propósito principal.

OPERACIONES RELACIONADAS CON LOS FINES DE TRATAMIENTO

	Aplicabilidad del riesgo	Mitigación	Medida de control / indicador de cumplimiento
Perfilado	Aplica	Significativamente mitigado	1. Convenios de confidencialidad. 2. Politicas, procedimientos y manual de seguridad de informacion T. I. 3. Aceptacion de tratamiento de datos del titular; 4. Actas de reuniones de comités en los que se incorpora la gestión del tratamiento de datos.
Evaluación de sujetos	No aplica		
Predicción	Aplica	Significativamente mitigado	1. Convenios de confidencialidad. 2. Politicas, procedimientos y manual de seguridad de informacion T. I. 3. Aceptacion de tratamiento de datos del titular; 4. Actas de reuniones de comités en los que se incorpora la gestión del tratamiento de datos.
Control del empleado	Aplica	Significativamente mitigado	1. Convenios de confidencialidad. 2. Politicas, procedimientos y manual de seguridad de informacion T. I. 3. Aceptacion de tratamiento de datos del titular; 4. Actas de reuniones de comités en los que se incorpora la gestión del tratamiento de datos.
Control de acceso a internet	Aplica	Significativamente mitigado	Politicas, procedimientos y manual de seguridad de informacion T. I.
Observación	Aplica	Significativamente mitigado	1. Convenios de confidencialidad. 2. Politicas, procedimientos y manual de seguridad de informacion T. I. 3. Aceptacion de tratamiento de datos del titular; 4. Actas de reuniones de comités en los que se incorpora la gestión del tratamiento de datos.
Monitorización	No aplica		
Supervisión	No aplica		
Rastreo de contactos	No aplica		
Control físico de acceso	Aplica	Significativamente mitigado	Politicas, procedimientos y manual de seguridad de informacion T. I.
Localización	No aplica		
Identificación unívoca	No aplica		
Decisiones Automatizadas sin intervención humana	No aplica		
Tratamiento automatizado para soporte a toma de decisiones	No aplica		
Decidir sobre, o impedir, el ejercicio de derechos fundamentales	No aplica		
Decidir sobre el control del interesado de sus datos personales	No aplica		
Decidir sobre el acceso a un servicio	No aplica		
Decidir sobre la realización o ejecución de un contrato	No aplica		
Decidir sobre el accesos a servicios financieros	No aplica		
Efectos jurídicos sobre las personas	No aplica		
Evaluación y/o predicción de enfermedad/salud genéticamente	Aplica	Significativamente mitigado	1. Convenios de confidencialidad. 2. Aceptacion de tratamiento de datos del titular;
Conservación con fines de archivo	Aplica	Significativamente mitigado	1. Convenios de confidencialidad. 2. Politicas, procedimientos y manual de seguridad de informacion T. I. 3. Aceptacion de tratamiento de datos del titular; 4.Procedimiento de gestion documental de archivo y eliminacion; 5 Actas de reuniones de comités en los que se incorpora la gestión del tratamiento de datos

Reiniciar | Atras | Siguiente

Factores de riesgo relacionados con el ámbito del tratamiento que se derivan de los datos recogidos, procesados o inferidos en el tratamiento.

TIPOS DE DATOS UTILIZADOS

	Aplicabilidad del riesgo	Mitigación	Medida de control / indicador de cumplimiento
Documentos personales	Aplica	Significativamente mitigado	1. Convenios de confidencialidad. 2. Politicas, procedimientos y manual de seguridad de informacion T. I. 3. Aceptacion de tratamiento de datos del titular; 4.Procedimiento de gestion documental de archivo y eliminacion; 5. Actas de reuniones de comités en los que se incorpora la gestión del tratamiento de datos
Información de aplicaciones de registro de actividades vitales	No aplica		
Aspectos personales	No aplica		
Preferencias de consumo, gustos, hábitos (no categorias especiales)	No aplica		
Rendimiento laboral	Aplica	Significativamente mitigado	1. Convenios de confidencialidad. 2. Politicas, procedimientos y manual de seguridad de informacion T. I. 3. Aceptacion de tratamiento de datos del titular;
Situación económica	Aplica	Significativamente mitigado	1. Convenios de confidencialidad. 2. Politicas, procedimientos y manual de seguridad de informacion T. I. 3. Aceptacion de tratamiento de datos del titular; 4.Procedimiento de gestion documental de archivo y eliminacion
Estado financiero	No aplica		
Medios de pago	No aplica		
Datos de comportamiento	Aplica	Significativamente mitigado	1. Convenios de confidencialidad. 2. Politicas, procedimientos y manual de seguridad de informacion T. I. 3. Aceptacion de tratamiento de datos del titular; 4.Procedimiento de gestion documental de archivo y eliminacion
Datos de localización	No aplica		
Datos sanitarios	Aplica	Significativamente mitigado	1. Convenios de confidencialidad. 2. Politicas, procedimientos y manual de seguridad de informacion T. I. 3. Aceptacion de tratamiento de datos del titular; 4.Procedimiento de gestion documental de archivo y eliminacion
Datos biométricos	Aplica	Significativamente mitigado	1. Convenios de confidencialidad. 2. Politicas, procedimientos y manual de seguridad de informacion T. I. 3. Aceptacion de tratamiento de datos del titular; 4.Procedimiento de gestion documental de archivo y eliminacion
Datos genéticos	No aplica		
Categorías especiales de datos o que permitan inferirlos	No aplica		
Categorías especiales de datos seudonimizados	No aplica		
Datos personales relativos a condenas e infracciones penales (o administrativas)	No aplica		
Metadatos	No aplica		
Identificadores únicos	Aplica	Significativamente mitigado	1. Convenios de confidencialidad. 2. Politicas, procedimientos y manual de seguridad de informacion T. I. 3. Aceptacion de tratamiento de datos del titular; 4.Procedimiento de gestion documental de archivo y eliminacion
Datos y metadatos de la comunicaciones electrónicas	Aplica	Significativamente mitigado	1. Convenios de confidencialidad. 2. Politicas, procedimientos y manual de seguridad de informacion T. I. 3. Aceptacion de tratamiento de datos del titular; 4. Actas de reuniones de comités en los que se incorpora la gestión del tratamiento de datos.
Datos de navegación web	Aplica	Significativamente mitigado	1. Convenios de confidencialidad. 2. Politicas, procedimientos y manual de seguridad de informacion T. I. 3. Aceptacion de tratamiento de datos del titular; 4. Actas de reuniones de comités en los que se incorpora la gestión del tratamiento de datos.

Reiniciar Atras Siguiente

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.

EXTENSIÓN Y ALCANCE DEL TRATAMIENTO

	Aplicabilidad del riesgo	Mitigación	Medida de control / indicador de cumplimiento
Sistemático	Aplica	Limitadamente mitigado	1. Convenios de confidencialidad. 2. Politicas, procedimientos y manual de seguridad de informacion T. I. 3. Aceptacion de tratamiento de datos del titular; 4.Procedimiento de gestion documental de archivo y eliminacion
Exhaustivo sobre las personas	No aplica		
Involucra gran número de sujetos	No aplica		
El volumen de datos tratado es muy elevado	No aplica		
Duración del tratamiento elevada	Aplica	Limitadamente mitigado	1. Convenios de confidencialidad. 2. Politicas, procedimientos y manual de seguridad de informacion T. I. 3. Aceptacion de tratamiento de datos del titular; 4.Procedimiento de gestion documental de archivo y eliminacion
Actividad del tratamiento de gran alcance geográfico	No aplica		
Tratamiento a gran escala	No aplica		
Recopilación excesiva de datos con relación al fin del tratamiento	No aplica		

Reiniciar | Atras | Siguiente

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.

CATEGORIAS DE INTERESADOS

	Aplicabilidad del riesgo	Mitigación	Medida de control / indicador de cumplimiento
Menores de 14 años	No aplica		
Víctimas de violencia de género	No aplica		
Menores dependientes de sujetos vulnerables	No aplica		
Persona bajo guardia y custodia de víctimas de violencia de género	No aplica		
Mayores con discapacidad	No aplica		
Personas mayores	No aplica		
Personas con enfermedades mentales	No aplica		
Discapacitados	No aplica		
Personas que acceden a servicios sociales	No aplica		
Sujetos en riesgo de exclusión social	No aplica		
Empleados	Aplica	Significativamente mitigado	1. Convenios de confidencialidad. 2. Politicas, procedimientos y manual de seguridad de informacion T. I. 3. Aceptacion de tratamiento de datos del titular; 4.Procedimiento de gestion documental de archivo y eliminacion
Solicitantes de asilo	No aplica		
Pacientes/Examenes ocupacionales	Aplica	Significativamente mitigado	1. Convenios de confidencialidad. 2. Politicas, procedimientos y manual de seguridad de informacion T. I. 3. Aceptacion de tratamiento de datos del titular; 4.Procedimiento de gestion documental de archivo y eliminacion
Sujetos vulnerables	No aplica		

Reiniciar Atras Siguiente

Factores de riesgo que se derivan de la naturaleza del tratamiento al implementarse con determinadas características técnicas o tecnologías.

FACTORES TÉCNICOS DEL TRATAMIENTO

	Aplicabilidad del riesgo	Mitigación	Medida de control / indicador de cumplimiento
Sistema de información hospitalaria	No aplica		
TV interactiva	No aplica		
Servicios web	Aplica	Significativamente mitigado	1. Convenios de confidencialidad. 2. Politicas, procedimientos y manual de seguridad de informacion T. I. 3. Aceptacion de tratamiento de datos del titular; 4.Procedimiento de gestion documental de archivo y eliminacion
Aplicaciones móviles	No aplica		
Sistemas de registro de localización	No aplica		
Reconocimiento facial	No aplica		
Huella dactilar/datos biométricos	Aplica	Significativamente mitigado	1. Convenios de confidencialidad. 2. Politicas, procedimientos y manual de seguridad de informacion T. I. 3. Aceptacion de tratamiento de datos del titular; 4.Procedimiento de gestion documental de archivo y eliminacion
IoT (Internet de las Cosas)	No aplica		
Uso innovador o nuevas soluciones organizativas	No aplica		
Uso innovador de tecnologías consolidadas	No aplica		
Tecnologías combinadas con otras	No aplica		
Nuevas tecnologías	No aplica		
Alto grado de fragmentación de los actores que intervienen en el desarrollo e implementación de los productos/servicios que implementan el tratamiento	No aplica	Significativamente mitigado	1. Convenios de confidencialidad. 2. Politicas, procedimientos y manual de seguridad de informacion T. I. 3. Aceptacion de tratamiento de datos del titular; 4.Procedimiento de gestion documental de archivo y eliminacion
Tratamientos automatizados	No aplica		
Sistema inteligente	No aplica		
Videovigilancia	Aplica	Limitadamente mitigado	1. Convenios de confidencialidad. 2. Politicas, procedimientos y manual de seguridad de informacion T. I. 3. Aceptacion de tratamiento de datos del titular; 4.Procedimiento de gestion documental de archivo y eliminacion

Reiniciar Atras Siguiente

Factores de riesgo que se derivan de la naturaleza del tratamiento al recogerse o generarse datos de forma específica.

RECOGIDA Y GENERACIÓN DE DATOS

	Aplicabilidad del riesgo	Mitigación	Medida de control / indicador de cumplimiento
Acceso a bases de datos de referencia de crédito	Aplica	Significativamente mitigado	1. Convenios de confidencialidad. 2. Politicas, procedimientos y manual de seguridad de informacion T. I. 3. Aceptacion de tratamiento de datos del titular; 4.Procedimiento de gestion documental de archivo y eliminacion
Acceso a bases de datos sobre fraude	No aplica		
Acceso a bases de datos sobre blanqueo de capitales o financiación del terrorismo	No aplica		
Datos personales obtenidos en zonas de acceso público	No aplica		
Recogida de datos de los medios sociales públicos	Aplica	Significativamente mitigado	1. Convenios de confidencialidad. 2. Politicas, procedimientos y manual de seguridad de informacion T. I. 3. Aceptacion de tratamiento de datos del titular; 4.Procedimiento de gestion documental de archivo y eliminacion
Recogida de datos de redes de comunicaciones	No aplica		
Recogida de datos de aplicaciones	No aplica		
Datos procedentes de dos o mas tratamientos con finalidades diferentes	No aplica		
Datos procedentes de dos o mas responsables distintos	No aplica		
Asociación de conjuntos de datos	No aplica		
Combinación de conjuntos de datos	No aplica		
Enlaces de registros de base de datos de dos o mas tratamientos con finalidades o responsables diferentes	No aplica		
Recogida de datos por un responsable distinto al que trata y aplica excepción de información	Aplica	Significativamente mitigado	1. Convenios de confidencialidad. 2. Politicas, procedimientos y manual de seguridad de informacion T. I. 3. Aceptacion de tratamiento de datos del titular; 4.Procedimiento de gestion documental de archivo y eliminacion
Falta de transparencia del momento preciso de la recogida de datos	No aplica		
Nuevas formas de recogida de datos con riegos para derechos y libertades	No aplica		

Reiniciar | Atras | Siguiente

Factores de riesgo que se derivan del contexto del tratamiento al poder generarse consecuencias no contempladas en los propósitos originales previstos del tratamiento.
En este caso, no se ha evaluado el nivel de riesgo, sino solo el impacto que podría tener. El responsable tendrá que evaluar la probabilidad de que estas amenazas se materialicen en su tratamiento, por lo que se deja la columna "Probabilidad" vacía. Una vez completada, podrá determinar el nivel de riesgo empleando, por ejemplo, la matriz de riesgo "probabilidad x impacto" de la Guía.

EFECTOS COLATERALES DEL TRATAMIENTO

	Aplicabilidad del riesgo	Probabilidad	Mitigación	Medida de control / indicador de cumplimiento
Excede las expectativas del interesado	No aplica			
Posible reversión no autorizada de la seudonimización	No aplica			
Posible pérdida de control por el responsable de los datos procesados por el encargado del tratamiento	No aplica			
Riesgo de reidentificación de usuarios	No aplica			
Podría determinar la situación financiera	Aplica	Muy alta	Significativamente mitigado	1. Convenios de confidencialidad. 2. Politicas, procedimientos y manual de seguridad de informacion T. I. 3. Aceptacion de tratamiento de datos del titular; 4.Procedimiento de gestion documental de archivo y eliminacion
Podría determinar la solvencia patrimonial	Aplica	Muy alta	Significativamente mitigado	1. Convenios de confidencialidad. 2. Politicas, procedimientos y manual de seguridad de informacion T. I. 3. Aceptacion de tratamiento de datos del titular; 4.Procedimiento de gestion documental de archivo y eliminacion
Podría deducir información relacionada con categorías especiales de datos	Aplica	Muy alta	Significativamente mitigado	1. Convenios de confidencialidad. 2. Politicas, procedimientos y manual de seguridad de informacion T. I. 3. Aceptacion de tratamiento de datos del titular; 4.Procedimiento de gestion documental de archivo y eliminacion
Pudiera privar a los afectados de sus derechos y libertades	No aplica			
Pudiera impedir el control sobre sus datos personales	No aplica			
Puede provocar exclusión	No aplica			
Puede provocar o genera discriminación	No aplica			
Posible usurpación de identidad	No aplica			
Posible fraude	No aplica			
Posible daño reputacional	No aplica			
Posible perjuicio económico significativo	No aplica			
Posible perjuicio moral significativo	No aplica			
Posible perjuicio social significativo	No aplica			
Posible pérdida de confidencialidad de datos sujetos al secreto profesional	Aplica	Baja	Significativamente mitigado	1. Convenios de confidencialidad. 2. Politicas, procedimientos y manual de seguridad de informacion T. I. 3. Aceptacion de tratamiento de datos del titular; 4.Procedimiento de gestion documental de archivo y eliminacion
Podría impedir el ejercicio de un derecho	No aplica			
Podría impedir el acceso a un servicio	No aplica			
Podría impedir el acceso a un contrato	No aplica			
Podría recoger datos personales distintos de los usuarios de servicio	No aplica			
Posible manipulación de las personas	No aplica			
Posibilidad de autocensura	No aplica			
Posibilidad de provocar un cambio cultural para claudicar derechos y libertades	No aplica			
Usos imprevistos o no deseados que pudieran afectar a derechos fundamentales	No aplica			

Reiniciar Atras Siguiente

Factores de riesgo que se derivan del contexto específico del sector de actividad, modelo de negocio o tipo de entidad.
En este caso, entendido generalmente para tratamientos que no forman parte de los procesos de soporte de la entidad.

CATEGORÍA DEL RESPONSABLE / ENCARGADO

	Aplicabilidad del riesgo	Mitigación	Medida de control / indicador de cumplimiento
Sociedad de la información	No aplica		
Empresa de biotecnología	No aplica		
Mercadotecnia	Aplica	Significativamente mitigado	1. Convenios de confidencialidad. 2. Politicas, procedimientos y manual de seguridad de informacion T. I. 3. Aceptacion de tratamiento de datos del titular; 4.Procedimiento de gestion documental de archivo y eliminacion
Hospitales	No aplica		
Investigadores privados	No aplica		
Entidad de evaluación de información crediticia	No aplica		
Entidad de evaluación de fraude	No aplica		
Entidad financiera	No aplica		
Empleador	Aplica	Significativamente mitigado	1. Convenios de confidencialidad. 2. Politicas, procedimientos y manual de seguridad de informacion T. I. 3. Aceptacion de tratamiento de datos del titular; 4.Procedimiento de gestion documental de archivo y eliminacion
Proyectos de investigación	No aplica		
Ensayos clínicos	No aplica		

Reiniciar Atras Siguiente

Factores de riesgo que se derivan del contexto en el que se realizan las comunicaciones de datos a terceros en el marco del tratamiento.

COMUNICACIONES DE DATOS

	Aplicabilidad del riesgo	Mitigación	Medida de control / indicador de cumplimiento
Transferencia habitual a estados u organizaciones en otros países sin un adecuado nivel de protección	No aplica		
Falta de transparencia de los actores involucrados en el tratamiento	No aplica		

Reiniciar Atras Siguiente

OTROS FACTORES DE RIESGO ESPECÍFICOS DEL TRATAMIENTO

	Aplicabilidad del riesgo	Probabilidad	Impacto	Mitigación	Medida de control / indicador de cumplimiento
Pérdida de información en archivos físicos o digitales	Aplica	Baja	Limitado	Significativamente mitigado	1. Politicas, procedimientos y manual de seguridad de informacion T. I. 2.Procedimiento de gestion documental de archivo y eliminacion
Prolongado almacenamiento de archivos físicos o digitales	Aplica	Baja	Limitado	Significativamente mitigado	1. Convenios de confidencialidad. 2. Politicas, procedimientos y manual de seguridad de informacion T. I. 3. Aceptacion de tratamiento de datos del titular; 4.Procedimiento de gestion documental de archivo y eliminacion
Introduce breve descripción del factor de riesgo					
Introduce breve descripción del factor de riesgo					
Introduce breve descripción del factor de riesgo					
Introduce breve descripción del factor de riesgo					
Introduce breve descripción del factor de riesgo					
Introduce breve descripción del factor de riesgo					
Introduce breve descripción del factor de riesgo					
Introduce breve descripción del factor de riesgo					

Reiniciar | Atras | Siguiente

SEGURIDAD EN LOS TRATAMIENTOS

	Aplicabilidad del riesgo	Probabilidad	Impacto	Mitigación	Medida de control / indicador de cumplimiento
Pérdida de confidencialidad	Aplica	Baja	Limitado	Significativamente mitigado	1. Convenios de confidencialidad. 2. Politicas, procedimientos y manual de seguridad de informacion T. I. 3. Aceptacion de tratamiento de datos del titular; 4.Procedimiento de gestion documental de archivo y eliminacion. 5.Clausulas para contratistas con el cumplimiento del tratamiento de datos
Pérdida de integridad	Aplica	Baja	Limitado	Significativamente mitigado	1. Convenios de confidencialidad. 2. Politicas, procedimientos y manual de seguridad de informacion T. I. 3. Aceptacion de tratamiento de datos del titular; 4.Procedimiento de gestion documental de archivo y eliminacion. 5.Clausulas para contratistas con el cumplimiento del tratamiento de datos
Pérdida de disponibilidad	Aplica	Baja	Significativo	Significativamente mitigado	1. Convenios de confidencialidad. 2. Politicas, procedimientos y manual de seguridad de informacion T. I. 3. Aceptacion de tratamiento de datos del titular; 4.Procedimiento de gestion documental de archivo y eliminacion.
Pérdida de trazabilidad	Aplica	Baja	Limitado	Significativamente mitigado	1. Convenios de confidencialidad. 2. Politicas, procedimientos y manual de seguridad de informacion T. I. 3. Aceptacion de tratamiento de datos del titular; 4.Procedimiento de gestion documental de archivo y eliminacion.
Pérdida de autenticidad	No aplica				
Deficiencias en resiliencia	No aplica				
Fallos en medidas y garantías técnicas de protección de datos	Aplica	Baja	Limitado	Significativamente mitigado	1. Convenios de confidencialidad. 2. Politicas, procedimientos y manual de seguridad de informacion T. I. 3. Aceptacion de tratamiento de datos del titular; 4.Procedimiento de gestion documental de archivo y eliminacion. 5.Clausulas para contratistas con el cumplimiento del tratamiento de datos
Errores en las operaciones técnicas de tratamiento	Aplica	Baja	Limitado	Significativamente mitigado	1. Convenios de confidencialidad. 2. Politicas, procedimientos y manual de seguridad de informacion T. I. 3. Aceptacion de tratamiento de datos del titular; 4.Procedimiento de gestion documental de archivo y eliminacion. 5.Clausulas para contratistas con el cumplimiento del tratamiento de datos

ANEXO 3
ESQUEMA DEL PLAN DE CUMPLIMIENTO DEL DPD – FASE PREVENTIVA

ESQUEMA DEL PLAN DE CUMPLIMIENTO DEL DPD – FASE CORRECTIVA

ANEXO 4

Propuesta del Plan de Cumplimiento para el Delegado de Protección de Datos Personales

AREA Responsable	AREA Corresponsables	FINALIDAD - NATURALEZA	CUMPLIMIENTO NORMATIVO	CONSECUENCIA INFRACCIÓN
OPERACIONES	N/A	Acciones del Comité Ejecutivo: Aprobar proyecto Designar responsables del EQUIPO DE GESTIÓN DE PROYECTO Y RESPONSABLES POR COMPONENTES Seguimiento de avance de proyecto Aprobar recursos Aprobar acompañamiento especializado para la puesta en marcha del plan de implementación Priorizar actividades	Art. 68.- Infracciones graves del Responsable de protección de datos. Se consideran infracciones graves las siguientes: 1) No implementar medidas administrativas, técnicas y físicas, organizativas y jurídicas, a fin de garantizar el tratamiento de datos personales que realice conforme la presente ley, su reglamento, directrices, lineamientos y regulaciones emitidas por la Autoridad de Protección de Datos Personales y normativas sobre la materia.	Sanción: Del 0,7 al 1% del volumen de negocio (ingresos brutos del año anterior)
DPO/Compliance, BI, OPT	Responsables por componente	Acciones de responsables de gestión de proyecto: Diseñar y estructurar proyecto y sus componentes Proponer responsables por componentes Presentar informes de avance de proyecto Gestionar recursos Proponer priorización de actividades Capacitar y actualizar en la materia al delegado de protección de datos personales. Acompañamiento y entrenamiento al equipo de protección de datos personales a lo largo de la implementación Evaluación sobre la necesidad de obtener certificaciones en protección de datos.	Art. 68.- Infracciones graves del Responsable de protección de datos. Se consideran infracciones graves las siguientes: 1) No implementar medidas administrativas, técnicas y físicas, organizativas y jurídicas, a fin de garantizar el .tratamiento de datos personales que realice conforme la presente ley, su reglamento, directrices, lineamientos y regulaciones emitidas por la Autoridad de Protección de Datos Personales y normativas sobre la materia. Art. 23, art. 47,numeral 13 y art. 49 Ley Orgánica de Protección de Datos Personales	Del 0,7 al 1% del volumen de negocio (ingresos brutos del año anterior)
DPO- Comité de gestión de protección de datos de datos personales (DPO/Compliance, BI, OPT (Negocio y Procesos), Legal, Talento Humano, IT, Seguridad Digital, Tuenti)	DPO (ODPO/OCompliance), BI, OPT (Negocio y Procesos), Legal, Talento Humano, IT, Seguridad Digital, Tuenti	Creación del sistema de gestión de protección de datos personales (estructura, seguimiento y controles). Levantar un procedimiento para el desarrollo del registro de actividades de tratamiento, su actualización y su respectivo monitoreo. Definir directrices, políticas y procesos del sistema de gestión de protección de datos personales (roles, responsabilidades por áreas, registro de actividades de tratamiento, PIAS, gestión de riesgos, evaluación de impacto medidas de control, medidas de seguimiento) Identificación de áreas de riesgo (Atención al cliente, Negocios, BI, Prepago, Tuenti, etc.) Perfiles de puesto con asignación de nuevas funciones. Diseño del programa de sensibilización, concienciación y formación permanente Crear en la estructura interna la independencia de la oficina de DPO y Compliance (Informe del perfil del Delegado de Protección de Datos Personales y nombrar al delegado mediante nombramiento) Elaborar guías orientadas a trabajadores, según sus roles específicos. Incluir en las distintas políticas un mecanismos de recopilación de lecciones aprendidas respecto de la revisión y auditorías implementadas.	Art. 68.- Infracciones graves del Responsable de protección de datos. Se consideran infracciones graves las siguientes: 1) No implementar medidas administrativas, técnicas y físicas, organizativas y jurídicas, a fin de garantizar el .tratamiento de datos personales que realice conforme la presente ley, su reglamento, directrices, lineamientos y regulaciones emitidas por la Autoridad de Protección de Datos Personales y normativas sobre la materia.	Del 0,7 al 1% del volumen de negocio (ingresos brutos del año anterior)
BUSINESS INTELIGENCE	BI, Procesos, Legal, IT, seguridad, Compras, DPO, Talento Humano, B2C, B2B.	Creación estructura de gobierno de protección de datos Identificación de riesgo de gobierno de datos Gestionar los flujos de información y su relacionamiento (Inventario de repositorios digitales y físicos, inventario de datos, proveedores, entidades relacionadas, etc.) Definir los Roles para gestionar los flujos de información y su relacionamiento (data owners y data steward) Denifir estándares de protección de datos personales en el ciclo de vida del dato (Directrices de finalidades, calidad, minimización, conservación, eliminación, acceso, rectificación,actualización, oposición, portabilidad, perfilamientos, decisiones automatizadas, adquisiciones, transferencias, comunicaciones y cesiones, nonimización, responsabilidad proactiva y demostrada). Definir los campos el registro de actividades de tratamiento y su gestión por parte de los responsables del área (Elementos de datos, atributos, inventarios, catálogo, clasificación de datos personales, metadatos, conservación, eliminación, etc.) DEFINIR DATA SET: ARSO+, encargados de tratamiento (proveedores, distribuidores). Levantar registros de actividad de tratamiento usando PRIVATECA. Levantar los riesgos de cada actividad de tratamiento usando PRIVATECA. Levantar los controles de cada actividad de tratamiento usando PRIVATECA. Definir las responsabilidades de OTECEL S.A. como encargado de tratamiento Definir los RF Definir proceso y crear política para el monitoreo de flujo de datos personales en conexiones punto a punto Diseñar y manterner el reporte y actualización de registro nacional de protección de datos personales. Analizara los retos relativos a Tuenti, Prepago, Histórico de información y como punto de inflección desde la vigencia del régimen sancionatorio de la ley: campaña masiva de identidad y consentimiento y calidad.	Art. 68.- Infracciones graves del Responsable de protección de datos.Se consideran infracciones graves las siguientes: 1) No implementar medidas administrativas, técnicas y físicas, organizativas y jurídicas, a fin de garantizar el .tratamiento de datos personales que realice conforme la presente ley, su reglamento, directrices, lineamientos y regulaciones emitidas por la Autoridad de Protección de Datos Personales y normativas sobre la materia. 2) Utilizar información o datos para fines distintos a los declarados; 3) Ceder o comunica: datos personales sin cumplir con los requisitos y procedimientos establecidos en ja presente ley y su reglamento, directrices lineamientos y regulaciones emitidas por la Autoridad de Protección de Datos Personales y normativas sobre la materia, 4) 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; 5) No realizar evaluaciones de impacto al tratamiento de datos en los casos en que era necesario realizarlas; 6) 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; 7) 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; 8) No notificar a la Autoridad de Protección de Datos Personales del titular las vulneraciones de seguridad y protección de datos personales, cuando exista afectación a los derechos	**Actual:** **COIP (delitos de violación a la intimidad y revelación ilegal de bases de datos)** **Acciones de protección (reparación integral)** **Habeas Data (reparación integral)** **Daños y perjuicios** **Daño moral** **A partir de 26-05-2023** **Multa: Del 0,7 al 1% del volumen de negocio (ingresos brutos del año anterior)** **Considerar medidas correctivas, reiteración, reincidencia e individualización de infracciones** **Considerar negligencia y dolo**
OPERACIONES TRANSVERSALES	Procesos, legal, IT, seguridad, DPO, Talento Humano	Diseñar e implementar canales informativos, de comunicación y consulta de los interesados para que estos conozcan y puedan ejercer sus derechos. Diseño de políticas y procesos para atender derechos ARSO+ a través de los canales disponibles Diseñar e implementar canales informativos, de comunicación y consulta con el delegado de protección de datos personales con relación al tratamiento de sus datos personales a fin de ejercer sus derechos. Diseñar RF Diseñar proceso de capacitación permanente.	Art. 67.- Infracciones leves del Responsable de protección de datos.Se consideran infracciones leves las siguientes: 1. No tramitar, tramitar fuera del término previsto o negar injustificadamente las peticiones o quejas realizadas por el titular; Art. 68.- Infracciones graves del Responsable de protección de datos.Se consideran infracciones graves las siguientes: 1) No implementar medidas administrativas, técnicas y físicas, organizativas y jurídicas, a fin de garantizar el .tratamiento de datos personales que realice conforme la presente ley, su reglamento, directrices, lineamientos y regulaciones emitidas por la Autoridad de Protección de Datos Personales y normativas sobre la materia. 2) Utilizar información o datos para fines distintos a los declarados; 3) Ceder o comunica: datos personales sin cumplir con los requisitos y procedimientos establecidos en ja presente ley y su reglamento, directrices lineamientos y regulaciones emitidas por la Autoridad de Protección de Datos Personales y normativas sobre la materia, 4) 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; 5) No realizar evaluaciones de impacto al tratamiento de datos en los casos en que era necesario realizarlas; 6) 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;	**Del 0,7 al 1% del volumen de negocio (ingresos brutos del año anterior)**
Legal	Procesos, legal, IT, seguridad, Talento Humano, DPO	Diseñar el proceso de elaboración y actualización de política de protección de datos, consentimiento informados, cláusulas, adendas, convenios, etc. Levantar un reglamento general interno de protección de datos personales. Diseñar la gestión de los DPA e instrumentos jurídicos (directrices de reportería de los DPAs que no pasen por Legal, diseño de repositorio para seguimiento de encargados) Alinear los objetivos de negocio a protección de datos personales, a través del desarrollo de una política general de protección de datos personales Generación de la política de protección de datos personales y de cookies para sitio web y aplicaciones Incluir avisos de protección de datos personales y disclaimers para recopilar autorización para el tratamiento de datos personales Generar roles de acceso y actualizar convenios de confidencialidad con perspectiva de la Ley Orgánica de Protección de Datos Personales Generación de la política de protección de datos personales para proveedores y distribuidores	Art. 68.- Infracciones graves del Responsable de protección de datos.Se consideran infracciones graves las siguientes: 1) No implementar medidas administrativas, técnicas y físicas, organizativas y jurídicas, a fin de garantizar el .tratamiento de datos personales que realice conforme la presente ley, su reglamento, directrices, lineamientos y regulaciones emitidas por la Autoridad de Protección de Datos Personales y normativas sobre la materia. 2) Utilizar información o datos para fines distintos a los declarados; 3) Ceder o comunica: datos personales sin cumplir con los requisitos y procedimientos establecidos en la presente ley y su reglamento, directrices lineamientos y regulaciones emitidas por la Autoridad de Protección de Datos Personales y normativas sobre la materia, 4) 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; 5) No realizar evaluaciones de impacto al tratamiento de datos en los casos en que era necesario realizarlas; 6) 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; 7) 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; 8) No notificar a la Autoridad de Protección de Datos Personales del titular las vulneraciones de seguridad y protección de datos personales, cuando exista afectación a los derechos	**Del 0,7 al 1% del volumen de negocio (ingresos brutos del año anterior)**
Seguridad digital	Procesos, legal, seguridad, IT, Talento Humano, DPO	Analizar y ejecutar el análisis del alcance del SGSI Inventario de Gestión de incidentes de violación de datos personales para reporte a autoridad y a clientes, gestión de riesgos Actualización del proceso de seguridad de redes y comunicaciones sobre transferencia o comunicación de datos personales que incluya el almacenamiento y consulta de bases de datos de terceros. Diseñar elaborar la metodología de gestión de riesgos, amenazas, vulnerabilidades y violaciones de datos personales Diseño de controles a proveedores actuales para garantizar el cumplimientos de los DPA y 3PS. Diseñar e implementar un procedimiento de notificación de violaciones de protección de datos personales para la Superintendencia de protección de datos personales y/o a lo clientes. Diseñar e implementar un instructivo que los encargados de tratamiento deben cumplir para notificar a la organización de los eventos, incidentes, vulnerabilidades y violaciones de protección de datos personales.	Art. 68.- Infracciones graves del Responsable de protección de datos.Se consideran infracciones graves las siguientes: 1) No implementar medidas administrativas, técnicas y físicas, organizativas y jurídicas, a fin de garantizar el .tratamiento de datos personales que realice conforme la presente ley, su reglamento, directrices, lineamientos y regulaciones emitidas por la Autoridad de Protección de Datos Personales y normativas sobre la materia. 2) Utilizar información o datos para fines distintos a los declarados; 3) Ceder o comunica: datos personales sin cumplir con los requisitos y procedimientos establecidos en ja presente ley y su reglamento, directrices lineamientos y regulaciones emitidas por la Autoridad de Protección de Datos Personales y normativas sobre la materia, 4) 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; 5) No realizar evaluaciones de impacto al tratamiento de datos en los casos en que era necesario realizarlas; 6) 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; 7) 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; 8) No notificar a la Autoridad de Protección de Datos Personales del titular las vulneraciones de seguridad y protección de datos personales, cuando exista afectación a los derechos	**Del 0,7 al 1% del volumen de negocio (ingresos brutos del año anterior)**