Universidad Continental

FACULTAD DE DERECHO

Escuela Académico Profesional de Derecho

Tesis

La vulneración de los datos personales por parte de los establecimientos de salud y servicios médicos de apoyo en Lima - Perú, 2020-2021

Ana Ruth Natsumi Ames Carrion
Julio Adrian Delgado Conislla
Andalucia Marife Mendoza Torres

Para optar el Título Profesional de Abogado

Huancayo, 2024

INFORME DE CONFORMIDAD DE ORIGINALIDAD DE TRABAJO DE INVESTIGACIÓN

A	:	Eliana Carmen Mory Arciniega Decana de la Facultad de Derecho
DE	:	Martha Silvia Rivera Ricapa Asesor de tesis
ASUNTO	:	Remito resultado de evaluación de originalidad de trabajo de investigación
FECHA	:	22 de Julio de 2024

Con sumo agrado me dirijo a vuestro despacho para informar que, en mi condición de asesor del trabajo de investigación:

Título:
La vulneración de los datos personales por parte de los establecimientos de salud y servicios médicos de apoyo en Lima-Perú 2020-2021

Autores:
Ana Ruth Natsumi Ames Carrion – EAP. Derecho
Julio Adrian Delgado Conislla – EAP. Derecho
Andalucia Marife Mendoza Torres – EAP. Derecho

Se procedió con la carga del documento a la plataforma "Turnitin" y se realizó la verificación completa de las coincidencias resaltadas por el software dando por resultado 20 % de similitud sin encontrarse hallazgos relacionados a plagio. Se utilizaron los siguientes filtros:

- Filtro de exclusión de bibliografía — SI [x] NO [ ]
- Filtro de exclusión de grupos de palabras menores — SI [x] NO [ ]
  Nº de palabras excluidas **(20)**:
- Exclusión de fuente por trabajo anterior del mismo estudiante — SI [ ] NO [x]

En consecuencia, se determina que el trabajo de investigación constituye un documento original al presentar similitud de otros autores (citas) por debajo del porcentaje establecido por la Universidad Continental.

Recae toda responsabilidad del contenido del trabajo de investigación sobre el autor y asesor, en concordancia a los principios expresados en el Reglamento del Registro Nacional de Trabajos conducentes a Grados y Títulos – RENATI y en la normativa de la Universidad Continental.

Atentamente,

La firma del asesor obra en el archivo original
(No se muestra en este documento por estar expuesto a publicación)

Dedicatoria

Dedicado a mis padres y a pelusita, por su constante apoyo y motivación. Gracias por confiar en mí y siempre alentarme a cumplir mis sueños. Fueron mi soporte en este camino largo.

Ana

Dedico esta tesis a mis seres queridos, quiénes han sido mi motivación y pilar para poder seguir adelante en todo momento.

Julio

Esta tesis va dedicada a mis familiares y hermanas, quiénes me enseñan sobre la disciplina y constancias para alcanzar mis metas.

Andalucia

Agradecimiento

Agradecer a Dios y a nuestras familias por apoyarnos en todo momento; asimismo, como autores de la tesis, resaltar nuestro esfuerzo, dedicación y esmero. Destacamos, también, el apoyo de todas aquellas personas que nos han animado y motivado en este camino.

Ana, Julio y Andalucia

Tabla de Contenido

Lista de Tablas

Lista de Figuras

Acrónimos y Abreviaturas

AEPD	Agencia Española de Protección de Datos
ANPD	Autoridad Nacional de Protección de Datos Personales
Art.	Artículo
DGTAIPD	Dirección General de Transparencia, Acceso a la Información Pública y Protección de Datos Personales
DFI	Dirección de Fiscalización e Instrucción
DPDP	Dirección de Protección de Datos Personales
DSC	Dirección de Supervisión y Control
Exp.	Expediente
FTC	Federal Trade Commission
INDECOPI	Instituto Nacional de Defensa de la Competencia y de la Protección de la Propiedad Intelectual
LPDP	Ley de Protección de Datos Personales
LPAG	Ley del Procedimiento Administrativo General
MINJUS	Ministerio de Justicia y Derechos Humanos
NRPDP	The National Registry for the Protection of Personal Data
PAS	Procedimiento Administrativo Sancionador
RNPDP	Registro Nacional de Protección de Datos Personales
RD	Resolución Directoral
RLPDP	Decreto Supremo N° 003-2013-JUS
RAE	Real Academia Española
Resol.	Resolución
SIPDP	Sistema Integrado de Protección de Datos Personales
TC	Tribunal Constitucional
UIT	Unidad Impositiva Tributaria

Resumen

La presente tesis tiene como objetivo principal describir la situación de vulneración que se produce por la deficiente protección de datos personales y sensibles que se encuentran almacenados en los bancos de datos dentro de los establecimientos de salud y servicios médicos de apoyo, con base en las resoluciones emitidas por la "Autoridad Nacional de Protección de Datos Personales" (en adelante, ANPD). En esta misma línea, la metodología utilizada es la descriptiva – analítica, puesto que se han recolectado documentos para el análisis; por otro lado, el resultado de la presente investigación se enfoca en demostrar los criterios relacionados con la gestión de datos: transparencia, confidencialidad y seguridad de datos personales que contienen información sensible que tiene la ANPD al momento de emitir una resolución sancionadora. La conclusión principal destaca que la ANPD se centra en criterios relacionados con el uso no autorizado y la falta de consentimiento respecto al tratamiento de datos personales almacenados en las bases de datos que se utilizan en el ámbito de salud. De las revisiones de las 17 resoluciones, el 32 % y 24 % de estas, que tienen el índice más alto de análisis, se sustentan en los criterios del deber de informar sobre el tratamiento de datos personales/sensibles y cumplir con las medidas de seguridad para el tratamiento de datos personales/sensibles; mientras que el 10 % y 05 % corresponden a los criterios menos analizados: comunicar el uso del flujo transfronterizo a la DGTAIPD y deber de confidencialidad sobre los datos personales.

Palabras clave: Datos personales, datos sensibles, derecho a la intimidad, derecho a la privacidad, ANPD, autodeterminación informativa.

Abstract

The primary aim of this thesis is to elucidate the vulnerability resulting from inadequate protection of personal and sensitive data housed in databases within healthcare institutions and medical support services, as outlined by resolutions from the National Registry for the Protection of Personal Data (hereinafter "NRPDP"). Employing a descriptive-analytical methodology, we gathered relevant documents for analysis. Our research primarily focuses on elucidating the criteria pertaining to data management, namely transparency, confidentiality, and security of personal data, including sensitive information, as delineated by the NRPDP in its sanctioning resolutions. The principal finding of our study underscores the NRPDP's emphasis on criteria related to unauthorized usage and lack of consent in processing personal data stored in healthcare sector databases. Upon reviewing the 17 resolutions, it was found that 32% and 24% of them, which received the most attention, are centered on the obligation to disclose how personal/sensitive data is being processed and ensuring compliance with security measures for handling such data. Meanwhile, only 10% and 5% of the resolutions focused on less scrutinized aspects, specifically communicating the use of cross-border data transfer to the FTC and upholding confidentiality duties regarding personal data.

Keywords: personal data, sensitive data, right to privacy, right to intimacy, NRPDP, information self-determination.

Introducción

Día a día, la información circula de diversas maneras, y en el caso de los establecimientos de salud y servicios médicos de apoyo, la información es solicitada para generar una historia clínica física o virtual con el fin de tratar a los pacientes de manera eficaz, recabándose sus datos personales y sensibles; sin embargo, existen diversas situaciones a partir de las cuales se puede apreciar el mal uso y la deficiente protección de información revelada, siendo usada para otorgarse, venderse y/o ser robada por terceros. “Los sistemas de información deben ser seguros para los pacientes y profesionales de salud. Cuando nos referimos a los pacientes, la seguridad se relaciona con el adecuado resguardo, disponibilidad y acceso de los datos personales” (Curioso & Espinoza, 2015, p. 338).

En estos casos, se encuentra el caso de la RD N.º 1885-2020-JUS/DGTAIPD-DPDP del 30 de octubre de 2020; además de la RD N.º 1436-2021-JUS/DGTAIPD-DPDP del 02 de junio de 2021, que fueron primordiales para la investigación; asimismo, se pudo identificar el uso indebido de los datos otorgados por los usuarios por parte de los establecimientos de salud y servicios médicos de apoyo.

En la misma línea, el problema persistente radicó en que los datos compartidos con instituciones, como centros educativos, compañías de seguros, servicios de salud, entre otros, suelen ser recopilados por terceros no relacionados con estas instituciones.

Este proceso viola el derecho a la privacidad e intimidad de las personas, vulneración que se vuelve aún más preocupante en el ámbito de la salud, donde la información proporcionada suele ser más detallada y específica para recibir atención médica.

En el contexto de la salud, la información revelada puede abarcar aspectos económicos, familiares y detalles específicos sobre el estado de salud, siendo considerada como datos sensibles. Esta situación resaltó la delicadeza y el valor de esta información, la cual debería

manejarse con una protección aún mayor debido a su naturaleza confidencial y debido al potencial daño que podría acarrear su uso indebido o no autorizado.

El propósito de esta investigación fue analizar cómo el derecho a la intimidad y privacidad se vio afectado por el mal uso de la información por parte de los establecimientos de salud y servicios médicos de apoyo en Lima-Perú, durante el período 2020-2021. Se estudió la protección que brinda la LPDP, la cual tuvo como objetivo resguardar el sistema de almacenamiento, registro y transmisión de datos personales, a fin de salvaguardar uno de los derechos fundamentales más importantes establecidos en el art. 2, inciso 6) de la Constitución Política del Perú: proteger y preservar, respecto al uso de información computarizada e informática en establecimientos públicos y privados, la intimidad personal y familiar frente a usos inadecuados que puedan realizar los establecimientos de salud y servicios médicos de apoyo.

Es fundamental destacar que este estudio tiene como objetivo contribuir con nuevos conocimientos sobre la aplicación actual del registro de banco de datos en la RNPDP. Además, se demostró cómo se vieron afectados los datos personales y sensibles en los establecimientos que ofrecen servicios de salud. Teniendo clara su finalidad, la presente tesis sigue la siguiente estructura:

En el primer capítulo, titulado *Planteamiento del problema de investigación*, se identificó el problema que guía la tesis, incluyendo sus problemas específicos. Se proporciona una explicación detallada sobre cómo se formula el problema; asimismo, los objetivos tanto generales como específicos, además de presentarse la justificación del problema junto con las hipótesis. Todos estos elementos sirvieron como guía y fundamento para la investigación.

El segundo capítulo expone la elaboración del marco teórico, abarcando la recopilación de antecedentes a nivel internacional y nacional previos al trabajo de investigación en cuestión.

Luego, se procedió al desarrollo del marco teórico propiamente dicho, el cual se estructura en subcapítulos:

El primer subcapítulo, titulado *Derecho a la Intimidad*, aborda el concepto, origen, definiciones y la importancia de este derecho. El objetivo de este subcapítulo es proporcionar al lector información detallada para que pueda comprender plenamente la relevancia del derecho a la intimidad en el contexto de la investigación.

El segundo subcapítulo, titulado *Derecho a la privacidad*, se fundamenta en el origen y la importancia de este derecho, estableciendo su relevancia dentro de la presente investigación. El objetivo es sumergir al lector en el contexto del estudio, ofreciendo un análisis de este, su origen y destacando su importancia en el marco de la presente investigación.

El tercer subcapítulo, titulado *Derecho de protección de datos personales*, expone el origen, concepto y evolución a través del tiempo. Se enfoca en resaltar la importancia y la relevancia de salvaguardar esta información. El propósito es subrayar ante el lector la trascendencia de la protección de los datos personales.

Respecto al cuarto subcapítulo, titulado *La protección de los datos personales y la autodeterminación informativa en el Perú*, se desarrolla la connotación histórica de la autodeterminación informativa en el Perú. El objetivo es brindar más información respecto a este punto, el cual tiene una relación importante con el tema de investigación.

El quinto subcapítulo, titulado *ANPD*, se adentra en el origen, definición, funciones y mecanismos de esta entidad. Su propósito es informar sobre las competencias que posee y cómo las aplica en su quehacer diario. Este apartado busca resaltar la importancia de esta entidad en el contexto de la presente investigación.

El sexto subcapítulo, titulado *Establecimientos de salud y los protocolos de protección de datos personales*, desarrolla el concepto, legislación y directivas que salvaguardan los datos personales de los usuarios que son recopilados por los establecimientos de salud. Se analiza

cómo gestionan la información personal y qué protocolos de protección se tienen en vigor. El propósito es proporcionar al lector una comprensión detallada sobre la relación entre los establecimientos de salud y el tema de investigación, otorgando un rol central a estos entornos dentro del contexto del estudio.

El séptimo y último subcapítulo, titulado *Indecopi y las sanciones por vulneración al derecho de la privacidad*, resume y analiza cinco resoluciones en las que esta entidad impone sanciones, instruye y corrige acciones que afectan este derecho, siendo el propósito examinar cómo Indecopi aplica sanciones a entidades ajenas al ámbito de los servicios de salud, proporcionando una visión amplia respecto a la vulneración de datos personales que no se encuentra limitada únicamente al ámbito de salud. Se demostró que, aunque estas entidades no manejen datos sensibles como los establecimientos de salud, la protección de la privacidad sigue siendo relevante en múltiples contextos.

El Capítulo III se enfocó en la exposición de la metodología de la investigación. En este contexto, se abordaron aspectos relacionados con el enfoque, tipo, nivel de la investigación, población y muestra, así como las técnicas e instrumentos de recolección de datos.

En el Capítulo IV, se desarrollaron los resultados, continuando la secuencia propuesta por las preguntas planteadas. Al final, se contrastó la hipótesis teniendo en cuenta la información analizada y recopilada de las resoluciones de la ANPD.

En el capítulo V, se mostró que los bancos de datos, al ser inicialmente registros de declaración jurada, carecen de un nivel inicial de protección. En este sentido, se propuso una adición normativa que implemente un filtro para una fiscalización más efectiva. Esta medida pretende ser preventiva, evitando así que se afecte el derecho a la intimidad y privacidad.

El alcance de este estudio comprendió una evaluación detallada de la seguridad en la recopilación y gestión de datos sensibles en entornos médicos, centrándose en aspectos como la protección, accesibilidad y disponibilidad de esta información. Se llevo a cabo un análisis

exhaustivo de las resoluciones directivas para comprender su relevancia y aplicabilidad en el resguardo de los datos en el ámbito de la salud. Además, se examinaron casos específicos que ilustren el manejo deficiente de los datos realizados por los establecimientos médicos, reconociendo así que el intercambio no autorizado de datos en servicios de salud afecta la privacidad de las personas, especialmente en el contexto de la atención médica. Este estudio tuvo como objetivo ofrecer una visión completa sobre la protección de datos en el campo de la salud y su impacto en el derecho fundamental a la intimidad.

La investigación enfrentó límites significativos, como la restricción en el acceso a información detallada sobre casos específicos de mal uso de datos, debido a su carácter confidencial. Además, la complejidad legal y ética asociada con el manejo de datos médicos limitó la profundidad del análisis de sus implicaciones. También se encontraron limitaciones en la identificación y obtención de datos sobre terceros que recopilan información de instituciones médicas, debido a la falta de transparencia en estas prácticas, lo cual delimitó la presente investigación.

Capítulo I. Planteamiento del Estudio

1.1. Planteamiento del Problema de Investigación

La vulneración de datos personales, como señala Bruce Schneier, se ha convertido en una de las principales preocupaciones en la era de la información, donde la tecnología ha elevado el valor de nuestros datos personales como nunca. En la actualidad, al interactuar con diversos servicios de atención al cliente, las personas se enfrentan a la constante solicitud de datos personales necesarios para la prestación de servicios solicitados.

Este fenómeno se ha intensificado significativamente durante la pandemia, ya que muchos servicios migraron al espacio virtual para adaptarse a las restricciones de contacto físico. La recolección de datos personales se ha vuelto habitual a través de formularios, chats, mensajes, entre otros, y son dirigidos a bancos de datos que se encargan de resguardar y proteger la información. En consecuencia, cada servicio está obligado a cumplir con los requisitos establecidos por la ANPD para la inscripción del banco de datos en el RNPDP.

En este sentido, la falta de un control efectivo o protección adecuada de los bancos de datos en diversos establecimientos que ofrecen servicios, exponen a una mayor vulnerabilidad en el manejo de nuestros datos sin nuestro consentimiento. Esta situación es evidente en diferentes ámbitos, como la educación, el sector financiero, el ámbito de la salud, espacios que requieren constantemente información personal.

Por tanto, es relevante examinar minuciosamente el ámbito de la salud, ya que se ven comprometidos los datos personales y los datos sensibles. Estos últimos son extremadamente íntimos, y la gran mayoría, por no decir todas las personas, desea que esta información no sea revelada a terceros, dado que su divulgación puede tener diversas repercusiones que afectan la vida íntima.

En la actualidad, los establecimientos de salud y los servicios médicos de apoyo también se ven amenazados por terceros maliciosos que buscan obtener beneficios a través de

la vulneración de datos personales y sensibles. Estos actores logran su cometido al afectar directamente el banco de datos, donde convergen registros, historiales, informes y otros documentos relevantes.

Esta situación, sin embargo, no debería ocurrir, especialmente cuando se trata de datos sensibles, ya que se afecta un derecho fundamental: el de la intimidad. La protección adecuada de esta información es esencial para garantizar la confianza de los usuarios y pacientes en el sistema de salud y para cumplir con las normativas y estándares de privacidad establecidos por la ANPD y otros organismos regulatorios pertinentes.

Ante estos hechos, el Estado peruano brinda algunos requisitos para poder conformar un banco de datos cuyos requerimientos tienen carácter de declaración jurada. En esta línea, la administración pública posee la facultad de llevar a cabo fiscalizaciones posteriores, respaldada por el principio de presunción de veracidad sobre el administrado. Esta presunción permite realizar la fiscalización después de un periodo prolongado o, en los casos más críticos, cuando ya se han vulnerado los datos personales y sensibles del usuario.

Así, dado que la problemática central de esta investigación se enfoca en la descripción y análisis de las resoluciones emitidas por la ANPD con respecto a la vulneración de datos personales y sensibles en el ámbito de la salud, el estudio se concentrará exclusivamente en los establecimientos de salud y servicios médicos de apoyo. Además, se evaluará la viabilidad de establecer un filtro específicamente para estos, con el objetivo de prevenir la vulneración de datos personales y sensibles, y, por consiguiente, proteger el derecho fundamental a la intimidad.

1.2. Problema General

Considerando lo expuesto anteriormente, la pregunta principal que orienta esta investigación es:

¿Cuáles fueron los criterios de la ANPD para resolver casos de vulneración de datos personales en los establecimientos de salud y servicios médicos de apoyo de salud en 2020 y 2021?

1.2.1. Problemas Específicos

¿Cuáles son los hechos más frecuentes que fueron puestos en conocimiento de la ANPD en 2020 y 2021?

¿Cuál es la motivación de la ANPD en las resoluciones de los establecimientos de salud y servicios médicos de apoyo de salud en 2020 y 2021?

¿Cuál es la finalidad e importancia de graduar las sanciones y el cálculo de la multa en los fallos de las resoluciones emitidas por la ANPD en 2020 y 2021?

¿Cómo una propuesta legislativa de adición respecto a una función específica de la ANPD va a prevenir la vulneración de los datos personales/sensibles y los derechos fundamentales de sus titulares?

1.3. Objetivos de la Investigación

1.3.1 Objetivo General

Describir los criterios que tomó en cuenta la ANPD en las resoluciones de vulneración de datos personales en establecimientos de salud y servicios médicos de apoyo en 2020 y 2021.

1.3.2. Objetivos Específicos

Identificar los hechos más frecuentes que fueron puestos en conocimiento de la ANDP en 2020 y 2021.

Detallar la motivación de la ANDP en las resoluciones de los establecimientos de salud y servicios médicos de apoyo en 2020 y 2021.

Especificar la finalidad e importancia de graduar las sanciones y el cálculo de la multa en los fallos de las resoluciones emitidas por la ANDP en 2020 y 2021.

Establecer una propuesta legislativa con el fin de adicionar una función específica a la ANPD dentro del ámbito de la salud para prevenir la vulneración de los datos personales/sensibles y los derechos fundamentales de sus titulares.

1.4. Justificación

El presente tema es importante por la relevancia cotidiana que tienen los datos personales y sensibles en la vida de las personas. Estos datos son utilizados constantemente para acceder a una amplia gama de servicios, desde el ámbito educativo hasta compras físicas u online, y en la búsqueda de atención médica, lo cual revela información fundamental y privada. La recopilación y organización de estos datos se realiza con la finalidad de crear sistemas organizados que permitan el registro y seguimiento de trámites realizados por individuos. De esa manera, es importante sostener que "ya desde su inicio una parte de la concepción de la privacidad ha sido entendida como una forma de expresión de la primacía de los intereses individuales por sobre las pretensiones de la sociedad" (Corral, 2000).

Se observa que la vulneración de la protección de datos ocurre a través de los bancos de datos, lo que exige mayor rigurosidad en los requisitos para su creación. Esta investigación busca informar sobre cómo la ANPD resuelve casos relacionados con establecimientos de salud, destacando la importancia de la motivación para sancionar a los administrados. Además, se propone una adición legislativa para otorgar una nueva facultad, exclusivamente en el ámbito de la salud, a la ANPD.

El estudio pretende contribuir al avance en el conocimiento jurídico al explorar instituciones inversas como la protección de datos personales y analizar cómo la ANPD resuelve casos, promoviendo una evolución crítica en el manejo de los bancos de datos.

Los principales beneficiarios serán los usuarios de los establecimientos de salud, ya que contarán con una mayor protección de sus datos personales, lo cual generará confianza y

seguridad en la privacidad de estos. Asimismo, las empresas de salud se beneficiarán al recibir pautas para proteger y utilizar adecuadamente la información de sus usuarios.

Este estudio será de utilidad para los operadores del derecho, especialmente para la ANPD, al ofrecer una propuesta que podría prevenir la vulneración de datos personales y sensibles, y preservar el derecho fundamental a la intimidad.

En última instancia, la presente tesis ha profundizado en la importancia y las implicaciones de la gestión de datos personales en la era digital. Se ha explorado cómo la recopilación, el almacenamiento y el análisis de datos personales han transformado diversos aspectos de la sociedad, desde el comercio electrónico hasta la atención médica. Sin embargo, el campo de los datos personales es vasto y está en constante evolución, y aún quedan muchas áreas por explorar y comprender completamente. En este sentido, existe una gran oportunidad para futuras investigaciones que aborden diversos aspectos de la privacidad, la seguridad y la ética en el manejo de datos personales y sensibles. De esa manera, se busca que esta investigación inspire futuros estudios sobre la protección de datos personales y fomente el avance en este campo.

Capítulo II. Marco Teórico o Conceptual

2.1. Antecedentes del Problema

2.1.1. Antecedentes Internacionales

El estado actual del tema en cuestión tiene poca información de desarrollo; sin embargo, la manipulación de datos, tanto personales como sensibles, es necesaria para el día a día en los establecimientos de salud y servicios médicos de apoyo.

En su investigación, Piña (2021) aborda el desafío relacionado con el acceso y la protección de los datos personales en el sector público de la salud. Destaca la necesidad de que cualquier tratamiento de datos personales se ajuste a los principios, deberes y derechos establecidos en la normativa de protección de datos personales. Utilizando una metodología analítica, el autor concluye que las entidades del sector salud manejan una cantidad significativa de información que les proporciona un acceso rápido a datos; sin embargo, subraya la importancia de implementar mecanismos para proteger estos datos. Además, señala que las personas responsables del manejo de esta información deben adherirse a las normas para evitar infringir el derecho a la intimidad. Por otro lado, sostiene que las instituciones del sector salud deben establecer estándares adecuados para la protección de los datos personales en sus actividades diarias.

En la misma línea de investigación, Olvera (2017) tuvo como uno de sus objetivos caracterizar quiénes son las personas legitimadas para acceder a los datos personales de salud y esclarecer cuáles son las vías concretas por las normas correspondientes para el acceso de datos personales de la entidad legitimada en el sistema de México. La metodología utilizada fue descriptiva y las conclusiones principales a las que arribó el autor fueron: 1) señalar que no se encuentran protocolos de capacitación a quienes brindan atención médica; 2) los trabajadores de salud no disponen del respectivo conocimiento para brindar acceso de los

pacientes a su propia información, lo cual muestra la relevancia de la inclusión de los derechos ARCO en el sistema de salud.

2.1.2. Antecedentes Nacionales

Macutela (2020), en su investigación de especialización, refiere que el uso de sistemas de geolocalización y cámaras de lecturas de temperatura por medio de una metodología analítica descriptiva, tiene ahora una mayor importancia en la recopilación de datos personales y sensibles, por la misma coyuntura de la pandemia. Estos datos otorgados por los usuarios a establecimientos de salud, son datos sensibles y son usados para poder prevenir, diagnosticar y tratar enfermedades de interés público o salud pública; asimismo, los aportes entregados por la ANDP no representan un avance significativo para la protección de datos sensibles en el Perú.

Praeli (2015) manifiesta que la protección de datos personales es consagrada como derecho fundamental, por el mismo desarrollo de la sociedad y la tecnología. Su estudio buscó establecer, mediante la LPDP, una mejor protección al art. 2 inciso 6 de la Constitución. Además, el ente encargado de verificar, proteger y hacer respetar la intimidad de los datos personales es la ANPD.

Al respecto, se hará referencia a noticias relevantes relacionadas con el tema:

- Redacción Gestión (2020), en su noticia, refiere que la ANPD en 2020, época de pandemia, recaudó la suma total de S/. 970,853.90 en multas por infracciones a la LPDP, puesto que hubo una filtración de estos; asimismo, los sectores que cuenta con más denuncias, procesos sancionadores y sanciones efectivas son el financiero, telecomunicaciones y el de seguros.
- En su nota de prensa a través de ANPD, MINJUSDH (2020) brindó recomendaciones para que se evite la vulneración a la privacidad de pacientes con Covid-19; asimismo, enfatizó que compartir información sobre la salud de una persona, como identificarla

sin su consentimiento, es una infracción a la LPDP, y el infractor puede hacerse acreedor a una sanción con una multa. En esta misma línea, se recomendó proteger la identidad del paciente y que se limite el acceso público a información confidencial. Los establecimientos de salud deberán implementar medidas de seguridad óptimas para que esta información no recaiga en terceros no autorizados; además, se recordó que la única manera con la que se pueden revelar datos sensibles de un paciente es mediante su consentimiento, que debe ser previo, expreso, libre e informado. Se enfatiza que deberá ser por escrito. Los datos sensibles protegen datos íntimos y personales y su vulneración origina lesiones a los derechos y libertades de los pacientes.

Los trabajos de investigación mencionados tendrán una conexión directa con la presente tesis, ya que permitirá dotar de mayor respaldo la sustentación de las hipótesis referidas a las causales de la problemática planteada.

2.2. Bases Teóricas

A continuación, se presentan los fundamentos teóricos relevantes para esta tesis. Esta sección se organiza en siete subsecciones con el propósito de facilitar la comprensión y presentación de la investigación, lo cual permite realizar un análisis minucioso, estructurado y conciso.

2.2.1. El Derecho a la Intimidad

El término *right of privacy* fue desarrollado por Samuel Warren y Louis Brandeis, publicado en Harvard Law Review en 1890, surgiendo así el derecho a la intimidad a fines del siglo XIX en Estados Unidos. La presenta acosaba a Warren para saber sobre su vida conyugal, la cual está inmersa en su vida privada, todo ello sin su consentimiento; es así como se desarrolla de manera esencial la importancia respecto a los límites jurídicos que deben establecerse.

En su estudio da a conocer que ninguna persona puede entrometerse en la vida privada de un individuo sin su consentimiento. Además, se brinda una definición como aquel derecho que tiene todo persona sobre la seguridad personal, lo cual es aún más perjudicial cuando se inmiscuyen los medios de comunicación.

La sentencia de la Corte, que fue emitida por el Tribunal Supremo Norteamericano en el año 1965, definió al derecho a la privacidad como aquel derecho específico y autónomo de las personas, en relación con el derecho a la intimidad respecto a la preservación de la intimidad y la vida sexual.

William L. Prosser menciona que existen cuatro aspectos mediante los cuales se amplía la protección al derecho a la intimidad, a saber: "a) la apropiación de la imagen o identidad de una persona con el objetivo de obtener un beneficio; b) la publicidad que presenta al individuo de manera distorsionada ante el público (atribución falsa de una imagen para asociar falsamente a una persona con un hecho); c) la divulgación pública de hechos privados embarazosos sobre el individuo; y d) los actos de intromisión que perturban el retiro o la soledad del individuo (fisgoneo, persecución)".

En Europa, el Tribunal de Derechos Humanos conceptualiza el derecho a la intimidad como el disfrute de confidencialidad y retiro. Esto hace referencia a áreas de las cuales el individuo se puede excluir de los demás, lugares donde la información puede estar protegida de intrusiones no deseadas y lejos del ámbito público.

En España, Praeli (2016) menciona que los actos o hechos protegidos por la reserva de la intimidad o privacidad están supeditados necesariamente a su realización en lugares o escenarios privados, como el domicilio personal o familiar; también podrán tener similar carácter a pesar de verificarse en lugares públicos, tales como calles, plazas, restaurantes o locales donde no existen restricciones para el ingreso del público. Obviamente, el principio es que aquello que está vinculado a la intimidad se desarrolla en lugares privados y exentos del

acceso de extraños, pero debe admitirse que ciertos hechos deben conservar reserva y privacidad, y no ser divulgados, a pesar de verificarse en lugares públicos.

La Constitución de 1867 dio a conocer el derecho a la vida privada a través de su artículo 20, señalando:

> Todos pueden hacer uso de la imprenta para publicar sus escritos, sin censura previa y sin responsabilidad en asuntos de interés general. En las publicaciones sobre asuntos personales, se hará efectiva la responsabilidad de los autores y editores conforme a lo dispuesto, para esta clase de asuntos, en la ley que instituye el jurado. Toda publicación que ataque la vida privada de los individuos será firmada por su autor.

Por otra parte, la Constitución de 1979, en su art. 5 menciona:

> Al honor y la buena reputación, a la intimidad personal y familiar, y a la propia imagen. Toda persona afectada por afirmaciones inexactas o agraviada en su honor por publicaciones en cualquier medio de comunicación social, tiene derecho de rectificación en forma gratuita, sin perjuicio de la responsabilidad de ley.

En la Constitución de 1993, el derecho a la intimidad se encuentra consagrado en el inciso 7 del art. 2, que menciona lo siguiente: “Al honor y a la buena reputación, a la intimidad personal y familiar, así como a la voz y a la imagen propias”. En este sentido, se puede entender que el derecho a la intimidad personal y familiar resguarda la esfera privada mediante el cual el individuo puede desarrollar su personalidad de forma libre. Este derecho da la autonomía a cada persona para que pueda establecer los límites de exposición de su vida privada.

Existen dos vertientes del derecho a la intimidad: la primera es aquella potestad que tiene toda persona respecto a la información personal que va a compartir con terceros; la segunda se entiende como la capacidad de mantener reservados ciertos aspectos de la vida privada de la persona, sin compartirlo con otras personas.

La intimidad como derecho resguarda la esfera privada de cada individuo para sí mismo, incluyendo la conservación de la privacidad, la serenidad, la independencia para tomar decisiones y actuar. De la misma manera, el dominio de la información respecto a la vida privada de la persona debe mantenerse confidencial. El propósito de este derecho es prevenir que, tanto individuos como el Estado, violen esta esfera mediante intrusiones indebidas.

La RAE describe la intimidad como el espacio íntimo, ya sea de índole espiritual o física, que pertenece a una persona o a un conjunto de personas. De manera similar, define la privacidad como la característica de ser privado y no público, incluyendo el ámbito de la vida privada que merece ser resguardado de intrusiones no deseadas.

Sobre la base de estas diferencias, se puede deducir que este derecho se ve reflejado en un ámbito específico donde se desarrollan aspectos más reservados de la vida de un individuo. Esto contrasta con la privacidad, que engloba el ámbito general de la vida privada.

2.2.2. Derecho a la Privacidad

El derecho a la vida privada y a la intimidad es un derecho universal y se encuentra en la Declaración Universal de los Derechos Humanos de 1948, en el art. 12 que establece que "nadie será objeto de injerencias arbitrarias en su vida privada, su familia, su domicilio o su correspondencia, ni de ataques a su honra o a su reputación. Toda persona tiene derecho a la protección de la ley contra tales injerencias o ataques".

Puente (1980) señala que la privacidad es lo que una persona se reserva para sí, que no es lícito a los demás invadir; es todo lo que una persona puede sustraer del conocimiento de los demás".

En Estados Unidos la privacidad se encuentra regulada en la cuarta enmienda de la Constitución, la cual establece que:

> La privacidad solo se considera "fundamental" cuando se ve amenazada por un abuso gubernamental en el trato de la información personal y, por tanto, la ley federal

interviene solo frente a él o también cuando se trata de negocios que almacenan información personal sensible; salvadas estas circunstancias, la protección de los datos se considera un elemento disponible por parte de los ciudadanos.

En los Estados Unidos existe legislación estatal, sectorial y federal que regula ámbitos específicos de protección del *privacy right.*

En Europa, el derecho a la vida privada se encuentra fundamentado en el art. 8 del Convenio Europeo de Derechos Humanos de 1950, el cual garantiza el derecho a la vida privada y familiar como un derecho fundamental, y establece que "toda persona tiene derecho a que se respete su vida privada y familiar, de su domicilio y de su correspondencia".

En Latinoamérica se establece como derecho fundamental el *habeas data*, el cual protege los datos personales frente al método indebido o ilegal de conseguir los datos de carácter personal, que muchas veces son filtrados por bases de datos o archivos públicos y privados.

El derecho a la privacidad se entiende como aquella facultad libre que tiene toda persona en el desenvolvimiento de su personalidad, ya sea en un ámbito personal, familiar o social, de acuerdo a su conducta, hábitos o costumbres. Por lo que ninguna persona puede entrometerse o inmiscuirse en ella, sin la autorización de la persona misma; la persona podrá decidir en qué medida compartirá con los demás sus sentimientos, pensamientos o hechos de vida personal que incluyan información como la imagen, edad, sexo, nacionalidad, salud, hábitos sexuales, individualidad, voz, ideas religiosas, etc., datos que son considerados muy particulares de la persona.

2.2.3. Origen: Derecho a la Privacidad

Saldaña (2012) señala que la privacidad como concepto jurídico empieza en los años de 1960 en Norteamérica; sin embargo, el desarrollo que tuvo el derecho a la privacidad tiende a ser más histórico que dogmático. Se tiene a autores como Alan Furman Westin, quien considera a la privacidad como un derecho que tiene la facultad de poder controlar, gestionar, editar y eliminar información acerca de uno mismo, y decidir cómo, cuándo y en qué proporción se brinda la información a los demás. Asimismo, Thomas Cooley hizo referencia a *the right to be let alone*. En cuanto a Warren y Brandeis, definieron *the right to privacy* que dan comienzo al desarrollo de este derecho.

2.2.4. Protección de Datos Personales en el Marco del Derecho a la Privacidad

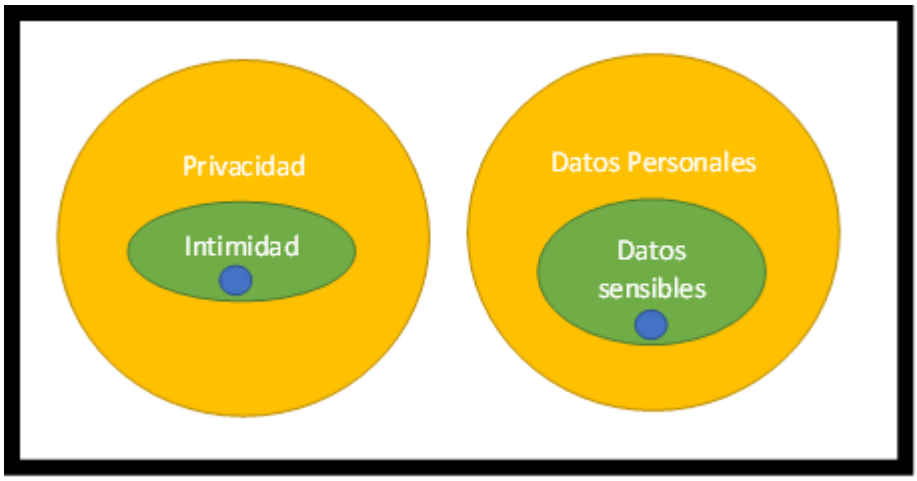
2.2.4.1. Repercusiones que Genera la Vulneración del Derecho a la Privacidad. Ahora bien, el daño una vez vulnerado el derecho a la privacidad es sumamente grave, puesto que esta información es personal y, en algunos casos, sensible, lo cual afecta no solo este derecho, sino también el derecho a la dignidad humana y al plan de vida. En otras legislaciones, como es el caso de España, se evita entregar información a terceros desconocidos en los ámbitos de salud, para proteger al enfermo.

Por otro lado, la legislación internacional menciona que no muchos países tienen una regulación sobre la base de protección de datos, puesto que aún no la implementan o no la ven necesaria; sin embargo, existe una gran asimetría de protección de datos a nivel internacional. Se puede apreciar que los Estados no buscan brindar garantías que protejan al ciudadano con respecto a este tipo de vulneración de datos personales o sensibles. En Perú, se busca proteger los datos personales mediante la LPDP o la misma ANPD, y siempre se vincula este derecho con otros de índole fundamental y de mayor relevancia, puesto que los datos son compartidos diariamente.

Símil entre Derecho a la Privacidad y Derecho a la Intimidad

Figura 1

Símil entre Derecho a la Privacidad y Derecho a la Intimidad, su conexión con los datos personales y los datos sensibles



Nota. Elaboración propia.

De la investigación realizada, se entiende que, dentro de los datos personales, se ven inmersos los datos sensibles, puesto que los datos personales se tratan de aquellos datos que permiten a un sujeto ser identificable e individualizado, considerando lo siguiente: nombres, apellidos, DNI, correo electrónico. Por el contrario, los datos sensibles tienen que ver con información como los datos biométricos, de salud (enfermedades), diagnósticos y demás. Por tanto, al divulgar un dato personal sin el consentimiento o autorización del titular de los datos, se vulnera el derecho a la privacidad, que engloba de manera general la protección de los datos personales (los datos sensibles se encuentran dentro de este); mientras que, si se hace de conocimiento un dato sensible, sin autorización o consentimiento de su titular, entonces se vulnera el derecho a la intimidad al encontrarse dentro de la esfera más personal de un sujeto. Esto no quiere decir que, al vulnerarse un dato sensible, se estaría afectando el derecho a la privacidad. Tanto el derecho a la intimidad como el derecho a la privacidad son conexos.

2.2.5. Derecho de Protección de Datos Personales

2.2.5.1. Origen: Derecho de Protección de Datos Personales. En 1983, en Alemania, la sentencia de la Primera Sala del TC Federal Alemán, basada en el derecho a la dignidad humana y el libre desarrollo de la personalidad, propugnó la defensa de la continuidad y garantía, dando lugar a la creación de un nuevo derecho conocido como autodeterminación informativa. En este contexto, se enfatizó la necesidad de establecer mecanismos para salvaguardar los datos personales no tanto por su naturaleza estrictamente privada, sino por el riesgo de un uso no autorizado, con el potencial de ser empleado sin el debido consentimiento.

Posteriormente, los tribunales españoles en las Sentencias 290/2000 y 292/2000 de 30 de noviembre: la primera confirma la constitucionalidad de la Ley Orgánica 5/1992 de 29 de octubre, y con la segunda se brindó la inconstitucionalidad de la comunicación de datos entre ficheros de la Administración Pública cuando se carezca del consentimiento del titular de los datos o de previsión legal.

Asimismo, se tiene la sentencia (El derecho a la protección de datos de carácter personal, 2000) que desarrolla (La Ley de Transparencia y Acceso a la Información Pública, 2002):

> «7. [El derecho a la protección de datos de carácter personal] consiste en un poder de disposición y de control sobre los datos personales que faculta a la persona para decidir cuáles de esos datos proporcionar a un tercero, sea el Estado o un particular, o cuáles puede este tercero recabar, y que también permite al individuo saber quién posee esos datos personales y para qué, pudiendo oponerse a esa posesión o uso. Estos poderes de disposición y control sobre los datos personales, que constituyen parte del contenido del derecho fundamental a la protección de datos, se concretan jurídicamente en la facultad de consentir la recogida, la obtención y el acceso a los datos personales, su posterior almacenamiento y tratamiento, así como su uso o usos posibles por un tercero,

> sea el Estado o un particular. Y ese derecho a consentir el conocimiento y el tratamiento, informático o no, de los datos personales, requiere como complementos indispensables, por un lado, la facultad de saber en todo momento quién dispone de esos datos personales y a qué uso los está sometiendo, y, por otro lado, el poder oponerse a esa posesión y usos». (STC 292/2000, 2000, p.7)

2.2.5.2. Derecho a la Identidad. Fernández (1997) menciona que "la identidad es el conjunto de datos biológicos y de atributos y características que, dentro de la igualdad del género humano, permiten distinguir indubitablemente a una persona de todas las demás" (p. 248).

El derecho a la identidad está vinculado jurídica y dogmáticamente al derecho civil, como un elemento esencial del derecho de las personas, es así que cada persona posee derechos y obligaciones que son inherentes; por ende, la identidad, al ser un derecho, da la potestad al individuo para poder elegir libremente por sí mismo todas aquellas características que le afecten de manera personal.

Asimismo, se remonta a Italia, a las últimas décadas del siglo XX, puesto que se crea a partir de la Sentencia del Pretor de Roma (1974), la cual denomina derecho a la identidad como "identificación"; así, se empezaron a emitir jurisprudencias relativas a la dimensión dinámica del derecho a la identidad. El jurista Fernández Sessarego empezó a estudiar esta denominación y fue en el año 1988 que realizó una ponencia titulada "El derecho a la identidad personal".

Además, se posee dos vertientes: la dimensión pasiva y la dimensión dinámica. Varsi (2018) denomina a la primera como identidad pasiva, la que no cambia desde el nacimiento, y la identidad dinámica o activa que comprende la total manera de ser y actuar de la persona durante su trayectoria existencial; comprende su personalidad, su profesión, sus actividades, su posición religiosa, ideológica, política, etc.

2.2.6. La Protección de los Datos Personales y la Autodeterminación Informativa en el Perú

En el Perú, desde la constitución de 1993, se reconoce la disposición que tiene el ciudadano sobre sus datos, esto siempre mediante el consentimiento previo, encontrándose regulado en el art. 6.2 de la Constitución Política del Perú. Con posterioridad, el TC desarrolló el art. 61.2 dentro del Código Procesal Constitucional, brindando más relevancia a la protección de datos, y así se denominó autodeterminación informativa.

Dentro de este proceso de desarrollo de la autodeterminación informativa, el TC precisó los derechos que la componen: la capacidad de exigir jurisdiccionalmente el acceso de información; posibilidad de añadir información en los registros, ya sea para la actualización de datos o inclusión de los datos no registrados; posibilidad de corregir datos ya registrados; y la capacidad de impedir que la información personal registrada se difunda para fines para los cuales no fue recopilada. Sin embargo, el TC tomó en cuenta que se podría confundir este derecho con otros, por tanto, en su Sentencia del 29 de enero del 2003, recaída sobre el Exp. N° 1797-2002-HD/TC, menciona que el art. 2.6 de la Constitución es un derecho independiente y, de esa manera, desarrolla la distinción con el derecho de identidad, derecho a la imagen y derecho a la intimidad.

De este modo, el TC señala que el derecho de autodeterminación informativa tiene como finalidad resguardar la intimidad personal o familiar, la imagen y la identidad, frente al riesgo que implica el uso y la eventual manipulación de los datos.

2.2.6.1. Regulación Sobre los Datos Personales. Antes de la LPDP, el ordenamiento jurídico peruano con respecto a la protección de datos se encontraba inmerso dentro de la Constitución en su art. 6.2, donde se menciona que los ciudadanos tienen la disposición de sus datos. Posteriormente, el TC desarrolló el derecho a la autodeterminación informativa con el que menciona que este derecho protege al titular frente a abusos o riesgos que son consecuencia

del mal uso de los datos personales; además, este mismo derecho ofrece que el titular tenga control de su información personal.

En el Perú, la protección de los datos personales se encuentra regulada por la LPDP y su RLPDP; posteriormente, la ANPD se encargó de hacer cumplir las normas que se encuentran en la ley antes mencionada, puesto que había diversas maneras de vulnerar estas normas. Así, con los mecanismos se empezó a proteger los datos personales y sensibles de las personas, datos que son entregados a las entidades públicas o privadas.

2.2.6.2. Autodeterminación Informativa. Este derecho es joven, puesto que no hay mucho desarrollo doctrinario; sin embargo, sí tiene desarrollo jurisprudencial puesto que el TC brindó su concepto y los alcances que tiene este derecho frente a los datos personales. Este derecho es inherente al titular que brinda información a las entidades públicas y privadas. El titular puede disponer de este como le plazca, y puede solicitar copia de la información otorgada; sin embargo, para poder realizar estos actos debe cumplir requisitos establecidos y no solicitar algo que no está dentro de su alcance.

La Sentencia del TC Exp. N.º 0090-2004-AA/TC señala que, al generarse la vulneración de datos personales por parte de los establecimientos de salud, se afecta el derecho a la privacidad de la persona -titular de los datos-, vinculado al derecho a la autodeterminación informativa, sobre ello, en la Sentencia del TC Exp. N° 04739-2007-PHD/TC, en los fundamentos del 2 al 4, se expresa que el derecho a la autodeterminación informativa se refiere a un conjunto de capacidades que todo individuo posee para ejercer control sobre la información personal relacionada con él, ya sea que esté contenida en registros públicos, privados o informáticos. Este derecho tiene como objetivo hacer frente a posibles excesos en el manejo de dicha información. Está estrechamente vinculado al dominio sobre la información, siendo considerado como una autodeterminación en la vida íntima y en la esfera personal; por tanto, la autodeterminación informativa busca resguardar al sujeto no solo

respecto de sus derechos sobre su esfera personal, sino en todos los ámbitos; he aquí la diferencia con el derecho a la intimidad, puesto que este busca proteger la vida privada, mientras que el derecho a la autodeterminación informativa garantiza la capacidad de cada individuo para preservarlo mediante el control de registros, uso y revelación de los datos pertinentes. En este contexto, este derecho protege al titular de posibles abusos o riesgos derivados de la utilización de los datos, permitiéndole solicitar la exclusión de información considerada "sensible" que no debería difundirse ni registrarse. Además, le concede la facultad de difundir o transmitir dichos datos.

2.2.7. ANPD

2.2.7.1. Obligaciones de la ANPD. Este órgano es aquel encargado de velar por la protección de los datos personales, realizando las funciones de fiscalización, supervisión consultiva, orientadora y sancionadora, en el marco de la LPDP; asimismo, es el encargado de velar por el procedimiento trilateral de tutela.

2.2.7.2. Mecanismos Para el Control de Datos. Los mecanismos que tiene la ANPD para la protección de datos son los siguientes:

- El RNPDP registra todos los bancos de datos de la administración privada o pública, además de las sanciones impuestas por el ente y, finalmente, el flujo transfronterizo.
- Certifica la inscripción por parte de las entidades públicas o privadas en el RNPDP.
- Absuelve consultas sobre la protección de datos personales y busca promover eventos y campañas para la difusión y promoción de este derecho.

Se resaltan las más importantes, sin embargo, en el art. 33 de la LPDP se encuentran más mecanismos que empleó la ANPD para su debida protección.

Tabla 1

Sanciones

Leves	Graves	Muy graves
Recopilación de información necesaria.	No brindar la información solicitada por el titular de los datos.	Entregar documentos e información falsa a ANPD.
No rectificar datos personales.	No pedir el consentimiento del titular para el uso de sus datos.	
No suprimir datos personales.	No tener las medidas de seguridad para el trato de datos sensibles.	No cesar un tratamiento indebido.
No inscribir la base de datos en el registro.		

Nota. Las multas dependerán de la seriedad de la infracción cometida por las entidades, en concordancia con el art. 39 de la LPDP.

Mecanismo con el cual sancionan a la entidad pública o privada que vulnera la LPDP.

2.2.7.3. Conceptos Relacionados con la ANPD. Datos personales: Es la identificación de la información de la persona natural. A través de los medios, estos podrían ser utilizados con fines establecidos legalmente (Ley de Proteccion de Datos Personales, 2011).

Es la protección jurídica a las personas naturales, a los que concierne sus datos de forma personal (privada) al amparo contra la posible utilización de terceros (Conde, 2005).

Datos sensibles: Estos datos son individuales y se constituyen con base en datos biométricos, a partir de los cuales se puede reconocer su origen racial y étnico, ingresos económicos, creencias religiosas, información relacionada a la salud, entre otros (El Peruano, 2013).

Titular de datos personales: Es aquel individuo que ha de generar su información personal.

"(…) Titulares de la información personal puedan conocer y meritar los beneficios y eventuales desventajas que podría conllevar el tratamiento de sus datos" (Castro, 2008).

Banco de datos personales: Es la disposición de este. Para la protección deben convertirse en "automatizados o no, independientemente del soporte, sea este físico, magnético, digital u óptico" (LPDP, 2013).

LPDP: La ley tiene como objetivo poder avalar la protección de los datos personales y se rige bajo la interpretación de la Constitución Política del Perú en su art. 2 inciso 6), a la par del inciso posterior; en el 7) se reserva la protección a la intimidad. En ese sentido, este inciso contiene una regla funcional para lograrlo y es especialmente significativo en vista de que alude a las prestaciones computarizadas que recopilan una medida creciente de datos. La norma les impide dar información que desconozca el derecho a la protección mencionado anteriormente (Rubio, 2008).

ANPD: Entre sus funciones están la de administrar, supervisar, consultar, coactiva y promover la LPDP para la acción:

- Dirección de Datos Personales: Es la encargada de resolver en primera instancia sobre el proceso sancionador, además de los procedimientos trilaterales.
- DGTAIPD: Se encarga de resolver en segunda instancia el proceso administrativo; es decir, ante ella, el administrado y administrador pueden recurrir la resolución de primera instancia, y la resolución emitida por este ente finaliza el procedimiento administrativo.
- DFI:_Unidad Orgánica encargada de fiscalizar el reglamento de la ley, así como comenzar los procedimientos de sanción de esta. Es la encargada de poder instruir cómo es la actuación en la sanción (Gobierno del Perú, 2018).
- RNPDP: Tiene como motivo de la inscripción la diferenciación en todo el Perú sobre los bancos de datos personales de administración pública o privada, también las sanciones o medidas cautelares impuestas correctivamente sobre la ANPD (Gobierno del Perú, 2018).

- Información Pública: Es todo documento fomentado por el presupuesto público que aproveche de base una decisión en el entorno administrativo (La Ley de Transparencia y Acceso a la Información Pública, 2002).

2.2.8. Establecimientos de Salud y los Protocolos de Protección de Datos Personales

En el Perú, mediante la Ley General de Salud -Ley N.º 26842- y Reglamento de Establecimientos de Salud y Servicios Médicos de Apoyo -Decreto Supremo N.º 013-2006-SA-, se tiene considerado a los hospitales, postas, clínicas, es decir, cataloga a las instituciones que brinda servicios de salud como establecimientos de salud y servicios médicos de apoyo; no obstante, para los fines de la presente investigación, se utiliza el término "entidades de salud" para hacer referencia a los establecimientos de salud y servicios médicos de apoyo, puesto que es un término que hace alusión a lo comúnmente conocido, entendido y utilizado en la comunicación diaria.

Las entidades de salud son esenciales, ya que garantizan el bienestar de las personas y la satisfacción como pacientes al ofrecer atención médica. El Reglamento de Establecimientos de Salud y Servicios Médicos de Apoyo, Decreto Supremo N.º 013-2006-SA, en el art. 1 señala: "el presente Reglamento establece los requisitos y condiciones para la operación y funcionamiento de los establecimientos de salud y servicios médicos de apoyo, orientados a garantizar la calidad de sus prestaciones, así como los mecanismos para la verificación, control y evaluación de su cumplimiento".

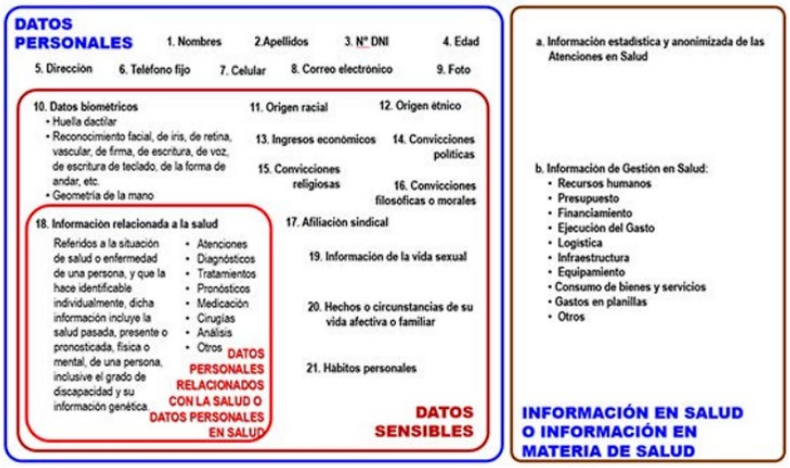
Para brindar la atención necesaria en los establecimientos de salud y servicios médicos de apoyo, primero realizan la historia clínica del paciente. El art. 2 del Reglamento de Establecimientos de Salud y Servicios Médicos de Apoyo, Decreto Supremo N.º 013-2006-SA, señala: "documento médico que registra los datos de identificación y de los procesos relacionados con la atención del paciente en forma ordenada, integrada, secuencial e inmediata de la atención que el médico u otros profesionales brindan al paciente".

Dichos datos, registrados en el historial clínico, son clasificados por la Directiva Administrativa N.º 294-MINSA/2020/OGTI en tres niveles interconectados: i) los datos personales que se conectan con el ámbito de la salud, incluyen información de esa índole, o enfermedades que un sujeto posee, siendo esta respecto a su pasado, presente o los pronósticos que se vayan creando, esto sobre la salud mental o física de la persona; también se puede incluir información sobre el grado de discapacidad o información genética del sujeto; ii) datos sensibles, comprende los datos personales que tienen que ver con la salud de un sujeto, además de incluir información como afiliación sindical, origen étnico, afiliación sindical, hábitos personales, datos biométricos, huella dactilar, reconocimiento facial y otros; iii) datos personales, incluye los datos conexos con la salud, datos sensibles y se agrega la información más genérica, como son los nombres, apellidos, edad, DNI, ubicación de domicilio, número de celular, correo electrónico.

Clasificación de los datos en el sector salud

Figura 2

Clasificación de los datos en el sector salud



Nota. Imagen obtenida de la Directiva Administrativa N.º 294-MINSA/2020/OGTI.

Con ello, los profesionales de la salud pueden elaborar diagnósticos precisos y exactos respecto a la dolencia que presente el paciente en atención; asimismo, permite poseer un conocimiento profundo del paciente y se reflejan las características clínicas del paciente y la

evolución periódica que tiene. Dicha historia clínica se guarda en el banco de datos que las entidades de salud poseen, pero, para poder contar con este banco de datos, previamente deben inscribirse en RNPDP. Al ingresar a la página del Gobierno del Perú, se advierte que se debe realizar un abono de S/. 75.80 en el Banco de la Nación, señalando el código 4232 para iniciar con el proceso de inscripción; asimismo, se muestra información relevante para tener en cuenta, y se especifican las sanciones, medidas correctivas o cautelares que podrán ser impuestas por la ANPD en caso se incurra en alguna causal que lo amerite.

Ingresando al enlace del formulario virtual, se observa que ha sido desarrollado por el SIPDP bajo la supervisión del MINJUS. Se advierte que, en el formulario de inscripción de banco de datos personales, se rellenan una serie de requisitos que son tomados como declaración jurada y que, al finalizar, la ANPD verifica que se cumplan y se emite la RD correspondiente en un lapso de 30 días hábiles, notificándose a la dirección que se encontrará en la solicitud enviada.

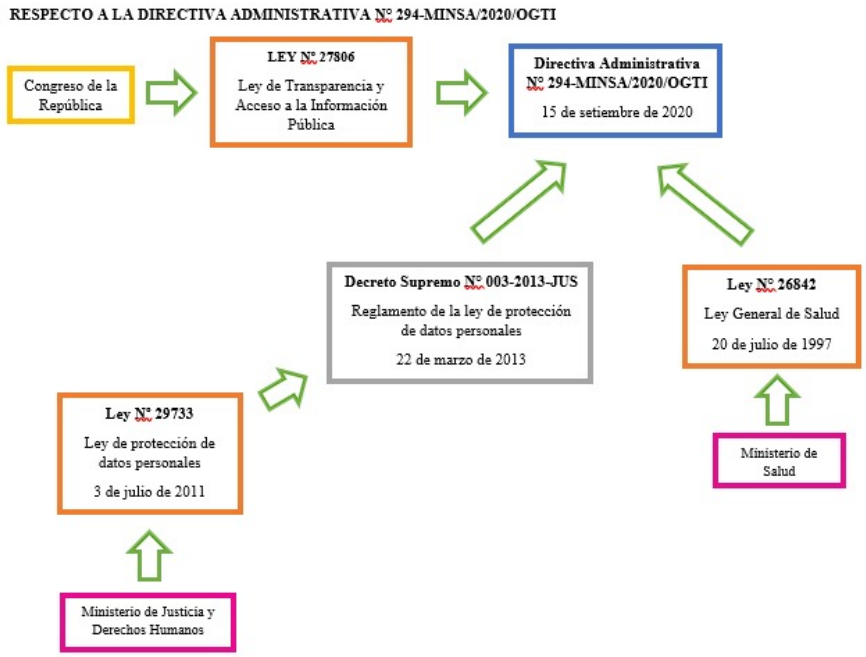
El inconveniente radica en que, rellenar el formulario, como se hizo mención, consta como declaración jurada, y la verificación respecto a si el banco de datos inscrito es correcto o no, se realiza ex post -si bien la administración ejerce su facultad de fiscalización posterior, en tanto, aplica el principio de presunción de veracidad al administrado-, lo cual incide en la vulneración a los datos personales en el caso de los establecimientos de salud y servicios médicos, puesto que solo se verifica lo rellenado en el formulario, tomándose como cierto, y una vez inscrito y en funcionamiento, cuando se genera la vulneración, recién se fiscaliza e intervine la ANPD, por lo que lo correcto sería realizar una fiscalización ex ante en pro de no tomar como cierto lo que consta en el formulario, sino, por el contrario, constatar la información, lo cual va de la mano con la primacía de la realidad; es decir, preferir lo que en la realidad percibe la ANPD al realizar la fiscalización correspondiente y no basarse en la declaración jurada al rellenar el formulario.

2.2.8.1. Directiva Administrativa que Establece el Tratamiento de los Datos Personales Relacionados con la Salud o Datos Personales en Salud. Mediante Directiva Administrativa N.º 294-MINSA/2020/OGTI, denominada Directiva Administrativa que establece el tratamiento de los datos personales relacionados con la salud o datos personales en salud, que fue emitida con fecha 15 de setiembre de 2020, se establecieron criterios administrativos para un adecuado control de los datos personales que son ofrecidos a entidades de salud. Además, esta directiva busca contribuir con la protección de la intimidad personal y familiar, respetando los documentos privados y brindando pasos para las actuaciones, a fin de evitar una vulneración de los datos personales ofrecidos.

Origen de la Directiva Administrativa N.º 294- MINSA/2020/OGTI

Figura 3

Leyes que amparan la Directiva Administrativa N.º 294- MINSA/2020/OGTI



Nota. La figura muestra cómo se relaciona la directiva con la LPDP, y la Ley N.º 26842 con la Ley N.º 27806, las cuales son importantes para su apropiada regulación.

2.2.9. INDECOPI y las Sanciones por Vulneración al Derecho a la Privacidad

- Procedimiento Administrativo Sancionador (2020) de Entel Perú SA: realizó llamadas para brindar promociones de sus productos a personas que no dieron consentimiento

para poder recibir este tipo de difusión; de esta manera, se está vulnerando el art. 58, numeral 58.1 y el literal e) de la Ley N.º 29571. Es así como la sanción ascendió a la suma de 45 UIT.

- Procedimiento Administrativo Sancionador (2019) de América Móvil Perú SAC: realizó comunicaciones comerciales sin previo consentimiento de los usuarios; por tanto, se hizo acreedor de una penalización por transgredir lo regulado en el art. 58, numeral 58.1 y el literal e) de la Ley N.º 29571, haciéndose acreedor de una sanción que ascendió a la suma de 150 UIT.
- Ley de Protección de Datos Personales (2011) sobre la empresa Telefónica del Perú S.A.A.: fue señalada por emplear tácticas comerciales agresivas al realizar comunicaciones con el objetivo de promover sus servicios sin obtener previamente el consentimiento necesario. Este actuar se considera una vulneración del art. 58, numeral 58.1 y del literal e) de la Ley N.º 29571. Como consecuencia de estas acciones, se impuso una sanción a la empresa, la cual ascendió a 40 UIT.
- Procedimiento Administrativo Sancionador (2019) que recae en la empresa RAPPI SAC: realizó envíos de mensajes sin consentimiento previo de los usuarios, y vulneró el art. 58, numeral 58.1 y el literal e) de la Ley N.º 29571. Recibió una amonestación.
- Procedimiento Administrativo Sancionador (2020) de El Banco Pichincha: fue objeto de atención debido a su práctica de llevar a cabo diversas comunicaciones con la finalidad de impulsar la contratación de productos y servicios, sin obtener el consentimiento previo por parte de los usuarios. Esta acción constituye una infracción al art. 58, numeral 58.1 y el literal e) de la Ley N.º 29571. Como consecuencia de esta conducta, el banco ha recibido una sanción de 45 UIT.
- Procedimiento Administrativo Sancionador (2020): La controversia en torno al Banco Internacional del Perú SAA radica en su práctica de llevar a cabo comunicaciones con

el propósito de fomentar la contratación de sus productos y servicios, sin obtener la autorización previa de los consumidores. Esta actuación condujo a que la entidad bancaria recibiera una sanción de 150 UIT.

El análisis realizado de las anteriores resoluciones emitidas por INDECOPI se orienta a tener una visión más amplia respecto de la vulneración de datos personales, puesto que, en la mayoría de los casos analizados, la principal afectación incurre en el hecho de que el usuario o el administrado no brinda su consentimiento para el uso o trato de sus datos personales; sin embargo, aun conociendo ello, las empresas utilizan los datos para poder beneficiarse de alguna manera. Por ello, INDECOPI sanciona a las empresas que afecten los datos personales, y de igual manera la ANPD debería sancionar a los establecimientos de salud y servicios médicos de apoyo de una manera más severa, puesto que en este tipo de establecimientos no solo se almacenan datos personales, sino también datos sensibles, logrando afectar a una o varias personas.

2.3. Definición de Términos Básicos

Derechos ARCO: Esos derechos trascienden a mérito de la LPDP, ya que pueden ser ejercidos por cada individuo en caso se transgreda sus datos personales, los cuales son:

- Derecho de acceso: Todos disponemos de derechos; si los solicitamos, deberíamos recibir información de cualquier ente del Estado (Constitucion Politica Del Peru, 1993).
- Derecho de rectificación: Si en todo caso ha existido una equivocación de la información exacta, esta posibilita corregirla (García, 2020).
- Derecho de cancelación: Este se da cuando se ha cumplido la finalidad de proporcionar datos personales, y se ha facultado solicitar la derogación de la información (García, 2020).
- Derecho de oposición: El derecho de solicitar la interrupción de los tratamientos de los datos personales porque no ha habido un consentimiento previo (García, 2020).

- Consentimiento: Definido como la autorización dada por un paciente de manera voluntaria y con pleno conocimiento de los detalles y posibles riesgos de un procedimiento médico o tratamiento (Beauchamp & Childress, 2011).
- Banco de Datos: Una estructura que almacena una gran cantidad de información organizada, con la capacidad de ser consultada, actualizada y manipulada para diversos fines (Elmasri & Navathe, 2015).
- Flujo Transfronterizo: Los flujos transfronterizos son los datos personales de las entidades privadas, entidades públicas y personas naturales que se envían fuera del territorio peruano (Gobierno del Perú, 2021).

Derecho de Privacidad: Se define como la libertad que cada persona posee para poder desenvolverse en el ámbito social o personal, ejerciendo de acuerdo con los propios estándares de conducta, prácticas o costumbres. Nadie podría privarse de ella si no es con su propia autorización (Quiroz, 2016).

Capítulo III. Metodología

3.1. Tipo y Método de la Investigación

3.1.1. Enfoque de Investigación

"El enfoque es la perspectiva que posee el investigador respecto a un punto de vista, con la finalidad de aproximarse a un objetivo" (Gallardo, 2017, p. 21). La categoría de la investigación es el enfoque cualitativo. Cuenya y Ruetti (2010) expresan que "busca comprender los fenómenos dentro de su ambiente usual, utilizando como datos descripciones de situaciones, eventos, personas, interacciones, documentos, etc." (p. 271).

Atendiendo al propósito de la investigación, existen dos criterios de clasificación: intrínseco o extrínseco.

Según el propósito intrínseco, la presente investigación fue de tipo descriptiva-analítica.

Respecto al tipo descriptivo, se entiende que "este criterio de clasificación hace referencia a qué es lo que se busca con la investigación en sí misma" (Rios, 2016, p. 9). En la presente investigación se analizaron resoluciones administrativas que se han recopilado del Compendio de Resoluciones de los Procedimientos Sancionadores, donde se registran las resoluciones administrativas a nivel nacional; asimismo, estas fueron halladas en la página del Gobierno del Perú respecto a la ANPD, a razón de que dicha información es pública. El periodo propuesto para la presente investigación, que es de 2020 a 2021, tiene 17 resoluciones que fueron objeto de estudio. El ámbito de emisión de este tipo de resoluciones, que refieren a la vulneración de datos personales y sensibles, es pequeña, puesto que el proceso para llegar a una sanción y/o absolución, dependiendo del caso, conlleva un plazo prolongado, a razón de la emisión de informes que se dan por la realización de diversas fiscalizaciones, lo cual hace que el tiempo se dilate. Además, al tratarse de datos personales y sensibles, estas fiscalizaciones son más minuciosas, y el tiempo requerido para la emisión de un informe es de un mes, aproximadamente, requiriéndose de tres a cinco de estos.

Sobre el tipo analítico, Charles C. Ragin indica que la investigación analítica implica el desglose minucioso de un problema en sus componentes esenciales, para comprender mejor sus interrelaciones y dinámicas. En el trabajo de investigación, a razón del desglose de las resoluciones, se obtiene los hechos controversiales, la motivación y las sanciones coercitivas impuestas, evidenciándose que una fiscalización ex post por la DFI (ANPD) al banco de datos de las entidades o terceros responsables, genera infracciones que vulneran los datos personales.

3.1.2. Tipo de Investigación

Se desarrollaron dos tipos de investigación de acuerdo con el propósito: pura y aplicada.

Investigación pura o teórica: "En la investigación básica o pura se tiene el objetivo de producir y recopilar la información para construir una base de comprensión que se va añadiendo a la información previamente existente" (Calla & Calla, 2019). Por tanto, el objetivo fue describir las resoluciones emitidas por la DPDP, así como una resolución emitida por la DGTAIPD con pronunciamiento distinto a la primera instancia.

Investigación aplicada: Se propuso una adición legislativa para que las fiscalizaciones realizadas por la DFI (ANPD) se realicen de manera ex ante.

Fuentes de información: La presente investigación es documental, por el hecho de utilizar materiales que no fueron tratados anteriormente como son las RD analizadas.

3.1.3. Método de Investigación

El presente trabajo de investigación se basa en el estudio de casos, puesto que se estudia en profundidad un problema dentro de una escala de tiempo limitada: las infracciones que cometen los establecimientos de salud y servicios médicos de apoyo.

3.2. Población y Muestra

Población: La población, en el marco de esta investigación, puede comprender tanto individuos como organizaciones e instituciones. En este estudio específico, se examinaron 17 resoluciones emitidas por la ANPD, las cuales están disponibles en su compendio publicado

en su página web oficial. Es importante destacar que este portal no solo contiene resoluciones relacionadas con la vulneración de datos personales en el ámbito de la salud, sino también en áreas como educación, finanzas y otras.

Muestra: En el contexto de la investigación actual, se ha optado por una muestra particular vinculada a los establecimientos de salud y servicios médicos de apoyo ubicados en Lima, Perú. En ese sentido, es relevante señalar que, dentro del periodo de años establecido para la presente investigación, solo se han registrado 17 resoluciones; por lo tanto, el análisis versa entorno a estas.

Criterios de inclusión: Se tomaron en cuenta las resoluciones de la ANPD de entidades relacionadas con la salud en los años 2020 y 2021 que refieran al uso de información de datos personales en el ámbito de la salud.

Criterios de exclusión: La información fue recopilada teniendo en cuenta la base de resoluciones que tiene la web Gob.pe, la plataforma digital del Estado peruano para la atención de sus ciudadanos; se encontró que en la sección de la ANPD se ubican específicamente las resoluciones emitidas en sus procedimientos, siendo una característica el tener un orden cronológico de años, emitidas por la DPDP utilizando el término “salud”. Se encuentran resoluciones en el transcurso del 2020 y 2021.

Criterio de comparación: Queda demostrado que fue útil tener en cuenta el eje temático en función del análisis que se realizó sobre el mal uso de información en las entidades de salud, ya que se analizaron algunas resoluciones emitidas por la entidad ANPD, con el fin de poder analizar los hechos, las motivaciones, las sanciones y clasificar las infracciones generadas por las administradas, las cuales fueron abordadas y analizadas aplicando la ficha de análisis documental.

3.3. Técnicas e Instrumentos de Recolección de Datos

3.3.1. Técnica de Recojo de Información

Se utilizaron técnicas de recolección de datos como cuestionarios, observación y levantamiento de información (Hernández, 2010). Se empleó, así, el análisis de resoluciones administrativas, teniendo como técnica la documentación.

Iñiguez (2008) menciona que la obtención del conocimiento a través del método designado es un procedimiento de rigor, orden lógico, que tiene como objeto mostrar el valor de la verdad sobre ciertos enunciados. El análisis documental de las resoluciones emitidas por la ANPD, entre los años 2020 y 2021, se realiza para considerar si ha existido vulneración de datos personales en el ámbito de salud.

3.3.2 Instrumentos de Recolección de Datos

Respecto al instrumento de recolección, se empleó la técnica cualitativa de revisión documental. Sobre la base de las resoluciones, se generó una variable de interés para poder identificar el accionar de la ANPD frente a lo que corresponde proteger, esto es, uno de los derechos fundamentales como es la privacidad. Se utilizó la ficha de registro de datos para identificar cuáles son los puntos controvertidos, las normas administrativas o constitucionales y, finalmente, cómo fue la parte resolutiva y si amerita sanción o no.

3.4. Técnicas de Análisis de los Datos

La técnica principal de análisis de datos consistió en identificar las violaciones a la protección de datos personales que se encuentran en el contenido de las resoluciones emitidas por la ANPD. Posteriormente, se procedió a la segmentación y análisis detallado de cada parte de las resoluciones en concordancia con los objetivos establecidos.

3.5. Aspectos Éticos de la Investigación

Para Rios (2016), los aspectos éticos de una investigación son la "manera correcta de conseguir la información, el trato adecuado de los sujetos a investigar, la confidencialidad, entre otros. Cualquier investigación que no respete aspectos éticos no podría ser considerada como una investigación pertinente" (p. 18).

Cabe resaltar que en la identificación y análisis de documentos públicos no se ha requerido el debido consentimiento porque la información se encuentra registrada para acceso gratuito en la página web mencionada; de tal forma, el uso de la información recopilada es, en su totalidad, académica. Además, sobre el uso de identidad, se encontró que es la misma entidad de la ANPD que menciona el no uso de la identidad de los administrados.

Para tal efecto, en caso de que existan casos delicados con respecto a los temas del mal uso de los datos personales en las resoluciones de la ANPD, se tuvo en consideración la reserva de identidad de las personas que fueron afectadas por esta acción por parte de las entidades privadas de salud. Es por esta razón que no se mencionan los nombres y solo se está abocado a mencionar los números de expedientes de los casos analizados.

3.5.1. Comité de Ética de la Investigación

Para Rios (2016), "todas las investigaciones que suponen estudios con sujetos o con información confidencial deberían ser aprobadas por un comité de ética que garantice que el proyecto está cumpliendo con todas las consideraciones necesarias" (p. 21).

Al respecto, la presente investigación fue presentada ante el Comité de Ética de la Universidad Continental, el cual se encargó de verificar la originalidad del tema de investigación y los demás aspectos de fondo y forma que debe cumplir para su aprobación.

Capítulo IV. Resultados

4.1. Categorías de Análisis

Se procederá a realizar un análisis detallado de cinco resoluciones específicas que son objeto de investigación. Este análisis se enfocará en extraer los mecanismos de control utilizados por la ANPD para abordar estos problemas. Se describirá la valoración realizada por la ANPD sobre los hechos y se estudiará la motivación que se otorga en cada caso para discernir la sanción apropiada.

Además, se buscará determinar si las sanciones aplicadas han sido efectivas en la prevención de la reincidencia de estas acciones. Se evaluará críticamente la eficacia de las medidas punitivas como una forma de disuadir futuras violaciones a la protección de datos personales.

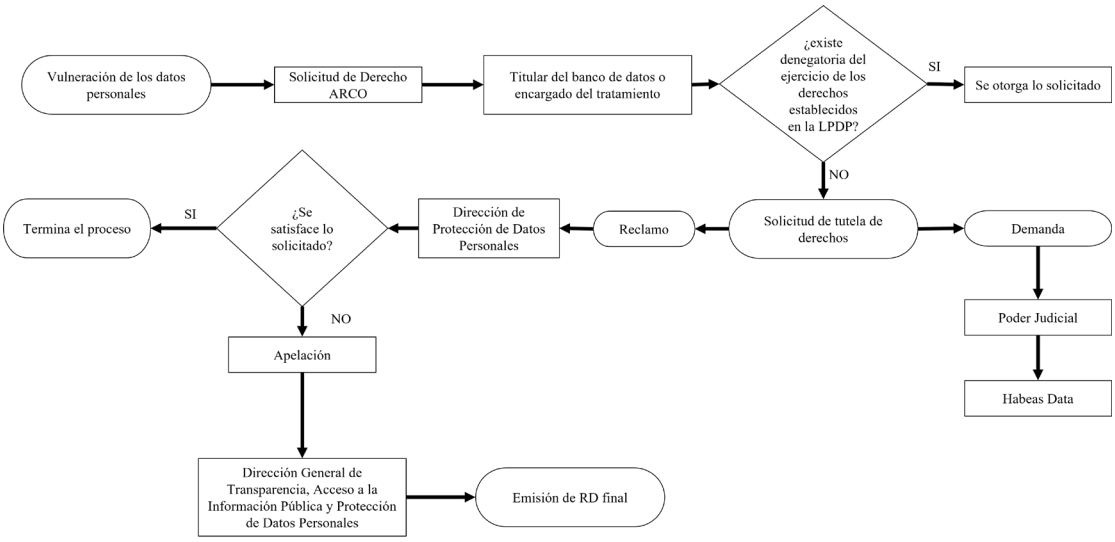
A través de este análisis exhaustivo, se aspira a obtener una comprensión más profunda de los métodos empleados por la ANPD para controlar estas situaciones, así como su impacto en la reducción de prácticas indebidas en relación con la seguridad de los datos personales.

Antes del análisis correspondiente, se explicará la conformación de procesos que presenta la ANPD.

Procedimiento de tutela de derechos

Figura 4

Procedimiento de tutela de derechos



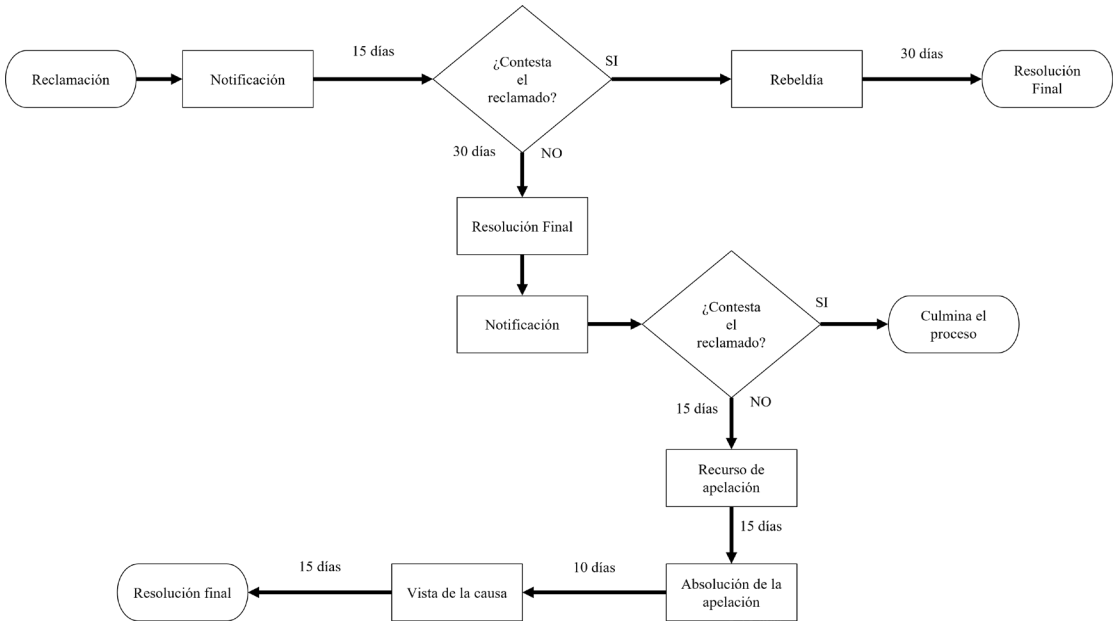
Nota. Elaboración propia.

Tutela de derechos: Inicia con la vulneración de los datos personales, luego el afectado debe presentar la solicitud de derechos ARCO ante el titular del banco de datos o encargado del tratamiento; si existe una denegatoria u omisión con respecto a la solicitud presentada, el afectado podrá solicitar tutela de derechos mediante un reclamo ante la DPDP. Luego de transcurrir 30 días, se emitirá una resolución, y si no satisface lo solicitado, se podrá apelar y, finalmente, se irá a la Dirección General de Trasparencia, Acceso a la Información Pública y Protección de Datos Personales. En el plazo de 30 días la dirección emitirá una resolución final.

Plazos del proceso de tutela de derechos

Figura 5

Plazos del procedimiento de tutela de derechos



Los plazos en este proceso comienzan a contar una vez que la reclamación ha sido notificada a la parte reclamada. A partir de esa notificación, se otorga un plazo de 15 días para que la parte reclamada presente su descargo. Si la parte reclamada no responde dentro de este plazo, se considerará como rebelde, y en un plazo de 30 días se emitirá una resolución final.

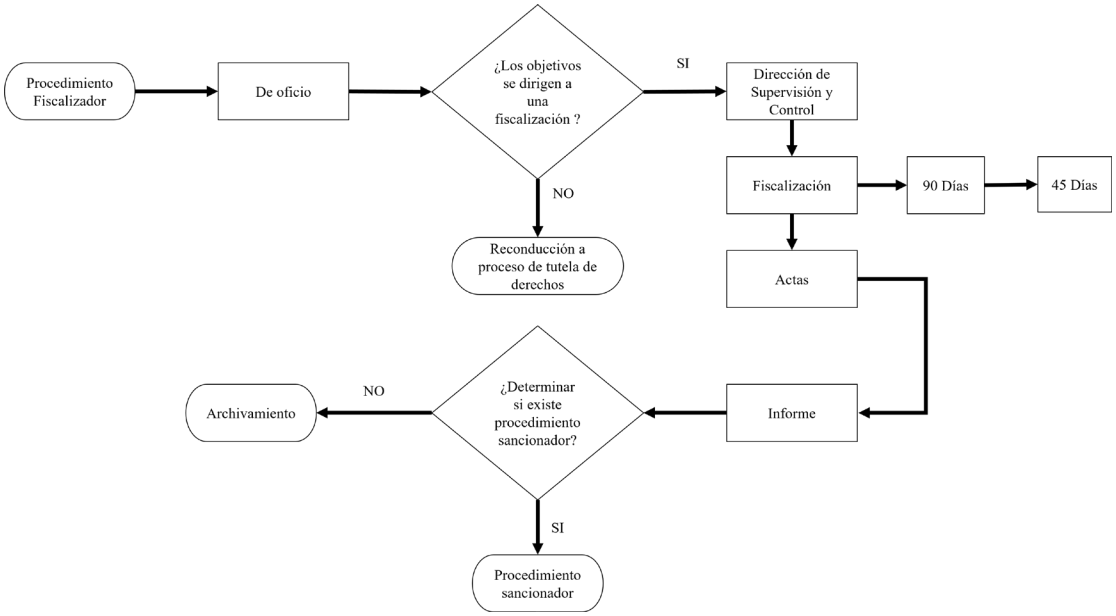
En caso de que la parte reclamada presente su descargo, este será evaluado, y se emitirá una resolución dentro de los 30 días siguientes. Posteriormente, se podrá ejercer el recurso de apelación dentro de los 15 días posteriores a la notificación de la resolución. La dirección encargada de absolver la apelación tendrá un plazo de 15 días para resolverla.

Después de esta resolución, se programará una audiencia de vista de la causa, la cual debe llevarse a cabo en un plazo de 10 días. Finalmente, después de la vista de la causa, se emitirá la resolución final en un plazo de 15 días.

Procedimiento Fiscalizador

Figura 6

Procedimiento Fiscalizador



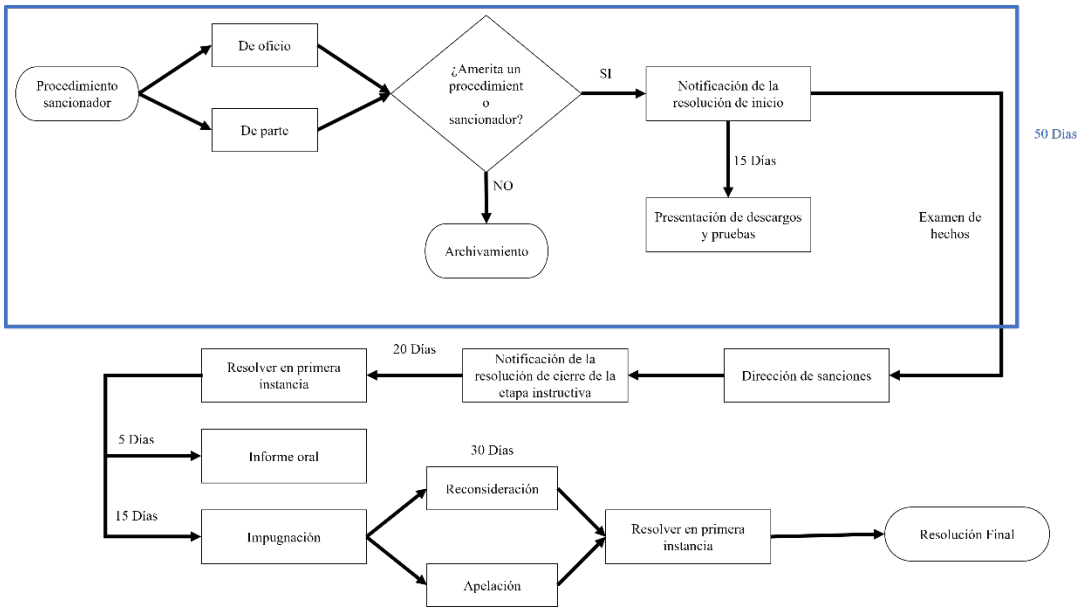
El procedimiento fiscalizador puede iniciarse a través de un oficio. La DSC evalúa si la situación en cuestión requiere una fiscalización o si está relacionada con la tutela de derechos. Si se determina que la fiscalización es necesaria, la DSC tiene un plazo de 90 días para llevar a cabo las inspecciones necesarias. En circunstancias excepcionales, este plazo puede ser extendido por un periodo adicional de 45 días.

El procedimiento culmina con la emisión de un informe que es revisado por el director de la Dirección de Sanciones. Este último verifica si los hallazgos ameritan la apertura de un proceso sancionador.

Procedimiento Sancionador

Figura 7

Procedimiento Sancionador



El proceso sancionador inicia de parte o de oficio, comienza con la recepción del informe emitido por la DSC, que es revisado por el director de la Dirección de Sanciones. Este director verifica si se justifica una sanción o, de lo contrario, decide archivar el caso.

Si se considera necesaria la sanción, se notifica el inicio del procedimiento al administrado, quien tiene un plazo de 15 días para presentar su descargo y aportar las pruebas pertinentes. Luego de esta etapa, se inicia el examen de hechos, que tiene un plazo de 50 días, incluyendo todo lo realizado hasta ese momento.

Una vez completado este período, la dirección tiene 20 días para emitir la resolución de primera instancia. Tras la emisión de esta resolución, se permite solicitar un informe oral en un plazo de cinco días. Luego, se abre un período de 15 días para interponer el recurso de apelación.

Finalmente, el director general de Protección de Datos Personales emitirá la resolución final.

En la problemática presente se ha realizado un análisis profundo respecto a las RD emitidas dentro del periodo 2020-2021, las cuales son:

4.2. ¿Cuáles son los Hechos que Fueron Puestos en Conocimiento de la ANPD en los Años 2020 y 2021, los Cuales Fueron Analizados por la DPDP y DGTAIPD, Respectivamente?

Importancia de los hechos

La relevancia de los hechos radica en el deseo de obtener información específica de una situación. De este modo, los hechos son fundamentales para crear un contexto que explique el motivo de una situación, proporcionando una perspectiva más clara para el desarrollo de un proceso. Asimismo, en la administración, como se observa en la ANPD, la necesidad de hechos es evidente, ya que estos son presentados tanto por la DFI como por la entidad administrada. Estos hechos son esenciales para determinar los aspectos a considerar en la motivación, siendo su alcance limitado por los propios hechos. Además, es común que un hecho infractor que no cuente con un respaldo adecuado por parte de la DFI sea desestimado, evitando así la necesidad de que la DPDP lo analice.

Origen de los hechos ante la ANPD

Los hechos se originan a partir de una fiscalización llevada a cabo por la DFI, la cual se encarga de elaborar informes en relación con el tratamiento de datos personales, siempre en el marco de la LPDP. Estos informes son fundamentales, ya que permiten que la entidad administrada realice las correcciones necesarias. Asimismo, proporcionan a la ANPD los puntos que deben ser analizados y aquellos por los cuales se impondrán sanciones. Es importante destacar que la elaboración de estos informes no suele ser rápida, ya que las resoluciones directorales hacen referencia a la realización de entre tres a cinco informes, con un lapso de aproximadamente dos meses entre cada uno de ellos.

Competencia en resolución de controversias en materia de datos personales

En la fase inicial, la DFI toma conocimiento de los hechos, ya sea por iniciativa propia o a través de denuncias. La responsabilidad de resolver en primera instancia recae en la DPDP, según lo facultado por el art. 74 del Reglamento de Organización y Funciones del MINJUS. En la segunda instancia, la DGTAIPD es la entidad encargada de emitir una resolución, siguiendo las disposiciones del art. 71, literal I, del mismo reglamento ministerial.

Una vez brindada información, que es aplicable a cada RD, se procede a desarrollar cada una:

Primer Exp. N.º 143-2018-JUS/DGTAIPD-PAS

RD N.º 1885-2020-JUS/DGTAIPD-DPDP

En el descargo realizado por la DFI, se tiene como:

1° Hecho infractor: la afectación del art. 5 de la LPDP, por el tratamiento de datos personales sin el consentimiento del titular, puesto que sea considerado válido el consentimiento deben juntarse cuatro presupuestos: libre, previo, expreso e informado; de esta manera, la DPDP consideró que la administrada vulneró este derecho, incluso cuando presentó dos descargos, puesto que lo presentado es considerado como posterior al proceso fiscalizador.

2° Hecho infractor: es la vulneración del art. 14, del cual se desprende que el titular de los datos personales debe ser informado de cómo serán tratados sus datos, sin embargo, la administrada presentó un descargo alegando que se cumple con lo solicitado en el art. 18 de la LPDP; en consecuencia, la DPDP consideró que no se cometió infracción al artículo.

En consecuencia, LA DFI sugiere imponer:

Para el 1° hecho, se sugiere una multa ascendente a 5,5 UIT.

Para el 2°hecho, se sugiere aplicar el eximente del art 257, inciso 1, literal f.

Segundo Exp. N.º 110-2019-JUS/DGTAIPD-PAS

RD N.º 1436-2021-JUS/DGTAIPD-DPDP

En el descargo realizado por la DFI, se tiene como:

1° Hecho infractor: La administrada realizó tratamiento de datos personales incumpliendo la obligación de confidencialidad, establecida en el art. 17 de la LPDP.

Por ese motivo, la DFI propone la siguiente multa:

1° hecho infractor, se sugiere una multa de 39,5 UIT.

Tercer Exp. N.º 127-2018-JUS/DGTAIPD-PAS

RD N.º 1045-2020-JUS/DGTAIPD-DPDP

En el descargo realizado por la DFI, se tiene como:

1° Hecho infractor: vulneración al art. 5 de la LPDP, por el tratamiento de datos sin consentimiento. La DPDP consideró que no se solicitaron los documentos necesarios para poder imputar tal vulneración.

2° Hecho infractor: afectación al art 18 de la LPDP, del cual se desprende la obtención de consentimiento para el tratamiento de datos. Se observó que se afectó a lo siguiente:

1° medio: la política de privacidad del sitio web de la administrada no presenta lo requerido por la LPDP, sin embargo, la DPDP procederá a ver si se cumplió en enmendar lo solicitado por la DFI.

2° medio: tratamiento de datos recopilados mediante EXCEL, la DPDP consideró que no se estaría afectando el art. 18 de la LPDP.

3° medio: el sistema de LOLCLI 9000++ vulnera el art 18 de la LPDP, puesto que no informa como debe, incumpliendo así el artículo antes mencionado.

4° medio: en el sistema cliente/servidor, denominado “sistema de gestión”, al ser una fuente que alimenta el otro sistema de LOLCLI 9000++ y comparten la misma base de datos; en consecuencia, la DPDP considera que no es objeto de análisis de ilicitud.

5° medio: sistema de chequeos ocupacionales – Mediweb no se desarrolla a tal punto que requiera un análisis de ilicitud.

6° medio: formulario físico denominado "formato de filiación", es una reproducción de la información contenida en el sistema de LOLCLI 9000++, de esa manera la DPDP sustrae su análisis.

3° hecho infractor: presunto incumplimiento sobre la no inscripción de los bancos de datos personales de trabajadores, pacientes, médicos, proveedores, videovigilancia, historias clínicas, usuarios del sitio web y chequeo ocupacional.

4° hecho infractor: sobre realización de flujo transfronterizo que realiza la administrada por los datos recopilados de su página web www.montefiori.com, la DPDP aprecia que la administrada solicitó la inscripción del flujo transfronterizo, sin embargo, esta fue observada y no hubo una subsanación.

5° hecho infractor: no implementar medidas de seguridad para el tratamiento de datos personales que contienen datos sensibles. De esta manera se afecta lo siguiente:

A: Afectación al art. 39 numeral 1, por no documentar los procedimientos de verificación y privilegios.

B: Afectación al art. 39 numeral 2, por no generar cierres de sesión de los usuarios producto de la interacción con los sistemas de tratamiento de datos.

C: afectación al art. 40, por no encontrar unas medidas adecuadas para el almacenamiento de datos personales.

D: Afectación al art. 42, por tener documentación no automatizada en espacios abiertos y no resguardados.

E: Afectación al art. 43, por no tener un procedimiento que restrinja la generación de copias y reproducción de documentos solo al personal autorizado.

De acuerdo con las recomendaciones de la DFI, se sugiere imponer multas para los hechos anteriores. Se propone lo siguiente:

Para el primer hecho, se sugiere una multa ascendente a 7 UIT.

Para el segundo hecho, se sugiere una multa equivalente a 1 UIT.

Para el cuarto hecho, se sugiere una multa de 1.5 UIT.

Para el quinto hecho, se sugiere una multa de 8 UIT.

En relación con el tercer hecho, la DFI sugiere archivarlo, indicando que no se recomienda imponer una sanción.

Cuarto Exp. N.º 144-2018-JUS/DGTAIPD-PAS

RD N.º 1459-2020-JUS/DGTAIPD-DPDP

1° análisis: comienza cuando la DPDP menciona que el recurso de consideración se solicita en el mismo órgano que emitió el pronunciamiento, la administrada presenta nuevos argumentos jurídicos con el fin de poder cambiar el veredicto que se realiza; sin embargo, la DPDP menciona qué características debe presentar una reconsideración.

2° análisis: la DPDP, al obtener el descargo presentado por la administrada, manifiesta que lo que presentó no es una prueba nueva, sino solamente modificada, lo cual no cumple.

Quinto Exp. N. º 207-2021-PTT

RD N. º 3454-2021-JUS/DGTAIPD-DPDP

1° análisis: la DPDP se pronuncia con respecto a la protección de datos personales y cómo esta se encuentra regulada por la constitución; y que, posteriormente, la DPDP vela por ellos mediante la LPDP. Por otra parte, el administrado solicita que le brinden información de donde se recabó la suya, puesto que este es un derecho del titular.

2° análisis: la DPDP alega que lo que solicita el administrado le compete más al derecho de petición que al derecho de acceso.

Sexto Exp. N.º 74-2018-JUS/DGTAIPD-PAS

RD N.º 3292-2019-JUS/DGTAIPD-DPDP

Del descargo generado por la DFI se tiene:

1° Hecho infractor: vulneración al art. 18 de por realizar tratamiento de datos personales a través de la página web www.clinicamundosalud.com.pe, además de formularios físicos denominados “compromiso de trabajador” "consentimiento de tratamiento de datos personales del profesional de salud" y "consentimiento de tratamiento de datos personales del paciente en la historia clínica".

2° Hecho infractor: afectación al art. 78 del RLPDP por no inscribir el banco de datos de "usuarios del sitio web" y "accesos".

3° Hecho infractor: afectación al art. 26 del RLPDP, que menciona la no información brindada a la DGTAIPD, puesto que el servidor físico del sitio web se encuentra en Inglaterra.

En consecuencia, la DFI propone imponer lo siguiente:

En caso del 2° y 3° hecho infractor, se le exime porque lo subsanó antes del inicio del proceso sancionador; con respecto al 1° hecho infractor, se sugiere imponer una multa de 5.1 UIT, además de imponer una medida correctiva para sus formularios físicos.

Séptimo Exp. N.º 141-2018-JUS/DGTAIPD-PAS

RD N.º 1049-2020-JUS/DGTAIPD-DPDP

Mediante descargo de la DFI se obtiene:

1° hecho infractor: presunta afectación al tratamiento de datos personales sin haber obtenido válidamente el consentimiento para ello, afectando los art. 5, 1 y 14 que versan sobre el tratamiento de datos. La administrada alega que el sitio web que mencionan en la primer RD no es la misma con el cual se le están imputando hechos.

2° hecho infractor: por incumplimiento del art. 18, por no informar el tratamiento de datos a los titulares, se desprende:

1° medio:

A: la administrada utiliza formularios físicos, sin embargo, estos no presentan la información necesaria que solicita el art. 18 de la LPDP. La administrada presentó un descargo alegando que sí se subsanó esta imputación, sin embargo, la DPDP menciona que esta fue una enmienda parcial, puesto que fue posterior.

B: afectación al art. 18 de la LPDP, por medio de un formulario físico, cámaras de vigilancia y no contar con una política de privacidad idónea que informe sobre ello.

3° hecho infractor: por afectación del art. 132, numeral 1, literal e, por no haber inscrito el banco de datos en el RNPDP.

En consecuencia, la DFI recomienda imponer las siguientes multas:

- 1° hecho infractor, se sugiere una multa de 5,5 UIT.
- 2° hecho infractor, se sugiere una multa de 10 UIT.
- 3° hecho infractor, se sugiere una multa de 2,5 UIT.

Octavo Exp. N.º 07-2019-JUS/DGTAIPD-PAS

RD N.º 1180-2020-JUS/DGTAIPD-DPDP

Del descargo otorgado por la DFI se obtiene:

1° Hecho infractor: la difusión de imágenes de personas en la página web www.centromedicoohi.pe sin el consentimiento adecuado constituye una violación al art. 13 de la LPDP y al art. 12 del RLPDP.

2° Hecho infractor: el tratamiento de datos personales recopilados a través de los formularios físicos denominados "historias clínicas ocupacionales" y "formato de antecedentes ocupacionales", así como en la página web, contraviene el art. 18 de la LPDP.

3° Hecho infractor: la omisión de inscribir en el RNPDP el banco de datos personales relacionados con "pacientes", "trabajadores" y "usuarios de sitio web", constituye una vulneración del art. 78 del RLPDP.

4° Hecho infractor: la falta de comunicación a la DGTAIGPD sobre el uso de flujo transfronterizo de datos personales recopilados por el sitio web, dado que el servidor físico se ubica en Canadá, implica una afectación al art. 26 del RLPDP.

De esta manera, la DFI propone sancionar a la administrada con las siguientes multas:

- 1° hecho infractor, se sugiere una multa de 6 UIT.
- 2° hecho infractor, se sugiere una multa de 6 UIT.
- 3° hecho infractor, se sugiere una multa de 2 UIT.
- 4° hecho infractor, se sugiere una multa de 0,5 UIT.

Noveno Exp. N.º 142-2018-JUS/DGTAIPD-PAS

RD N.º 1580-2020-JUS/DGTAIPD-DPDP

Del descargo otorgado por la DFI se obtiene:

1° Hecho infractor: el tratamiento de datos personales recopilados a través de los siguientes medios:

1° documento: historia clínica, consentimiento informado de hospitalización, informe de enfermería y evolución médica.

2° documento: mediante el Sistema integrado de Historias Clínicas.

3° documento: El formulario Contáctanos del sitio web: www.clinicalaluz.com.pe.

4° documento: Cámaras de vigilancia.

Este hecho contraviene el art. 18 de la LPDP.

2° Hecho infractor: la omisión de inscribir en el RNPDP el banco de datos personales de proveedores, constituye una vulneración del art. 78 del RLPDP.

3° Hecho infractor: la falta de comunicación a la DGTAIGPD sobre el uso de flujo transfronterizo de datos personales recopilados por el sitio web, dado que el servidor físico se ubica en Estados Unidos, implica una afectación al art. 26 del RLPDP.

4° Hecho infractor: la falta de implementación de medidas adecuadas para el tratamiento de datos personales que contienen información sensible constituye una violación a los art. 39 y 40 del RLPDP, mediante los siguientes medios:

1° incumplimiento: la omisión en documentar los procedimientos relacionados con la gestión de verificación y privilegios asignados.

2° incumplimiento: la ausencia de registros, así como la falta de generación de estos, que reflejen la interacción lógica con el banco de datos personales del soporte automatizado de pacientes.

3° incumplimiento: la carencia de un entorno adecuado en el centro de datos, evidenciado por la falta de extintores y la presencia de fallas en el sistema de aire acondicionado, que conllevan riesgos como goteo de agua.

De esta manera, la DFI propone imponerle las siguientes multas:

- 1° hecho infractor, se sugiere una multa de 10 UIT.
- 2° hecho infractor, se sugiere una multa de 0,5 UIT.
- 3° hecho infractor, se sugiere una multa de 1,5 UIT.
- 4° hecho infractor, se sugiere una multa de 5,1 UIT.

Décimo Exp. N.º 174-2019-JUS/DGTAIPD-PAS

RD N.º 3039-2021-JUS/DGTAIPD-DPDP

En el descargo realizado por la DFI, se tiene como:

1° Hecho infractor: La vulneración del art. 18 del LPDP, esto a través del sistema de "Filemarker Pro" y formularios físicos denominados "autorización de toma de muestras" y "solicitud para peritaje de paternidad por ADN; sin embargo, la administrada en su descargo manifiesta que sí cumple con informar lo que solicita el art. 18, no obstante, la DPDP al momento de valorar verifica que la administrada no cumple con informar el tiempo de

conservación de los datos, las transferencias y la posibilidad de ejercer los derechos ARCO. De esta manera, se afirma que la administrada incurre en el hecho infractor.

2° Hecho infractor: se origina con el incumplimiento de las medidas de seguridad establecidas en la ley, lo cual se llega a subdividir en las siguientes acciones infractoras:

1° medida de seguridad: incumplimiento del numeral 1 del art. 39 RLPDP, a partir del cual la administrada no presentó los documentos de gestión de acceso y privilegios de los usuarios para el acceso al sistema. En la controversia, la administrada presentó su descargo afirmando que tiene un documento que sí acredita el cumplimiento del art. y que fue implementado antes de la fiscalización; sin embargo, la DPDP, al constatar, se dio cuenta que la fecha era posterior a la fiscalización, desacreditando el argumento de la administrada.

2° medida de seguridad: incumplimiento del numeral 2 del art. 39 RLPDP, a partir del cual es importante mantener y generar registros con la interacción del sistema, para tener un mejor control. Mediante informe técnico quedó acreditado que la administrada cumplió con subsanar la infracción.

3° medida de seguridad: incumplimiento del art. 40 RLPDP, donde se desprende la importancia de la realización de copias de respaldo de los sistemas que realicen tratamiento de datos personales. La administrada subsanó la acción realizada, de esa manera la DPDP consideró subsanado el hecho.

4° medida de seguridad: incumplimiento del art. 42 RLPDP, en el que lo importante es el ambiente donde se guarda la documentación no automatizada; de esa manera la DFI informó a la DPDP que la administrada subsanó el hecho infractor, brindando un ambiente aislado con puerta y con un personal a cargo.

5° medida de seguridad: incumplimiento del art. 43 RLPDP, se desprende que el uso de las copias generadas o reproducción de documentos solo se realizan con el personal autorizado. La DFI, en la evaluación pertinente, apreció que el equipo del jefe de cómputo no

contaba con una contraseña ni usuario, posteriormente la administrada subsanó lo alegado por la DFI. En consecuencia, esto se informó a la DPDP, sin embargo, esta no consideró como subsanado.

Como recomendación, la DFI recomendó imponer una sanción administrativa por el primer hecho infractor que vulnera el art. 132, numeral 2, literal a del RLPDP, con una multa de 9 UIT, y por la vulneración del art. 132, numeral 1, literal a del RLPDP, con una multa de 1 UIT.

Undécimo Exp. N.º 154-2019-JUS/DGTAIPD-PAS

RN N.º 2077-2020-JUS/DGTAIPD-DPDP (1° instancia)

De lo recabado por la DFI se encontró que la PAS: Clínica del Pacífico SA realizó los siguientes hechos:

1° Hecho infractor: no se habría cumplido con implementar las medidas de seguridad para el tratamiento de datos sensibles que se realiza a través de los sistemas denominados "RIS" y "PACS".

A. No documentar los procedimientos de gestión de accesos.

B. No generar ni mantener registros de la misma interacción lógica de banda de datos.

2° Hecho infractor: se realiza el tratamiento de datos personales omitiendo la obligación regulada en el art. 17 de la LPDP.

De esta manera, la DFI recomienda imponer:

Por el 1° hecho infractor, la sanción de 5,5 UIT.

Por el 2° hecho infractor, la sanción de 20 UIT.

Duodécimo Exp. N.º 068-2018-JUS/DPDP-PS

RD N.º 515-2019-JUS/DGTAIPD-DPDP (1° instancia)

De lo recabado por la DFI se encontró que la Clónica Médica Cayetano Heredia S.A. realizó los siguientes hechos:

1° Hecho infractor: afectación de artículo 18 por el tratamiento de datos personales a través del "formulario de consultas" de su sitio web www.cmch.com.pe.

2° Hecho infractor: tratamiento de datos personales que fueron recopilados mediante "formulario de consultas", donde la fórmula de consulta resulta ser inválida.

3° Hecho infractor: no tener las medidas adecuadas para el tratamiento de datos personales que incluyen datos sensibles.

A. La DPDP alega que, durante la fiscalización realizada por la DFI, no se encontraba con las medidas adecuadas. Posteriormente, la administrada confirma ello a través de su descargo, puesto que en el momento de la inspección no contaba con la documentación que pueda acreditar; sin embargo, posteriormente realizó una subsanación, y la DPDP consideró esta acción como una enmienda.

B. No generar ni mantener registros de la misma interacción lógica de banco de datos.

De esta manera, la DFI recomienda imponer:

Por el 1° hecho infractor, la sanción de 2.5 UIT.

Por el 2° hecho infractor, la sanción de 2.5 UIT.

Por el 3° hecho infractor, la sanción de 5 UIT.

Décimo tercero Exp. N.º 150-2018-JUS/DGTAIPD-PAS

RD N.º 1529-2020-JUS/DGTAIPD-DPDP (1° instancia)

De lo recabado por la DFI se encontró que la Clínica Morillas S.A realizó los siguientes hechos:

1° Hecho infractor: afectación al artículo 13, puesto que se difundieron imágenes de las personas de la web www.clinicamorillas.com, además de usar datos personales de pacientes para finalidades no vinculadas al giro de negocio de la empresa.

2° Hecho infractor: tratamiento de datos personales que son recopilados por el sistema cliente/servidor LOLCLL 9000, por medio de formularios físicos, entre ellos historia clínica,

consentimiento informado para anestesia local, plan de mejora de la historia clínica, plan de mejora de la historia clínica, indicaciones de médico, plan de mejora de la historia clínica, informe médico alta, consentimiento informado para recopilar, registrar, almacenar, conservar, transferir, difundir y utilizar datos personales de pacientes, y consentimiento informado para recopilar, registrar, almacenar, conservar, transferir, difundir y utilizar datos personales de pacientes menores de edad, todo ello afectando el artículo 18 de la LPDP.

3° Hecho infractor: afectación del artículo 26 del reglamento de la LPDP, por no haber comunicado a la DGTAIPD la inscripción del RNPDP. Asimismo, el uso de flujo transfronterizo porque el servidor físico se ubica en Estados Unidos.

4° Hecho infractor: no implementar con seguridad adecuada los datos personales que incluyen datos sensibles.

De esta manera, la DFI recomienda imponer:

Por el 1° hecho infractor, la sanción de 8 UIT.

Por el 2° hecho infractor, la sanción de 8 UIT.

Por el 3° hecho infractor, la sanción de 1.5 UIT.

Por el 4° hecho infractor, archivar el Ps.

Décimo cuarto Exp. N.º 143-2019-JUS/DGTAIPD-PAS

RD N.º 1944-2021-JUS/DGTAIPD-DPDP

De lo recabado por la DFI se encontró que la PAS: Clínica del Pacífico SA realizó los siguientes hechos:

1° Hecho infractor: la administrada, a través de formularios físicos, no estaría brindando la información pertinente contenida en el art. 18 de la LPDP; sin embargo, la administrada presenta un descargo alegando que se cumple con lo que se debe informar; no obstante, la DPDP considera que la enmienda realizada no es suficiente.

2° Hecho infractor: la DFI alega que la administrada no presenta una inscripción del banco de datos personales en la RNPDP, ante lo cual la administrada presentó un descargo alegando que no tiene por qué tener un banco de datos, puesto que no tiene proveedores directos.

De esta manera, la DFI recomienda imponer:

Por el 1° hecho infractor, la sanción de 5,5 UIT.

Por el 2° hecho infractor, archivar el acotado.

Décimo quinto Exp. N.º 134-2018-JUS/DGTAIPD-PAS

RD N.º 418-2021-JUS/DGTAIPD-DPDP

De lo recabado por la DFI se encontró:

Hecho infractor: la DFI determinó que la administrada no otorgaba información con respecto al tratamiento de datos personales, por ello presenta un descargo sugiriendo y argumentando la enmienda realizada por las observaciones realizadas.

De esta manera la DFI recomienda imponer:

Por el hecho infractor, la sanción de 15 UIT.

Décimo sexto Exp. N.º 139-2019-JUS/DGTAIPD-PAS

RD N.º 1981-2020-JUS/DGTAIPD-DPDP

De lo recabado por la DFI:

1° Hecho infractor: se encontró que la administrada no brindaba información concerniente al tratamiento de datos personales, y esto se puede dilucidar por tres aspectos:

- A través del sistema cliente/servidor la administrada realizaba tratamiento de datos personales.
- Mediante la política de privacidad la administra no informó correctamente los estipulado en el art. 18 de la LPDP; sin embargo, la administrada implementó carteles

informativos y alegó que los pacientes completaban el formulario luego de leer la política de privacidad.

- La administrada informaba sobre las cámaras de vigilancia, pero no informaba completamente sobre el tratamiento de los datos personales, puesto que no se detallaba el tiempo de conservación de estos; sin embargo, las fotografías presentadas se realizaron antes de la imputación de cargos.

2° Hecho infractor: dentro de la fiscalización se constató que no se contaba con documentos de gestión de privilegios y usuarios, sin embargo, la administrada, mediante un descargo, acredita que sí lo realizaba, no obstante, no lo presentó adecuadamente y afectó así la propia acreditación.

De esta manera, la DFI recomienda imponer:

Por el 1° hecho infractor, la sanción de 7 UIT.

Por el 2° hecho infractor, la sanción de 2,5 UIT.

Décimo séptimo Exp. N.º 111-2019-JUS/DGTAIPD-PAS

RD N.º 313-2021-JUS/DGTAIPD-DPDP

De lo recabado por la DFI se encontró que la Ópticas GMO Perú S.A.C realizó los siguientes hechos:

1° Hecho infractor: realizar tratamiento de datos personales a través del sitio web http://gmo.com.pe sin informar lo solicitado por el artículo 18 de la LPDP; sin embargo, la DPDP considera que se debe acreditar de manera objetiva para poder desarrollar el supuesto ilícito cometido por la administrada.

De esta manera la DFI recomienda imponer:

Por el 1° hecho infractor, la sanción de 7 UIT.

4.3. ¿Cuál es la Motivación de la ANPD en las Resoluciones de los Establecimientos de Salud en los Años 2020 y 2021?

Para ello, es idóneo señalar ciertos aspectos que hagan entender lo esencial que es motivar de manera correcta un acto procesal, que para la investigación se denomina RD, las cuales son emitidas por la DPDP en primera instancia y DGTAIPD en segunda instancia (apelación).

La importancia y necesidad de la motivación

Tal como indicaba Luis Manuel Liza Castillo, es importante una debida motivación en los actos procesales, puesto que es un derecho constitucional (art. 139 numeral 5) que poseen los sujetos dentro de un proceso de cualquier índole, ya sea penal, civil, administrativa y pertinente para que conozcan las razones fácticas y jurídicas que los funcionarios y/o autoridades adoptan para resolver el conflicto. En caso de que estas decisiones no sean debidamente motivadas, causan agravio, es decir, para tener una decisión en derecho, se deben exponer las razones de hecho y derecho que dictaminan la parte resolutiva en un sentido u otro, pero dicha motivación no es ilimitada, puesto que deberá regirse y determinarse con las leyes pertinentes, además de considerar la doctrina y jurisprudencia nacional e internacional.

Mediante la Casación N.º 2799-2005, se hace mención que:

> La Constitución […] requiere que el Juez motive sus decisiones, ya que, de esta manera, la ciudadanía realiza un control de la actividad jurisdiccional. Así mismo, las partes intervinientes en el proceso saben las razones por las cuales es concebible o denegada la tutela concreta de un derecho o un interés legítimo; por lo cual, los jueces deben mencionar el proceso mental y analítico que los ha llevado a tomar esa decisión, cumpliendo así con la potestad de impartir justicia […].

El TC indica, en el Exp. N.º 0090-2004-AA/TC, que se brinda motivación a casos en los que se genera la vulneración de datos personales por parte de las entidades de salud, puesto

que dichos datos tienen un carácter de interés público y afectan a los usuarios que eligen cuidar su salud y proporcionan su información personal, la cual luego se comparte sin su consentimiento; por lo que es importante motivar correctamente el acto procesal administrativo a la hora de resolver y brindar las razones idóneas de por qué la parte resolutiva irá en un sentido. Se debe agregar que también se analizan como hechos infractores que no se brinde un correcto tratamiento de los datos personales, el indebido o inexistente registro del banco de datos ante la RNPDP, lo que permite proteger los datos personales y/o sensibles con la finalidad de no transgredir el derecho a la intimidad y privacidad, así como los derechos ARCO que atañen al usuario/cliente.

Jurisprudencia y doctrina sobre la motivación

En materia doctrinal, la revista oficial del Poder Judicial refiere la importancia de la motivación de las resoluciones, puesto que una decisión tomada radica, entre otros aspectos, en asegurar el principio normativo del debido proceso como manifestación del principio de protección procesal. En este sentido, es responsabilidad de las autoridades, especialmente de aquellos encargados de administrar justicia, presentar de manera clara y organizada los fundamentos legales y fácticos que respaldan su decisión, ya que la ausencia de argumentos sólidos y coherentes indicará la falta de motivación o justificación en la resolución, haciéndola inconstitucional. Esta omisión conlleva la anulación de la decisión y, además, se pueden imponer sanciones civiles, penales y disciplinarias al autor, según la gravedad del perjuicio causado, ya sea a petición de una parte o de oficio.

De forma jurisprudencial, según el Exp. N.º 04123-2011-PA/TC LIMA, el TC expresa que la motivación radica en el derecho a la certeza, que garantiza a los administrados que las decisiones estén respaldadas por un razonamiento jurídico explícito que vincule los hechos con las leyes aplicables, siendo este requisito esencial tanto para actos reglados como discrecionales, y esencial para la vigencia del principio de legalidad en un Estado de Derecho.

La jurisprudencia ha reiterado que la motivación adecuada es una condición indispensable para el debido procedimiento administrativo, y su ausencia constituye una vulneración de las garantías procesales. El TC en el Exp. N.º 00744-2011-PA/TC, se pronuncia alegando que la motivación debe ser proporcional al contenido del acto y conforme al ordenamiento jurídico. Además, debe ser expresa, relacionando hechos probados relevantes y exponiendo razones jurídicas. Por otra parte, se permite la motivación mediante referencia a dictámenes anteriores, siempre que se identifiquen claramente; mientras que se prohíben fórmulas generales, vagas o contradictorias que no aclaren específicamente la motivación del acto.

De manera específica, el TC ha indicado que la motivación protege al administrado contra la arbitrariedad de la Administración al emitir actos administrativos; y la LPAG, en su Título Preliminar, señala al debido procedimiento como uno de los principios del procedimiento administrativo, reconociendo a los administrados el derecho a ofrecer pruebas, exponer argumentos y recibir una decisión que se encuentre debidamente motivada y fundamentada en derecho.

Por todo lo expresado, se afirma que la motivación debida del acto administrativo es de importancia porque así se llega a una decisión que sea justa y razonable, además de estar debidamente fundamentada; y no por un mero capricho de una idea preconcebida; por el contrario, esta encuentra su límite en normativa concreta, como lo es la LDPD y su reglamento, así como la norma general que es la LPAG. Además, una debida motivación del hecho infractor que postula la DFI conlleva a imponer una sanción razonable, cumpliéndose con el art. 39 de la LPDP que la regula. A partir de ello, realizar una suerte de rectificación sobre un hecho insidiosamente incorrecto, como lo es la vulneración, indebido tratamiento y demás ilicitudes que afecten la seguridad de los datos personales y/o sensibles por entidades de salud.

Análisis de la motivación expresada en las RD

En la presente investigación, respecto del análisis de las resoluciones, se vislumbra la competencia que tiene la directora de Protección de Datos Personales para resolver en primera instancia el PAS, siendo que el art. 74 del Reglamento de Organización y Funciones del MINJUS indica que la unidad orgánica que es competente para resolver en 1° instancia es la DPDP, referente a procedimientos administrativos sancionadores que la DFI inicia. Asimismo, es conocedora y resolutora de los procedimientos trilaterales de tutela que los administrados pueden ejercer; también es el órgano competente para brindar el trámite correspondiente a los recursos de reconsideración que se puedan presentar, de acuerdo a lo que dispone el art. 219 del TUO de la LPAG.

Además, la DPDP, en su análisis, señala las "cuestiones previas", las cuales versan, en su mayoría, sobre la vinculación entre el informe de instrucción y el pronunciamiento que van a emitir, ello en concordancia con el art. 254 y 255 de la LPAG; en consecuencia, realizan una separación de lo que es la autoridad instructora y lo que es la autoridad sancionadora, también conocida como resolutora, puesto que ambas poseen autonomía sobre los criterios que expresan. Así, la autoridad sancionadora-resolutora puede hacer suyo lo que expresa la autoridad instructora, ya sea los argumentos, recomendaciones, conclusiones a las que arriba; no obstante, también podrá realizar apreciaciones disímiles, ya sea cuestionando hechos o brindando una valoración distinta a los hechos imputados, y eso no significa que se afecta la predictibilidad o expectativa del administrado, ni menos una vulneración al debido procedimiento que, en todo momento, debe ser resguardado. Es importante resaltar que las cuestiones previas analizadas dependerán del caso administrativo a resolverse.

Por otra parte, respecto a la responsabilidad de la administrada, se considera la aplicación del art. 257, numeral 1, literal f de la LPAG, que establece como eximentes de responsabilidad, la corrección voluntaria del acto infractor, y que se lleve a cabo antes de recibir la notificación de los cargos imputados. Así también, el art. 126 del RLPDP contempla los

factores de disminución de la responsabilidad, como son la cooperación con las autoridades y admisión voluntaria de las infracciones, siempre y cuando se tomen medidas correctivas, además de que esta puede concluir a una reducción justificada de la sanción, incluso por debajo de los límites establecido en la LPDP. En concordancia, se debe considerar junto con el art. 257, numeral 2 de la LPAG, ya que la condición para la atenuante es que el infractor reconozca explícitamente y por escrito su responsabilidad, y ahí se reduce la multa hasta no menos de la mitad del monto que se dictamina como importe, así se considerarán los atenuantes que se contemplen en normas especiales. Asimismo, para determinar una multa, se consideran los criterios de graduación que establece el art. 248, numeral 3) de la LPAG.

Asimismo, se han analizado resoluciones elevadas en grado, siempre y cuando el criterio es discordante con lo dictaminado en 1° instancia. Al respecto, previamente al análisis de los agravios incoados por el/la administrado(a), se indica que la DGTAIPD se encarga de resolver en segunda y última instancia administrativa procedimientos iniciados por la DPDP; además, para la admisión del recurso se analiza que se haya impugnado dentro de los días hábiles permitidos, que son 15 días de notificada la resolución de primera instancia.

Primer Exp. N.º 143-2018-JUS/DGTAIPD-PAS

RD N.º 1885-2020-JUS/DGTAIPD-DPDP (1° instancia)

1° Hecho infractor: La DPDP incoa el art. 5, art. 13, inciso 13.5 de la LPDP, puesto que el primero hace referencia al principio de consentimiento, y el segundo respecto a los alcances, haciendo énfasis que los datos personales solo serán objeto de tratamiento cuando el titular haya brindado su consentimiento, pero debe ser otorgado de manera inequívoca, expresa, informada y previa, esto se correlaciona con el art. 12 del RLPDP. En la misma línea, la DPDP refiere al art. 14 de la LPDP que indica las excepciones en las cuales el consentimiento no es necesario. Ahora, respecto al hecho analizado, la DPDP determina que la imputación se da por la evaluación que realiza la DFI del documento “autorización de uso de datos personales en

historia clínica", ya que induce en error al interesado, puesto que se solicita el consentimiento por todas las finalidades que son esenciales para que se dé la ejecución de la relación contractual, aun cuando no es así, no brindándole la opción al interesado de aceptar o rechazar cada una de manera individual. Asimismo, indica que la administrada no informa de manera correcta la finalidad del tratamiento cuando consigna en un apartado el término "entre otros"; mientras que la DPDP hace suyo lo indicado por la DFI en su evaluación, en referencia a que la fórmula que usa la administrada no posee la característica de ser informada ni libre sobre el consentimiento. Otro punto que analiza la DPDP tiene que ver con el hecho de que la administrada en su primer descargo, adjunta un documento sin modificación de la "autorización de uso de datos personales en historia clínica". Luego, adjunta el documento con las enmiendas realizadas, indicando que lo implementó antes de la notificación de la RD. La DPDP determina que, de analizado el documento, retiran la finalidad para la cual era necesaria que solicite el consentimiento y no tenía fecha cierta según lo establece el art. 245 del Código Procesal Civil. Se consideró la data de su escrito donde se adjunta este medio probatorio; aunado a ello, se debe considerar el art. 67 de la LPAG que indica que la información que se declare sea verificada por el administrado y compruebe su autenticidad, así como medio que se ampare en el principio de presunción de veracidad. Por ello, la DPDP considera dicho documento como una acción de enmienda en la responsabilidad que le atañe a la administrada, por ser de fecha posterior a la notificación del PAS de inicio, lo cual reitera en su fundamento expresado respecto al descargo posterior que realiza la administrada, siendo responsable por el hecho infractor y poseyendo a su favor las acciones de enmienda.

2° Hecho infractor: la DPDP señala que los titulares de los datos personales tienen el derecho de ser informados del tratamiento de su información, la recopilación, conservación, almacenamiento e idóneo. Lo importancia de dicho artículo radica en lo siguiente: su referencia al consentimiento que se debe entender juntamente con el art. 5 de la LPDP o en aquellos casos

que no se requiera a través del art. 14 de la LPDP. Ahora bien, la DPDP indica que, mediante dos actas de fiscalización, constata que la administrada recopila datos personales mediante su sistema y/o aplicativo, pero que no está en la obligación de solicitar el consentimiento para ello; sin embargo, eso no la exime de informar respecto al tratamiento que brindará a estas, lo cual la administrada prueba que realiza mediante su descargo de fecha 15 de agosto del 2019, cumpliendo con el art. 18 de la LPDP, y ello lo realiza con anterioridad a la notificación de la resolución que da inicio al proceso administrativo sancionador, por lo que se le debe eximir de responsabilidad.

Segundo Exp. N.º 110-2019-JUS/DGTAIPD-PAS

RD N.º 1436-2021-JUS/DGTAIPD-DPDP (1° instancia)

1° Hecho infractor: la DPDP señala el art. 17, el cual indica la confidencialidad de los datos personales, y refiere que las entidades que tratan los datos personales poseen la obligación de guardar confidencialidad sobre estos. Asimismo, brinda una definición de lo que es el tratamiento de datos personales y transferencia de datos personales que lo contiene el art. 2, numeral 19 y numeral 18 del mismo cuerpo normativo, respectivamente. La DPDP indica que la DFI imputa a la administrada haber brindado datos personales de su paciente a Avianca S.A., asegurando que fue un error, por lo que sancionaron a su colaboradora quién remitió dicha información, además de cursar una carta notarial a la empresa para que no utilicen la información; no obstante, la DFI mostró que la administrada comparte los datos personales a través de un correo electrónico y corroboró la documentación presentada por la administrada. Una precisión que realizó la DPDP es que la administrada presentó sus descargos después de realizada la notificación del cierre de la etapa instructiva, pues no se determinó el beneficio ilícito que poseen por cometer la infracción, si son o no reincidentes, el perjuicio económico o confiscatoria; asimismo, expresan que la multa recomendada los afectaría, aún más por la pandemia que se atravesaba en dicho momento; no obstante, reconocen haber brindado

información personal de su paciente y que esta no son datos sensibles, sino datos generales. Por otra parte, señalan que su conducta fue corregida voluntariamente y con anterioridad a la emisión de la resolución de sanción, también sancionaron a su trabajadora y reforzaron su procedimiento para evitar lo imputado. La DPDP indica que la DFI no imputa como una agravante que la información compartida haya sido sensible, sino que el hecho infractor se basa en la falta de confidencialidad de la administrada con su paciente sobres sus datos personales, expresándose de manera general; y por los actuados y el reconocimiento de la administrada del ilícito, se da por acreditado el incumplimiento del art. 17 (confidencialidad). Además, su accionar fue instantáneo porque se configuró cuando se transfirió la información sin consentimiento del titular, no pudiendo ejercer acción de enmienda la administrada porque ya Avianca (tercera entidad) poseía la información, sin perjuicio que la administrada realice acciones idóneas para no repetir el hecho infractor. Ello lo demuestra con el documento que presenta. La DPDP resalta que aplicará los criterios establecidos mediante Resolución Ministerial N.º 0326—2020-JUS con respecto a la multa.

Tercer Exp. N.º 127-2018-JUS/DGTAIPD-PAS

RD N.º 1045-2020-JUS/DGTAIPD-DPDP (1° instancia)

1° Hecho infractor: la DPDP incoa el art. 5 de la LPDP, el cual hace referencia al principio de consentimiento. Asimismo, al art. 13, inciso 13.5 del mismo cuerpo normativo, que informa que los datos personales solo serán objeto de tratamiento cuando el titular brinde su consentimiento, el cual debe ser otorgado de manera previa, expresa, inequívoca e informada; incluso ello se colige con el art. 11 y 12 del RLPDP: el primero indica las disposiciones generales del consentimiento sobre el tratamiento de datos personales, y el segundo las características de este. Asimismo, indica que se deben tener en cuenta las limitaciones del consentimiento que regula el art. 14 de la LPD. Aunado al análisis de lo propuesto por la DFI en sus informes, la DPDP señala que un hecho infractor debe ser

detectado, indagándose sobre este; es decir, no solo basta con verificar o visualizar el contenido o la composición de la página web de la administrada, sino la importancia radica en investigar si la divulgación de las imágenes ha sido autorizada por sus propietarios (titular de la imagen); y la DFI debe requerir dicha información al administrado. La DPDP indica que de autos no se acredita dicho accionar, y que en la etapa previa al inicio del proceso sancionador, solo se da a conocer la difusión de imágenes, por lo que, no habiéndose requerido dicha información a la administrada, ya sea por oficio o cuando se realizaron las visitas de fiscalización, pese al conocimiento de la difusión de las imágenes, no se exige ni se brinda la oportunidad de que la administrada se pronuncie; en consecuencia, la DPDP no propugna como objeto de sanción este hecho infractor.

2° Hecho infractor: la DPDP primero indica que el art. 18 de la LPDP se refiere a la obligación que posee el responsable del tratamiento de los datos personales de proporcionar información detallada al titular de los datos sobre cómo se utilizarán estos, cómo se recopilarán, su tratamiento, y demás, siendo que la referencia del art. incoado va más allá del simple consentimiento, lo que genera que el titular pueda ejercer sus otros derechos de manera efectiva; por tanto, la DPDP analiza punto por punto respecto al indebido tratamiento de datos personales. Su postura es la siguiente:

- **1° medio:** la DFI señala que en lo que refiere a política de privacidad: i) no se proporcionaba información sobre quiénes recibirían los datos personales; ii) la existencia del banco de datos donde se guardaría; iii) si hubiese transferencias nacionales o internacionales; y iv) cuánto tiempo se conservarían esos datos. Al respecto, la DPDP señala que la administrada presentó una nueva versión de su política de privacidad e indica que, respecto al punto i), ii) e iv), cumple con enmendar las omisiones que se le imputó; sin embargo, el punto iii) no se cumple, puesto que la administrada no informa que realiza transferencia internacional, pues el servidor físico

donde se almacena la información de los datos personales que recopila está en Estados Unidos. Sobre este punto, si bien existe responsabilidad por parte de la administrada, también se tienen acciones de enmienda para atenuarla.

- **2° medio:** la DPDP analiza que la administrada, en respuesta a su requerimiento de información, explicó que el personal del archivo es quien hace el registro de las historias clínicas, haciendo dicha gestión de manera indirecta, porque las solicitudes de atención se gestionan por el área de Admisión. Además, en el acta de fiscalización del 25 de julio del 2018 se advierte que el tratamiento automatizado de historias clínicas se lleva a cabo mediante un archivo Excel gestionado por el auxiliar de archivo; por ello la DPDP advierte que Excel es una herramienta que tiene como acceso restringido al personal del área de Archivo; en consecuencia, no sería aplicable el art. incitado como vulnerado (art 18 de la LPDP), y no sería objeto de sanción.
- **3° medio:** la DPDP señala que el sistema LOLCLI 9000++ es utilizado por ejecutivos del área de Admisión para que registren a pacientes que están en áreas de emergencias, hospitalaria y ambulatoria, siendo que solicitan su DNI y registran datos personales en dicho sistema, en la interfaz, puesto que la recopilación la realizan de manera verbal y directa con el paciente, y a través del Acta de Fiscalización N.º 1-2018 se verifica que la administrada no daba cuenta del tratamiento de los datos personales recolectados, no contaba con un formato que explique esto. Así, la DPDP indica que el derecho de información es esencial de toda persona natural cuando del tratamiento de sus datos personales se trata, puesto que permite el conocimiento de la finalidad de su recopilación a quiénes o a quién se transfieren, la forma y, más que nada, porque así se permite que ejerza sus derechos ARCO. Dicha información debería ser accesible e identificable, y el conocimiento de esta debe ser sobre lo relevante y conexo al tratamiento.

La DPDP indica que lo apropiado es que la administración disponga de un documento impreso que informe sobre la privacidad, protección y tratamiento de datos personales de los pacientes y usuarios de los servicios médicos, documento que debería ser accesible y estar en lugares visibles, como los *counters* o áreas de admisión. Así, se proporcionaría una guía informativa para el público, incluyendo pacientes y sus representantes legales o apoderados, que se presenten físicamente en las instalaciones del establecimiento de salud. La DPDP indica que, con ello, la administrada perfecciona lo que se le imputa como hecho infractor. En la misma línea, considera la inmediatez con la que se lleva a cabo la atención a los pacientes en dichas circunstancias de emergencias, urgencias, hospitalizaciones y demás; por dicho análisis, concluye que la administrada incumple con el deber establecido en el art. 18 de la LPDP.

- **4° medio:** la DPDP identifica un sistema cliente/servidor llamado "sistema gestión", mencionado por la administración como de uso interno y que se apoya en la información del sistema LOLCLI 9000++; y constata que ambos sistemas comparten una misma base de datos. El sistema gestión se alimenta del sistema LOLCLI 9000++, por lo que el art. 18 de la LPDP no se aplica, y no es sujeto a sanción.
- **5° medio:** la DPDP indica que sustrae el análisis de ilicitud, puesto que no se desarrolla el contenido explicativo de este, no pudiéndose motivar la imputación.
- **6° medio:** la administrada aclara que este documento es una impresión de los datos registrados previamente en el sistema LOLCLI 9000++. Por lo tanto, la DPDP indica que no constituye un método adicional de tratamiento de datos, sino más bien una reproducción de la información previamente recopilada, sustrayéndose su análisis como hecho infractor.

3° Hecho infractor: la administrada en sus descargos indica que solo tiene pendiente la inscripción del banco de datos de médicos y la DFI se pronuncia mediante su informe final de instrucción, brindando como recomendación que se archive en este extremo el PAS. Al

respecto, la DPDP indica estar de acuerdo con lo expresado por la DFI, por lo que se confirma el archivamiento definitivo.

4° Hecho infractor: la DPDP precisa la definición de lo que es la transferencia de datos personales (art. 2, numeral 18 de la LPDP), que existe la obligación de poner en conocimiento a la DPDP (art. 26 del RLPDP) y qué es objeto de inscripción (art. 34 de la LPDP y art. 77 del RLPDP); siendo así, la DPDP señala que, si bien existe una solicitud de la administrada para la inscripción del flujo transfronterizo, esta fue observada, pero no se realizaron las subsanaciones incoadas; por tanto, la administrada tiene responsabilidad al respecto.

5° Hecho infractor:

- **A y B:** al respecto: i) no registrar los procedimientos para gestionar los privilegios y realizar verificaciones periódicas de los privilegios asignados; ii) no realizar el cierre de sesión de los usuarios como resultado de su actividad en los sistemas que registran el tratamiento de datos personales. Mediante informe técnico, la DFI indicó que la administrada presenta documentación adicional donde se advierte que si cumple con el punto i) y ii), pero dicha evaluación del cumplimiento que realiza es con posterioridad y anterioridad al informe técnico emitido por la DFI.
- **C:** la DFI indica que la administrada no dispone de las medidas de seguridad idóneas en su "centro de datos", el cual está ubicado en un entorno aislado con una puerta que no cuenta con cerradura, y carece de extintores, un tablero eléctrico independiente y sistemas de alarmas contra incendios. Al respecto, la DPDP señala que la administrada ha cumplido con implementar todo ello, puesto que brinda sus descargos.
- **D:** la DPDP expresa que se debe archivar este extremo porque no se desprende la comisión de dicha infracción, puesto que el acta de fiscalización no cuenta o vislumbra que el área de Admisión no sea de acceso restringido o que esté al encuentro del público en general y pertinente. Además, en el descargo que brinda la administrada, vislumbra

que las historias clínicas se encuentran almacenadas en el *caunter* y que el acceso se restringe al personal de la administrada (clínica), pues dicha insinuación no ha sido contrarrestada en la fase de instrucción.

- **E:** la DFI también indica que la administrada no genera reproducción o copias a los documentos conexos a datos personales y/o sensibles que provienen de las historias clínicas; sin embargo, no se llega a observar ello, por lo que la DPDP archiva dicho extremo.

Por todo ello, la DPDP concluye que, si bien la administrada llega a tener responsabilidad de lo ya expresado, se consideran las atenuantes de las que es pasible para su graduación de sanción.

Cuarto Exp. N.º 144-2018-JUS/DGTAIPD-PAS

RD N.º 1459-2020-JUS/DGTAIPD-DPDP (1° instancia)

1° Análisis: la DPDP inicia incoando al art. 219 de la LPAG, el cual indica que el recurso de reconsideración se interpone ante el mismo órgano que ya emitió pronunciamiento sobre el caso, siendo un requisito primordial el presentar nueva prueba para que la autoridad pueda sustentar y emitir un nuevo criterio; es decir, al presentarse dicho recurso, el administrado busca que la autoridad varié su criterio y solo se dará ese supuesto cuando se evalúe que haya un nuevo hecho o prueba que no fue presentada o cuya actuación no se solicitó por desconocimiento de que existía o, en su momento, había imposibilidad de obtenerla y no fue valorada; sin embargo, no todos los elementos probatorios nuevos son idóneos para una reconsideración. Los nuevos hechos deberán ser tomados en conocimiento por la administrada después de la instrucción o que haya habido una imposibilidad para que se conozcan. La DPDP agrega que no se trata de realizar una argumentación jurídica nueva que ya habría evaluado o explicado técnicamente el hecho, por lo que concluye que no califica como nuevas pruebas aquellas que, por razones no imputables a la autoridad, no se presentaron en el expediente.

Asimismo, indica que, de manera esencial, su análisis versará en si existe o no prueba nueva, y cuando se determine ello, la pertinencia para que se revise lo ya resuelto en la RD N.º 1108-2020.

2° Análisis: la DPDP indica que, del escrito presentado por la administrada, no advierte medios probatorios que brinden indicios de hechos novedosos o que no hayan sido conocidos por la administrada ni por la autoridad resolutora, por lo que no se permite brindar nuevos argumentos ni se vislumbra el requerimiento de una nueva revisión de los hechos, puesto que la administrada presenta sus argumentos de descargo resumidos, sin aportar prueba de por medio; tales argumentos ya están en el expediente y ya fueron evaluados en la resolución. Asimismo, la DPDP señala la inexistencia de prueba nueva que sustente lo que la administrada alega en su pretensión, con el fin de que se emita un nuevo pronunciamiento. Otro punto que toca la DPDP es que los medios probatorios presentados vislumbran la realización de cambios, pero ello sobre la base de lo que la DPDP expuso en la RD N.º 1108-2020, en sus considerandos 56 al 62; por tanto, no es una prueba nueva, sino modificaciones tomadas y acciones realizadas con fecha posterior a la RD.

Quinto Exp. N.° 207-2021-PTT

RD N.° 3454-2021-JUS/DGTAIPD-DPDP (1° instancia)

1° Análisis: la DPDP indica que el derecho fundamental a la protección de datos lo resguarda el art. 2, numeral 6 de la Constitución. A través del art. 1 de la LPDP se hace referencia a ello, añadiendo que el objeto de creación de dicha ley radica en la protección de los datos personales que se darán cuando haya un adecuado tratamiento de estos, dentro de un marco de respeto a otros derechos fundamentales que se reconocen. Además, se dará tanto en el sector público como privado. Por otra parte, también la DPDP refiere al art. 2, numeral 4 de la LPDP, por el cual se brinda una definición de lo que es un dato personal y se indica que es toda información que permite identificar o hace identificable a un sujeto por medios idóneos a

utilizarse; de igual manera, incoa el art. 16 de la misma ley, que define al titular de los datos personales como el sujeto a quien corresponde la información. La DPDP concluye que tanto obligaciones como principios que se encuentran en la LPDP y su RLPDP sirven para brindar de seguridad y resguardo a la protección de los datos personales; además, el titular podrá ejercer sus derechos ARCO, encontrándose todo esto previsto del art. 18 al 22 de la LPDP. Por tanto, la DPDP menciona que el titular de banco de datos personales, que puede ser una entidad, persona natural o jurídica, es decir, el responsable del tratamiento, tiene la responsabilidad de implementar mecanismos idóneos para que el titular de los datos personales pueda ejercer sus derechos y este atenderlos. Así, el art. 19 de la LPDP regula el acceso que posee el titular sobre sus datos personales, y complementariamente se entiende junto con el art. 61 de la misma ley. Por todo ello, la DPDP concluye que el titular de la información posee la facultad de acceder a sus datos, sin embargo, en el caso, la DPDP advierte que el administrado solicita que se le proporcione información que no se orienta a conocer cómo sus datos fueron recopilados, para qué, de qué forma, transferencias realizadas e idóneo que se relacione con dicha idea.

En esa misma línea, se precisa que no todos los pedidos de los titulares de los datos personales se deberán atender bajo el foco del derecho de acceso; por el contrario, para el caso se atenderá por el derecho de petición.

2° Análisis: la DPDP indica que el derecho de petición se encuentra reconocido por el art. 2, inciso 20 de la norma madre y que da viabilidad a los sujetos para que formulen sus peticiones de forma individual y conjunta, y por escrito ante la autoridad que sea competente, y esta, a su vez, está obligada a brindarles una respuesta por escrito en el plazo establecido por ley, bajo su responsabilidad. Asimismo, se indica que este derecho, de manera amplia, es regulado por el art. 117 y siguientes el TUO de la LPAG, y de manera específica, en el numeral 117.2 del citado artículo, se indica que el interesado tiene la facultad para solicitar informaciones, entendiéndose como obligado a las entidades. La DPDP realiza una precisión

respecto a que el derecho de petición podrá incluir información o no de los propios administrados, y si fuese así, no es motivo para que se niegue la atención al ejercicio de este derecho; en consecuencia, concluye que se debe atender al administrado en ejercicio de su derecho de petición, lo cual queda fuera de su ámbito de aplicación al ser incompetente en razón de la materia.

Sexto Exp. N.º 74-2018-JUS/DGTAIPD-PAS

RD N.º 3292-2019-JUS/DGTAIPD-DPDP (1° instancia)

1° Hecho infractor: la DPDP inicia citando el art. 18 de la LPDP e indica que todo titular de su información (datos personales) debe ser informado sobre el tratamiento que se les brindará a sus datos de manera clara, completa y dicha información debe ser accesible porque así se permite que el titular ejerza otros derechos que le atañen. Además, se resalta que esta obligación de informar es independiente al consentimiento. El despacho resolutor señala que, mediante RD, se imputa a la administrada tratar la información de los titulares por un sistema y formularios físicos. Al respecto, analiza que, en el caso de los formularios, carecen de texto informativo alguno que señala el art. 18 de la LPDP, a pesar de que recopilan información personal sobre salud. La administrada, en su descargo, señala que actúa de buena fe y con la intención de cumplir con la normativa que se le está aplicando; sin embargo, no adjunta documento pertinente al respecto; no obstante, posterior a ello, la administrada presenta un escrito con una nueva versión de uno de los formularios, el cual contiene lo que, mediante RD, se le indica, encontrándose transcrito. La DPDP indica que aprecian en dicho documento que facilitan información respecto al domicilio de la administrada, su identificación como responsable del tratamiento, así como indicaciones precisas sobre dónde se almacena la información del banco de datos y su modalidad de ejercicio de los derechos que poseen los titulares de la información. Sin embargo, el despacho resalta que, para configurarse el documento, aprecia que una compañía de seguros se contempla que brinda tratamiento, sin

mencionar su identidad; además, se omite contemplar el lapso de almacenamiento de los datos personales, y agrega que son tres formularios utilizados conjuntamente. La DPDP entiende que lo incluido en este documento como material informativo es aplicable a las otras. Por todo ello, la DPDP declara responsable a la administrada, y si bien tiene intención de enmendar su conducta, no la perfecciona, no siendo aplicable atenuación alguna.

2° Hecho infractor: la DPDP inicia señalando lo establecido por el art. 34 de la LPDP, por el cual se dispone la creación del RNPDP que tiene como fin inscribir los bancos de datos personales, ya sea de administración privada como pública, permitiéndose, también, que cualquier sujeto realice consultas sobre la existencia y finalidad de banco de datos personales inscritos, sobre la identidad y domicilio de sus titulares. Asimismo, el art. 78 indica la obligación que ostenta la administrada para la inscripción, y referente a la fiscalización, se tiene que esta no realiza dicha acción respecto a su videovigilancia y proveedores. Mediante escrito, la administrada indicó que realiza la inscripción de su banco de datos, para cumplir y colaborar con la autoridad, pero la RD N.° 1802-2019 negó dicho registro sobre el sistema de vigilancia; por tanto, la administrada solo enmienda su conducta respecto a los proveedores, no pudiéndosele aplicar la atenuación de su responsabilidad administrativa e incurriendo en una infracción leve.

3° Hecho infractor: al respecto, la DPDP indica que un principio rector es el de seguridad, y ello lo establece el Título I de la LPDP, además de encontrar su regulación en el art. 9 del mismo cuerpo normativo. Así también, el art. 16 de esta ley indicada señala el objetivo de la seguridad que se debe brindar al tratar datos personales, puesto que hay medidas organizativas, técnicas y legales a adoptarse, así como evitar la pérdida, alteración, acceso o tratamiento que no se autorice respecto a los datos personales. La DPDP añade que a la administrada se le detecta que brinda un tratamiento automatizado a datos los personales

sensibles, y brinda la definición establecida en el art. 2 de la LPDP, imputándosele la comisión del art. 132, numeral 2, literal c) del RLPDP: una infracción grave.

Por otra parte, el despacho señala que el art. 39, numeral 1, del RLPDP, contempla los requisitos de documentar los procedimientos de gestión de privilegios, accesos, verificación periódica de privilegios, esto con respecto al tratamiento automatizado de los datos personales que se pueda dar. Es así que, a través de lo indicado en el artículo mencionado, la DPDP señala que se establece la obligación de los responsables de brindar tratamiento al control de la gestión de accesos y toda acción que se realice con los datos personales, además de que se debe predeterminar el acceso y privilegios de acción sobre estos, a través del medio de determinación de los perfiles de usuario del sistema por el cual se realiza el tratamiento de los datos personales, y detallarse la metodología para retirarlos u otorgarlos, lo cual debe estar en un documento de contenido estable y accesible a los usuarios.

El despacho indica que, mediante informe técnico, dos formularios no documentan la periodicidad de la revisión de perfiles, incumpliendo con el art. 39 del RLPDP. Se señala que la administrada, en sus descargos, remite nuevas versiones sobre sus documentos de seguridad, pero según el informe técnico no se establece el proceso ni los periodos en los que se realiza la verificación de los privilegios que se hayan asignado. Además, la DPDP enfatiza que la administrada no remite documento de esto luego de cerrada la etapa instructiva, sin enmendar la conducta infractora.

Después, el despacho procede a señalar lo que dispone el art. 39, numeral 2 del RLPDP, y se establece a los responsables de cumplir con su obligación de contar con registros de los pormenores de cada operación relevante respecto al tratamiento de datos personales, la identidad de quién lo realiza, el momento y en qué consistió. En la segunda visita de fiscalización, se constata que la administrada contaba con un sistema que brindaba tratamiento de los datos personales de los pacientes, pero verificado ello, se tiene que no genera ni se

mantienen registros de interacción lógica con esta información, siendo un hecho infractor según la RD. Al respecto, la administrada no remite documento que sustente el mantenimiento ni generación de esos registros, lo que se reitera en su escrito una vez cerrada la etapa instructiva, no teniéndose prueba de dicha implementación (acción correctiva).

La DPDP indica lo dispuesto por el art. 42 del RLPDP, el cual señala que la documentación no automatizada que contiene datos personales debe estar fuera del alcance de la generalidad del personal de la entidad responsable del tratamiento o a disposición de cualquier sujeto que acceda al establecimiento de la administrada; por ello se debe tener herramientas como la apertura con llave o equivalente, para que se garantice la confidencialidad, integridad y disponibilidad de la información para aquel que sí esté autorizado en realizar el tratamiento de ello. El despacho señala que, durante la fiscalización, se verificó que las historias clínicas se custodiaban en ambiente con puerta cerrada, pero no tenía una llave asignada a su personal responsable. En sus descargos, la administrada señala que ha estado implementado una puerta con cerradura y remite un acta de constatación notarial, en la cual describe los horarios de trabajo de los responsables del ambiente e incluye una foto de la apertura de la llave con cerradura. Además, la DPDP indica que dicho documento cuenta con fecha cierta, siendo más que suficiente ello para que el despacho lo considere como una acción de enmienda, debiendo ser analizado como atenuación a la responsabilidad que se le imputa a la administrada al encontrársela responsable de la infracción considerada como grave.

Séptimo Exp. N.º 141-2018-JUS/DGTAIPD-PAS

RD N.º 1049-2020-JUS/DGTAIPD-DPDP (1° instancia)

1° Hecho infractor: la DPDD incoa el art. 5 de la LPDP, que regula el principio de consentimiento. Además, del art. 13, inciso 13.5 de a LPDP, que indica que el consentimiento debe darse de manera inequívoca, expresa, informada y previa. De esta manera, podrán ser objeto de tratamiento. Se debe analizar juntamente con el art. 11 y 12 del RLPDP, al menos

que haya excepciones, indicadas en el art. 14 de la LPDP. Al respecto, la DPDP señala, luego de revisado el informe técnico de la DFI, que la administrada no cuenta con su sitio web activo, no realizando un tratamiento de datos personales; sin embargo, la DPDP identifica que la DFI imputa este hecho a un sitio web incorrecto, debiendo ser otro que también posee como titular a la administrada, indicando, de oficio, que se puede realizar la fiscalización y que, sin perjuicio de ello, la administrada tenga sus documentos con las autorizaciones correspondientes.

2° Hecho infractor: la DPDP indica que, si bien el art. 18 de la LPDP se relaciona con el consentimiento, su finalidad en sí es que al titular se le informe sobre el tratamiento que se les brindará a sus datos personales. Ahora bien, se le impone como hecho infractor tres puntos esenciales: el tratamiento de datos que se recopilan por el "sistema clínico", así como a través de formularios físicos y a través de su sitio web. El análisis es el siguiente:

- **1° medio:**
    - **A:** se analiza que la administrada utiliza formularios físicos donde se recopila información de los pacientes y, según la fiscalización realizada, no contaría con las cláusulas que informen el tratamiento de los datos personales. La DPDP ahí resalta la importancia como principal derecho el de la información que se debe brindar a una persona natural cuando versa sobre el tratamiento de sus datos, puesto que ello lo identifica y lo hace identificable. Además, se especifican las transferencias, cómo se hará y cuándo, y hace posible que ejerza sus derechos ARCO. En aplicación del art. 18 de la LPDP, el acceso a esa información del tratamiento debe ponerse a disposición del titular de los datos, así como hacer identificable y accesible su conocimiento. La DPDP concluye que es razonable que la administrada cuente con un formato impreso que indique e informe todos estos puntos (el tratamiento, protección, etc.), siendo de fácil acceso y visible al público. Dentro de los descargos de la administrada se tiene que presentar un documento sobre políticas de

privacidad con las que habría adecuado las observaciones que la RD de inicio realizó. Analizado el documento, la DPDP concluye que la administrada sí habría cumplido con informar aspectos relevantes que se relacionan con estas políticas; además, incluyen información respecto a que se recopilará en su página web a través del formulario, página que se encuentra debidamente inscrita en la RNPDP. Por otra parte, la observación que realiza la DPDP es que la administrada debe actualizar el código de los bancos de datos de pacientes y videovigilancias, puesto que pone unos disímiles a lo indicado por la RNPDP. En este sentido, la DPDP considera el accionar de la administrada de enmienda parcial, a razón de que, de su descargo, no se tiene fecha cierta de la presentación de los documentos y/o imágenes respecto a su difusión, si fue posterior o si esta sigue los lineamientos del art. 18 de la LPDP.

  - **B:** la DPDP indica que, si bien en la RD de inicio se señala que la administrada realiza tratamiento a los datos personales, por medio de un formulario físico y por cámaras de videovigilancia, lo hace sin contar con una política de privacidad idónea que informe ello, no cumpliendo con el art. 18 de la LPDP; sin embargo, no se expone ello de manera expresa como un hecho infractor, por lo que no puede ser objeto de sanción.

- **2° medio:** sobre el sitio web, se archiva este extremo en razón de que la RD de inicio presenta un formulario y políticas de privacidad pertenecientes a otro enlace de la administrada, siendo que la página web incoada se encuentra deshabilitada con anterioridad, no quitando que, de oficio, la DFI puede iniciar fiscalización respecto a la otra página web y abrir nuevos cargos si hay indicios suficientes para imputar un hecho infractor.

3° Hecho infractor: la administrada presenta su inscripción correspondiente, tiene su código señalado mediante RD que ha sido revisado por la web de la RNPDP; todos los bancos

de datos que constan en dicha resolución están debidamente inscritos bajo la titularidad de la administrada. Si bien la administrada ha señalado que está realizando cambios a su denominación social y a su nombre, la DPDP advierte que se varía el nivel de declaración respecto al nombre comercial ante la SUNAT, no siendo este relevante para la inscripción o modificación del banco de datos personales ante la RNPDP. Se considera que ello exime de responsabilidad, y se exige que dicho cambio de denominación social se actualice para que todo procedimiento sea transparente.

Octavo Exp. N.º 07-2019-JUS/DGTAIPD-PAS

RD N.º 1180-2020-JUS/DGTAIPD-DPDP (1° instancia)

1° Hecho infractor: al respecto, la DPDP indica lo dispuesto por el art. 13, inciso 13.5 de la LPDP, el cual señala que para que los datos personales se traten, debe existir consentimiento de ello por parte de su titular, y que este debe ser expreso, informado, previo e inequívoco. Asimismo, indica que dicho artículo se debe entender de forma conjunta con los artículos 11 y 12 del RLPDP; no obstante, dilucida la existencia de causales por las cuales no es necesario solicitar el consentimiento (art. 14 de la LPDP); en consecuencia, se imputa que la administrada difundía imágenes de personas en su página web sin previo consentimiento para ello; sin embargo, la DPDP indica que, en estos casos, para poder constatar el carácter ilícito, no se puede realizar una revisión únicamente, sino que se debe constatar que cada imagen cuente con el consentimiento de su titular. Del expediente administrativo se tiene solo las imágenes, pero no una constatación de cómo se obtuvieron estas y si hubo consentimiento para su difusión. En la fiscalización, y con anterioridad a esta, no se solicita a la administrada dicha información, no demostrándose la comisión de la infracción, por lo que no es pasible de ser objeto de sanción.

2° Hecho infractor: la DPDP refiere el art. 18 de la LPDP que indica el deber de información, y señala que los titulares de los datos personales poseen el derecho de ser

informados respecto al tratamiento que se realizará a su información personal, que se le indique el fin, el almacenamiento, la existencia de un banco de datos, y si es así, que se señale la conservación, el lugar, es decir, es nacional o internacional, e información pertinente.

Con la fiscalización realizada a la administrada, la DFI concluye en su informe de fiscalización que sería responsable por no informar del tratamiento de datos personales de sus pacientes y usuarios en lo que respecta al sitio web; es decir, vulnerándose el art. 18 de la LPDP, y ello configura una infracción grave que se encuentra regulada en el art. 132 del RLPDP. Si bien la administrada presenta sus descargos, no se llega a verificar el cumplimiento de dicha obligación, puesto que primero adjunta documentos para desacreditar la imputación y luego admite que, por desconocimiento, no realizaron gestiones idóneas para cumplir con la LPDP, si ser su intención. Luego del análisis a los documentos, la DPDP indica que el cambio realizado era más de forma que de fondo; asimismo, precisa que no se trata de poner bajo qué política y protección se tratan los datos personales o conceptos que dispone la LPDP, sino que lo importante reside en informar detalladamente las condiciones de tratamiento de estos. Por otra parte, también se analiza la página web de la administrada que no cumplía con brindar información sobre el tratamiento de los datos personales, pero la DPDP concluye que no se recopilaba información personal, puesto que cesaron con brindar el tratamiento, no requiriéndose contar con políticas de privacidad, por lo que la DPDP lo considera como una acción de enmienda, puesto que el cese fue posterior a la imputación de cargos. Por todo ello, la DPDP concluye que la administrada es responsable por no realizar su obligación de informar a los titulares de los datos personales respecto al tratamiento de estos, incurriendo en una infracción grave (literal a) del numeral 2 del art. 132 del RLPDP) al no cumplir con lo establecido en el art. 18 de la LPDP.

3° Hecho infractor: en la resolución se desprende que el art. 34 de la LPDP dispone la creación de la RNPDP, lo cual es importante porque permite que los ciudadanos puedan

acceder a información sobre los bancos de datos personales, y en el art. 78 de la LPDP se indica la obligación de su inscripción ante la RNPDP. Sobre el caso, se tiene que la administrada, al momento de la fiscalización, no habría inscrito los bancos de datos y, con el informe correspondiente, se concluye que por ello se afectó el art. 132, numeral 1 del RLPDP, siendo una infracción leve. En la motivación que brinda la DPDP refiere que la administrada era titular del banco de datos, por lo que tenía que registrar estos en el RNPDP y que, si bien la administrada presenta su descargo, no consta alegato que desvirtué lo que se le viene imputando; sin embargo, mediante otro informe, la DFI indica que la administrada ya no recopilaba datos personales en su sitio web, no siendo ya exigible la inscripción, lo cual comprueba la DPDP. Asimismo, en su segundo descargo, la administrada presenta la solicitud de inscripción que realiza, y se verifica en el RNPDP que efectivamente consta esta, cumpliéndose con el deber que se le imputa como infracción, pero fue posterior a la notificación de la resolución de imputación de cargos, lo cual es una acción de enmienda a la responsabilidad acreditada de la administrada.

4° Hecho infractor: la DPDP incoa el art. 34, numeral 2 de la LPDP, que describe las funciones de la RNPDP, a partir de las cuales se debe inscribir las comunicaciones de flujo transfronterizo de datos personales. Asimismo, el art. 26 del RLPDP establece la participación que tiene la DGPDP respecto al conocimiento de este. De la fiscalización se tiene que la administrada realiza tratamiento de datos personales a través de su sitio web y que el servidor que almacena esta información se encuentra en Canadá. En su primer descargo, la administrada indica que realizaron cambios a la página web y que ya no recopilan información; ello también lo indica la DFI mediante su informe, por lo que la administrada no realizaba flujo transfronterizo y ello es constatado por la DPDP. Se debe recalcar que la DPDP determina que la administrada cesa el tratamiento de los datos personales con posterioridad a la notificación, siendo esto un atenuante de la responsabilidad que posee por el hecho infractor; además, toma

como fecha cierta, respecto al cese, el día donde realiza su descargo, y que, a la fecha de emisión de la resolución, la administrada cumple en su totalidad con lo indicado por el art. 26 del RLPDP.

Noveno Exp. N.º 142-2018-JUS/DGTAIPD-PAS

RD N.º 1580-2020-JUS/DGTAIPD-DPDP (1° instancia)

1° Hecho infractor: la DPDP procede a realizar el análisis de las cuestiones en discusión e indica que la imputación versa sobre el incumplimiento del art. 18 de la LPDP; además, brinda la precisión de la obligación, que dictamina el artículo en mención, de informar al titular sobre el tratamiento de sus datos, ya sea que deba solicitar el consentimiento al titular sobre sus datos (art. 5 de la LPDP) o cuando no se requiera (art. 14 de la LPDP).

- **1° documento:** mediante el acta de fiscalización N.° 03-2018, se determina que la administrada, mediante papel, recopilaría datos personales de sus pacientes a través del "file historia clínica", siendo un soporte no automatizado que contenía otros documentos con datos sensibles. Si bien la administrada realizó su descargo indicando que estarían implementado lo referido por el art. 18, no adjuntó medio probatorio alguno, es así que la DPDP acredita dicho extremo. Además, el deber de informar sobre el tratamiento de los datos personales se realiza en un inicio, puesto que los demás documentos se generan a partir del llenado de la historia clínica.
- **2° documento:** recopila datos como sexo, nacimiento, nacionalidad, código, estado civil, grupo sanguíneo y demás pertinentes; asimismo, la DPDP indica que estos datos eran distintos a los requeridos en las historias clínicas. Si bien la administrada en su descargo señala que estarían realizando implementaciones, ello no se llega a observar. Otro punto a destacar es que motivan el art. 18 a razón de que el derecho de información es el principal derecho de un sujeto respecto al tratamiento que se brindará a sus datos personales, porque estos lo hacen identificable e identifican, por tanto, la información

mínima que se debe conocer: qué, para qué, por qué, la finalidad, cómo dicha información será recopilada, transferida y más, y así poder ejercer sus derechos ARCO. Además, la materialización de que se está brindando de dicha información respecto al tratamiento de los datos, se pudo realizar en formato impreso, en un lugar visible y de acceso fácil para aquellos que se presenten en el establecimiento de manera presencial. Según la DPDP, ello tiene que ver con el hecho de la inmediatez de brindar esta información sobre el tratamiento de datos personales dada la dinámica que se presencia y realiza la administrada. Por ello, se acredita dicho extremo y se estaría ante el tratamiento de datos sensibles como lo indica el art. 2, numeral 5 de la LPDP, concordante con su RLPDP. Así, se brinda una protección mayor a este tipo de datos, puesto que su vulneración es más significativa en los titulares del dato proporcionado, relacionado a su esfera más íntima, siendo un agravante a la infracción que se imputa.

- **3° documento:** a través del informe de fiscalización N.° 183-2018, se encuentra activo y habilitado, recopilando, así, datos personales. Asimismo, se encontraba implementado el formulario denominado “suscríbete a nuestro boletín”; la recopilación que se realizaba era de nombre, correo electrónico, mensaje, celular. Al pie del sitio web se constata que figura un enlace denominado “Contáctanos” que contiene el documento de “política de privacidad”, pero no se cumple con informar sobre el tiempo de conversación de los datos, si la transferencia es nacional o internacional, lo que conlleva cuando el titular proporciona sus datos o cuando está ante la negativa de hacerlo, respecto a la existencia del banco de datos, la identidad de los que son o pueden ser los destinatarios; y si bien la administrada presenta su descargo respecto a la implementación que vienen realizando, no se acredita esta con medio alguno, por lo que la DPDP confirma el extremo.

- **4° documento:** las cámaras de video tenían el fin de brindar seguridad, pero no se informa de ello a los pacientes y/o personal que se encontraba en las instalaciones; además, la administrada brinda su descargo anexando fotografías y afirmando el cumplimiento del art. 18; sin embargo, mediante RD N.º 2533-2018, la DPDP advierte que la administrada, ante la RNPDP, inscribe el banco de datos personales de videovigilancia, con la finalidad de otorgar seguridad y contar con información para investigar situaciones o hechos que incidan en la empresa. Como carácter identificativo se incluye "imagen", sin embargo, este tipo de tratamiento posee ciertas particularidades según la Directiva N.º 01-2020 que desarrolló la ANPD, pero la DPDP considera que, al momento de la fiscalización e inicio del procedimiento, solo se le podía exigir a la administrada la comunicación a los titulares de los datos personales que eran grabados, pero que debían adecuar un cartel informativo con lo indicado por la directiva a *posteriori*. Además, la DPDP brinda un vínculo donde el Gobierno del Perú ha realizado una guía respecto al deber de informar.

2° Hecho infractor: la DPDP indica que la creación de la RNPDP se dispone a través del art. 34 de la LPDP, con ello se posibilita a los ciudadanos realizar consultas o saber el fin, nombre de la identidad y domicilio de los titulares; en la misma línea, realizar dicha inscripción es obligatoria, ya sea que se modifiquen, cancelen o creen los bancos de datos por personas naturales o jurídicas. Así, se le imputa a la administrada el no registrar el banco de datos personales de "proveedores"; y en su descargo presenta la solicitud realizada a través del formulario de inscripción; sin embargo, la DPDP advierte que esto se realiza posterior a la imputación de cargos, acreditándose el incumplimiento por parte de la administrada. Se considera dicha inscripción generada como una atenuante de responsabilidad.

3° Hecho Infractor: la DPDP indica que la administrada tiene el deber de que se comunique, en caso realice flujo transfronterizo a la RNPDP, siendo esto una obligación para

que así la DGPDP tome participación al respecto (art. 26 del RLPDP). Además, el art. 77 del RLPDP señala que "las comunicaciones referidas al flujo transfronterizo de datos personales" son objeto de inscripción; y en el análisis se tiene que la necesidad de informar a la DPDP sobre el flujo transfronterizo recae en realizar una supervisión de las exigencias legales que se deben cumplir. Ahora, en el caso, advierten que la administrada recopila datos en su sitio web y, posteriormente, realiza el flujo transfronterizo de estos, siendo que el servidor físico está en Estados Unidos, pero ello no lo informa, lo cual consta en el informe de fiscalización N.º 183-2018. En su descargo, la administrada manifiesta que realizó la solicitud de inscripción, adjuntando copia de esta; sin embargo, en la RNPDP no advierte comunicación alguna sobre el flujo transfronterizo, por tanto, se acredita lo imputado.

4° Hecho infractor: la DPDP hace una referencia previa al art. 39 del RLPDP, el cual indica el tratamiento que se debe brindar a la información digital, a nivel de seguridad. Asimismo, señala al art. 40 del RLPDP, el cual refiere el ambiente donde se deben dar los procesos de recuperación, conservación y respaldo de los datos personales.

- **1° incumplimiento:** la DPDP examina que en el informe técnico N.º 211-2018 consta que la administrada (Clínica La Luz) incumple con documentar el procedimiento; y si bien en su descargo indica que posteriormente presentaría los documentos idóneos para acreditar el cumplimiento de lo que se le viene imputando, en el informe técnico N.º 167-32019, realizado con posterioridad, se vuelve a indicar dicho incumplimiento, pero recién en el segundo descargo que realiza la administrada se presenta la documentación; sin embargo, mediante informe técnico N.º 213-2020 se señala que, si bien se demuestra la documentación de los procedimientos de gestión de accesos, ello no es así respecto de la gestión de verificación y privilegios, por lo que la DPDP encuentra responsable a la administrada.

- **2° incumplimiento:** el informe técnico N.º 211-2018 señala que la administrada no genera ni mantiene registro de interacción lógica sobre el banco de datos personales que se encuentra en soporte automatizado de pacientes; y la DPDP analiza que, posterior a esto, la administrada presenta su descargo, pero no adjunta medio probatorio alguno, puesto que indica que lo hará después. Mediante informe técnico N.º 167-2019, se ratifica lo señalado por el informe técnico antes aludido. La administrada, recién en su segundo descargo, brinda la documentación, pero mediante informe técnico N.º 213-2020. La DFI señala que igual no se genera este registro de manera adecuada, siendo la administrada responsable.
- **3° incumplimiento:** se indica que la administrada no disponía de un ambiente con las medidas de seguridad idóneas para almacenar, procesar y tramitar información de datos personales; sin embargo, en su descargo adjuntan fotografías que acreditan la existencia de extintores y aire acondicionado, y la DPDP considera dicha acción como una enmienda realizada, la cual se lleva a cabo con posterioridad al PAS, por lo que su responsabilidad sobre lo imputado se ve atenuada (art. 126 del RLPDP).

Décimo Exp. N.º 174-2019-JUS/DGTAIPD-PAS

RD N.º 3039-2021-JUS/DGTAIPD-DPDP (1° instancia)

1° Hecho infractor: la DPDP indica que el art. 18 de la LPDP tiene relación con el requisito de validez que es el consentimiento, sin embargo, sostiene que el titular o responsable del banco de datos tiene el deber de informar al titular de los datos personales el tratamiento que se le brindará a su información, de manera clara, completa y accesible, porque, de lo contrario, se le recortaría su ejercicio sobre otros derechos que le atañen. Cabe resaltar que la DPDP indica que el deber de informar no se vincula con el consentimiento, ya que en la LPDP se encuentran excepciones en las que la obtención de los datos personales no será pasible de un consentimiento previo según el art. 14, por tanto, lo que siempre debe persistir es el deber

de informar respecto al tratamiento que se brinda a los datos personales de un individuo-cliente; de lo contrario, habrá una inobservancia a un tratamiento ilícito.

El análisis de la DPDP sostiene que la administrada señala en su escrito que posee un formulario para recopilar los datos personales, y una vez que el titular lo rellena estos datos son ingresados a su sistema, generando otro documento; sin embargo, la DPDP precisa que el deber de informar se debe realizar en el primer contacto entre administrada y cliente. Además, según escrito presentado por la administrada el 19 de enero de 2021, se tiene que el documento que se genera al ingresar los datos del cliente es accesorio al formulario de recopilación de los datos, por lo que se declara infundado dicho extremo. En el mismo sentido, la DPDP determina que los datos recopilados a través del formulario son vaciados al sistema "Filemarker Pro", resolviendo en el mismo sentido. Sobre la cláusula "declaración de información y consentimiento para el tratamiento de datos personales", la DPDP indica que no logra verificar el deber de informar a los titulares de datos personales las transferencias, tiempo de conservación de los datos personales y la posibilidad de que el cliente ejerza sus derechos ARCO. Además, en lo que respecta a las transferencias, no se indica la razón social, si la transferencia es nacional o internacional, no se indica el país en caso sea internacional, y si no versa transferencia alguna. Sobre la conservación de los datos personales, no se indica el tiempo ni la norma que la regula, puesto que la administrada refiere que su fin es exponer la información a la administración pública. En lo que respecta al ejercicio de los derechos ARCO, se señala que la administrada remite su página web, pero no indica el link del formulario o implementación de este; por todo ello, se desestiman los argumentos que la administrada expresó de la no valoración de sus medios de prueba, constatándose que no se cumple con el deber de informar a los titulares de los datos personales sobre el tratamiento de su información. Otro punto esencial tiene que ver con los verbos rectores o la terminología utilizada sobre el

consentimiento, lo cual, según la DPDP, no es óptimo para el ejercicio de las buenas prácticas de datos personales.

Por otra parte, la DPDP toma como acción de enmienda que la administrada, en su escrito del 19 de enero de 2021, presenta documento para generar como fecha cierta el 18 de enero de 2021, y la RD se inicia el 12 de noviembre de 2021; sin embargo, a pesar de certificarse la copia fiel a la original, la fecha cierta no se certifica; asimismo, el documento que se tiene, denominado "política interna de datos personales", no estaba orientado al deber de informar, sino acreditar el deber de confidencialidad, siendo cosas distintas. Además, da cuenta que antes de la imputación de la RD de inicio, la administrada no contaba con documento que acreditase las condiciones de tratamiento a otorgarse a los datos personales de sus clientes y el formulario no contaba con un *ítem* en relación a ello, acreditándose el no deber de informar. Si bien la administrada presenta un documento donde se implementa un párrafo para cumplir con dicho deber, se advierten falencias; por todo ello, la administrada incurre en el hecho infractor que protege el art. 18 de la LPDP, configurándose una infracción grave (art. 132, numeral 2, literal a del RLPDP).

2° Hecho infractor: la DPDP indica que el principio de seguridad es un principio rector (art. 9 de la LPDP). Asimismo, se establece, según la LPDP, la existencia de la obligación de adoptar medidas de seguridad respecto al tratamiento de los datos personales (art. 16.). Se divide cada incumplimiento normativo:

- **1° medida de seguridad:** la DPDP refiere que el art. 39, numeral 1 del RLPDP desprende la obligación de dictaminar y definir procedimientos documentados en lo que respecta a la gestión de accesos y de privilegios de los usuarios, con el fin de acceder al sistema, que se los pueda identificar y verificar periódicamente los privilegios o modificaciones que se puedan advertir. La DPDP, al brindar su análisis, indica que la administrada el 04 de diciembre de 2020, mediante su escrito, presenta un

documento que fue evaluado por la DFI, por lo que concluye, a través de su informe técnico N.º 422-2020, que la administrada incumple con este artículo. Posteriormente, el 30 de diciembre de 2020, la DFI, a través del informe N.º 160-2020, concluye que dicho documento no reviste de formalidad, al no contar con fecha cierta que acredite el tiempo de implementación de lo requerido; y si bien la administrada indica que la fecha de ejecución data del 20 de agosto de 2019, para lo cual remite un correo, la DPDP concluye que es meramente de coordinación, no acreditándose la fecha cierta de implementación o suscripción. Además, la certificación notarial data del 18 de enero de 2021, un día antes de la presentación del escrito de descargos, por lo cual, si bien la copia certificada notarialmente es fiel a la original, no se cuenta con la fecha cierta, acreditándose que la administrada no contaba con medidas de seguridad al momento de la fiscalización.

- **2° medida de seguridad:** la DPDP indica que el art. 39, numeral 2 del RLPDP señala la obligatoriedad de crear y conservar registros donde haya pruebas de las interacciones que los usuarios tienen con el sistema, como inicio y cierre de sesión. La DFI, mediante su informe técnico N.º 422-2020, ante el descargo de la administrada, indica que se observa que cuenta con un único usuario que accede al sistema donde se realiza el tratamiento de datos personales, por lo que cumple con lo requerido por el artículo; y si bien se encuentra responsabilidad en la administrada respecto a no generar ni mantener registros de interacción lógica del sistema “Filemaker Pro”, se llega a determinar acción de enmienda suficiente a su favor que es posterior al inicio del PAS.
- **3° medida de seguridad:** en el análisis de la DPDP, la DFI responsabiliza a la administrada por no cumplir con la implementación de medidas de seguridad para el manejo de datos personales, ya que no asegura la realización de copias de seguridad de la información almacenada en el sistema "Filemaker Pro". Al respecto, la administrada,

como descargo, indica que las copias se realizan en “Dropbox”, lo cual está bajo responsabilidad de la administradora, y no se presenta el documento por desconocimiento técnico. La DFI, al emitir su informe técnico N.º 422-2020, indica que la administrada realiza copias de respaldo. En el informe N.º 160-2020 del 30 de diciembre de 2020, precisa que cumple con las medidas de seguridad. Así, en su análisis, toman como fecha cierta la presentación del escrito que data del 04 de diciembre, porque una captura de pantalla no cuenta con la formalidad de la fecha cierta, y que la administrada sí pudo presentar su prueba, siendo antes de la RD de inicio por conocer de la infracción, lo cual se acredita con la notificación del informe de fiscalización N.º 181-2019. En consecuencia, se desestima el argumento del desconocimiento.

- **4° medida de seguridad:** la DPDP hace referencia que el art. 42 del RLPDP indica las medidas de seguridad que deben adoptarse cuando se trata del tratamiento de datos personales, y según la imputación realizada por la DFI, la administrada indica que los documentos no automatizados están resguardados en dos anaqueles con cerradura, y la llave la custodia la administradora, siendo la única persona que realiza trabajo presencial. La DFI, a través de informe técnico N.º 422-2020, da la razón a la administrada, señalando que se cumple con el artículo incoado. La DPDP toma como fecha cierta la presentación del medio de prueba que data del 04 de diciembre de 2020, que forma parte de su descargo, y detalla que una captura de pantalla no reviste de formalidad sobre fecha cierta y que se pudo presentar la evidencia con anterioridad a la RD de inicio al estar bien notificado con el informe de fiscalización correspondiente.
- **5° medida de seguridad:** la DPDP refiere que las copias o reproducciones de documentos solo pueden efectuarse bajo la supervisión de personal autorizado y advierte que, en las fiscalizaciones realizadas, que se encuentran en el informe técnico

N.º 145-2018, se acredita que el equipo usado por el jefe de atención al cliente no posee su usuario ni contraseña de acceso, disponiendo de puertos USB activos, acceso a correos personales, acceso a internet sin restricciones, vulnerándose el artículo incoado. Si bien en su descargo presentado a la RD de inicio, que se analizó en el informe técnico N.º 422-2020, concluyen que se habrían implementado las medidas de seguridad, en la etapa de fiscalización no se acredita la obtención real de copias de documentos que contienen información sobre datos personales. El artículo analizado sanciona el que se realice copias o reproducciones de documentos no autorizados, más no los riesgos que se genere de esto, probándose por parte de la DFI el riesgo de que se realicen las copias, no que haya sucedido, declarándose infundado el extremo.

Dicha motivación de cada punto conllevó a que la DPDP afirme que la administrada incurrió en los supuestos infractores del art. 39, numeral 1 y 2, y art. 40 y 42 del RLPDP; y al existir una acción de enmienda, se configura una infracción leve indicada en el art. 132, numeral 1 del mismo cuerpo normativo.

La DPDP también analiza la fecha cierta de los documentos que presenta la administrada y precisa que, si bien existen documentos con fecha posterior y anterior a la imputación de cargo, no cumplen con lo exigido por el art. 245 del Código Procesal Civil, al no acreditarse la fecha cierta; sin embargo, por el principio de veracidad se hace necesario que la información presentada cumpla con lo establecido en el art. 67 de la LPAG de manera conjunta con los principios de buena fe y colaboración procedimental. La DPDP refiere que los documentos presentados por la administrada son auténticos, por lo que los documentos anexados al escrito de la administrada que datan del 11 de agosto de 2021, y los que obran a fs. 228 al 238, al figurar el sello de notario público del 18 de enero de 2021, se toma como acciones de enmienda, al ser posteriores a la notificación de la RD de inicio.

Undécimo Exp. N.º 154-2019-JUS/DGTAIPD-PAS

RD N.º 2077-2020-JUS/DGTAIPD-DPDP (1° instancia)

1° Hecho infractor: la DPDP hace referencia que, en el Título I de la LPDP, se encuentra establecido el principio rector de seguridad para la protección de datos personales, siendo regulado en el art. 9 de la LPDP. Además, añade en su análisis el art. 16 de la LPDP sobre la seguridad que se debe brindar al momento de tratarse los datos personales y el art. 10 del RLPDP que se expresa sobre el principio de seguridad, así como el art. 39 que refiere sobre la seguridad para el tratamiento que se brinda a la información digital. El hecho infractor que se imputa y que comete la administrada es por la razón del incumplimiento de la obligación que está contenida en el art. 39 del RLPDP sobre los sistemas "RIS" y "PACS", los cuales son utilizados para visualizar y programar radiografías, tomografías y diagnósticos que se obtengan por imágenes; estas actividades se sustentan por fiscalización que se realizaron en las instalaciones de la administrada, así como por la evaluación de los documentos que fueron remitidos por esta. Además, la DPDP resalta el informe de fiscalización N.º 163-3019, concluyendo que de los alegatos realizados por la administrada, así como la documentación que obra en el expediente, no permiten mostrar que los sistemas "RIS" y "PACS" cuentan con las medidas de seguridad suficientes ni debidas que permitan su implementación en su funcionamiento. La DPDP señala que la administrada admite esta falta, ya que no cumple con lo indicado en el RLPDP, puesto que no cuenta con mecanismos idóneos para controlar los privilegios y/o accesos, ni genera un registro de interacción lógica que permita identificar quién ingresó, el momento y la acción sobre el manejo de los datos realizados por el sistema.

- **A:** por otra parte, la DPDP se pronuncia sobre el proyecto que presenta la administrada, esto respecto a la documentación de los procedimientos de acceso y gestión de privilegios; sin embargo, este proyecto se encuentra en "elaboración", sin una versión final y una

materialización en su implementación y aplicación efectiva, lo cual no se considera una acción de enmienda.

- **B:** la DPDP señala que la administrada, en sus descargos, indica la existencia de un proyecto de actualización de los sistemas "RIS" y "PACS", donde se considera la interacción lógica, además de solicitarse, a través de un oficio al MINSA, a la Oficina General de Tecnologías de la Información, apoyo para evaluar las especificaciones técnicas sobre estos sistemas. Sin embargo, la DPDP advierte que no se acredita la adecuación de los sistemas, y que solo consta la solicitud que la administrada realizó, no mostrando lo que se puede mantener o generar de los registros de interacción lógica.

Otro punto que toca la DPDP es, a razón del informe técnico N.º 60-2020, a partir del cual la DFI realizó un informe complementario sobre la implementación de medidas de seguridad, en función a los descargos emitidos por el administrado. Así, reafirmó sus conclusiones sobre el incumplimiento del art. 39 del RLPDP por parte de la administrada.

Por todo ello, la DPDP encuentra responsable a la administrada por incumplir con el art. 39 del RLPDP respecto a las medidas de seguridad. En aplicación de un concurso de infracciones, sobre el incumplimiento de los sistemas respecto a las medidas de seguridad, será subsumida la multa a la infracción de mayor gravedad, por incumplir la obligación de confidencialidad del art. 17 de la LPDP.

2° Hecho infractor: la DPDP indica que la LPDP, en su art. 5, establece como principio rector al consentimiento, debiendo ser informado, libre y expreso; además, señala el art. 13, numeral 1 de la LPDP sobre el tratamiento de datos personales y cómo, al realizarlo, se debe guardar un respeto a los derechos fundamentales de los titulares y derechos que la ley confiere. Señala, también, que cuando una entidad realiza un tratamiento para que se ejecute la prestación de los servicios que se ofrece a sus usuarios, para guardar respeto y resguardo a los datos personales, debe cumplir con su obligación de ser confidencial, lo cual está regulado en el art.

17 de la LPDP; no obstante, la DPDP señala el acápite donde se expresa que dicha obligación es relevada cuando hay consentimiento previo del titular de los datos personales, pero brindado de manera expresa, informada, previa e inequívoca. Por otra parte, la DPDP enfatiza que, cuando se tiene un tratamiento sobre datos sensibles, hay una mayor importancia, como es el tema de salud, puesto que debe prevalecer como fin la protección de la esfera íntima que posee el titular. Además, el responsable de realizar el tratamiento debe supervisar e instaurar de manera rigurosa que el personal asignado para brindar sus servicios cumpla con la prohibición de no revelar o facilitar a ajenos el acceso y/o conocimiento de esta información, a excepción de aquellos que tengan autorización debida.

Asimismo, la DPDP precisa que, si bien se imputa a la administrada el incumplimiento del art. 17 de la LPDP, esta configuración de la infracción se da por dos supuestos: primero, existe dentro de la organización una divulgación activa y consciente que trata los datos hacia ajenos no autorizados; segundo, existe una omisión en la seguridad que es significativa para que, dentro de la organización, no se pueda permitir o facilitar datos a terceros ajenos que se suponen deben estar resguardados y bajo reserva del titular de banco de datos. De esta manera, la DPDP refiere que, a su criterio, la administrada incurre en ambas, ya que el personal de la entidad de salud captó fotografías por medio de sus celulares del estado físico del paciente mientras estaba en estado de trauma (*shock*), así como de su tomografía, propiciando que se filtre en diversos medios, por lo que enfatiza que la administrada es responsable de todo perjuicio o daño que se ocasione a sus pacientes o usuarios de sus servicios, por la imprudencia o negligencia de su personal, técnicos y auxiliares. En consecuencia, desestiman el argumento de la administrada que sostiene que las personas que filtraron dicha información no actuaron en su representación ni como sus intermediarios y que han sido sometidas a procedimientos administrativos disciplinarios. Dicho argumento, sostenido por la DPDP, se encuentra recogido en el art. 48 de la Ley General de Salud - Ley N.º 26842. En concordancia, la DPDP señala que

la administrada no cumple con entregar los contratos del personal médico a cargo que atendió al paciente en emergencia o documento alguno que acredite la confidencialidad que debe mantener su personal cuando ejercen sus funciones, no acreditándose que la administrada cuenta con acuerdos de confidencialidad con su personal y/o trabajadores con los que comparte un vínculo, ya sea de forma independiente o por una cláusula de confidencialidad que conste en su trabajo y/o prestación de servicios con respecto a la protección que se debe brindar a los datos personales de sus pacientes.

La DPDP también señala que la administrada no poseía un nivel suficiente y adecuado de protección de los datos personales, al no implementar los sistemas automatizados "PACS y RIS". Además, en el área de servicio ubicado en el quinto piso se consta que había una computadora visible al público, el acceso a esta era por medio de un usuario genérico denominado "quinto piso" y una contraseña única utilizada por residentes de turno y médicos, por lo que el descargo de la administrada fue desestimado porque no propiciaron un entorno confiable y seguro para tratar los datos personales.

En ese sentido, la DPDP indica que el deber de confidencialidad es clave para regir en toda forma respecto al tratamiento de los datos personales que garanticen una adecuada protección de estos y se evite su exposición o tratamiento para fin distinto, sin tener el consentimiento de sus titulares. Este deber se vincula con la implementación de medidas organizativas, técnicas y legales preventivas sobre riesgos que se puedan generar y que son inherentes al utilizarse sistemas automatizados y/o informáticos, y cuando se trata de datos personales. La administrada quiebra el deber de confidencialidad al no contar con una actuación preventiva que no acredita una observancia o adecuación de la normativa sobre datos personales, ni acción de mitigación con la que, a futuro, se repita lo que se le imputa como infracción.

La DPDP precisa que los datos expuestos fueron del tipo sensibles relacionados con la salud, lo cual se relaciona con la esfera íntima de la persona, agravándose la conducta infractora, ya que se atenta contra la dignidad humana consagrada en el art. 1 de la norma madre, esto a razón de que los datos expuestos fueron extremadamente sensibles sobe información conexa a la intervención médica realizada a un paciente en una situación de emergencia, incluyendo imágenes obtenidas en un lugar que no era de acceso público.

Para concluir, la DPDP indica que la administrada infiere que la RD de inicio tuvo una incorrecta motivación, pero no se identifica el extremo específico, por lo que no versa pronunciamiento sobre ello, añadiendo que la administrada cumple con la infracción imputada de incumplimiento al art. 17 de la LPDP sobre confidencialidad.

Duodécimo Exp. N.º 068-2018-JUS/DPDP-PS

RD N.º 515-2019-JUS/DGTAIPD-DPDP (1° instancia)

1° Hecho infractor: la DPDP hace mención al art. 18 de la LPDP, el cual se vendría incumpliendo por parte de la administrada, e indica que, de dicha norma, se tiene que los titulares que otorgan sus datos personales poseen el derecho de ser informados sobre el tratamiento que se le brindará a estos: la finalidad de la recopilación, dónde se almacenará, si existe un banco de datos que conserva dicha información y que especifique si es nacional o internacional, o, en su defecto, si no existiese, qué persona se encargará de la administración y demás aclaraciones pertinentes. En su análisis, la DPDP refiere que, del acta de fiscalización N.º 02-2017 e informe N.º 014-2018, se tiene que la administrada recopilaba información por su página web y agrega que en el expediente se anexó una copia del formulario de la página donde se observa la recopilación de datos personales, como lo son el nombre, celular, apellido, correo. En esa misma línea, se indica que la administrada en su escrito señala que sí informa a los pacientes/usuarios lo que establece el art. 18 de la LPDP a través de su publicación de términos y condiciones, adjuntando una impresión de este artículo; sin embargo, la DPDP

advierte que no se informa quién o quiénes son los destinatarios de los datos, ni respecto al titular del banco de datos personales, así como su domicilio. Por ello, ante el incumplimiento de informar en su totalidad lo que establece el art. en mención, se resuelve iniciar el PAS, y se da inicio a la RD N.º 101-2018. Mediante hoja de trámite, la administrada en su descargo señala que complementó dicha información dando cumplimiento al art. 18 de la LPDP, solicitando la atenuación de la multa.

Al respecto, la DPDP señala, luego de revisar el documento con dicho cambio, que solo existe una transferencia prevista y es distinta de las empresas del Grupo Red Med Cayetano, puesto que no son destinatarias de datos, ya que la administrada solo distribuye información de los productos que la empresa señala. Además, el tratamiento se realiza en sistemas como base de datos que la administrada tiene, sin que necesariamente se refiera a la definición de banco de datos de pacientes con que cuenta la entidad. En este sentido, se emite el informe final de instrucción N.º 089-2018 por el cual la administrada presenta sus descargos y reitera lo que ya había indicado, advirtiéndose una modificación en sus términos y condiciones, considerándose por la DPDP como una acción de enmienda y debiéndose reducir en un 50 % la aplicación del art. 257, numeral 2 literal a) del art. 257 de la LPAG. Además, la detección de la infracción es alta y fácil, y no hubo intencionalidad al cometerla. La DPDP enfatiza que, por el principio de especialidad, se aplican leyes especiales que regulan lo controvertido (LPDP y su RLPDP), y solo en caso de un vació legal se aplicará la LPAG. La DPDP finaliza indicando que la administrada es responsable de lo que se le imputa, precisando que no informaba en su totalidad lo que establece el art. 18 de la LPDP y que sí realizó acciones de enmienda posterior al inicio del procedimiento, debiéndose atenuar la sanción.

2° Hecho infractor: la DPDP inicia mencionando el art 4 de la LPDP, respecto al principio de consentimiento siendo rector en la protección de los datos personales; asimismo, incoa al art. 13 del mismo cuerpo normativa, el cual señala que, al otorgar el consentimiento,

se debe hacer de forma inequívoca, expresa, informada y previa. Se indica, también, el art. 12 del RLPDP, por el cual se especifica cada uno de los componentes descritos en el art. 13 de la LPDP. Por último, sobre este análisis, incluye al art. 14 de la LPDP que indica las limitaciones del consentimiento, en qué casos no se requiere el consentimiento del titular. La DPDP indica que, en caso el tratamiento no se encuentre inmerso en una de estas causales, se debe otorgar la libertad para poder denegar esta información, y el titular puede, voluntariamente, manifestarlo. Asimismo, se debe brindar información sobre el tratamiento de los datos a realizarse, para que no haya duda al momento de otorgarse el consentimiento, acreditándose su validez por reunir todo lo que la ley establece.

Sobre el caso, la DPDP señala que la administrada, mediante su escrito, remite copia de los términos y condiciones de su página web y se aprecia que el tratamiento de datos personales es con fines distintos a la prestación de su servicio o para absolver alguna consulta, además que el formato no posee modo alguno para que se permita al usuario aceptar o denegar el consentimiento para que se de tratamiento para dichas finalidades. Mediante escrito posterior, la administrada indica que tuvo una mejora en dicho formato, agregándose las opciones de “aceptar” o “no aceptar” para que los usuarios puedan decidir si autorizan o no el tratamiento de su información (datos personales), lo cual la LPDP lo verifica en una captura de pantalla adjuntada. De manera posterior, la DPDP advierte que la administrada, en sus descargos, reitera sus alegatos y agrega que no hubo intención de su parte de incurrir en la infracción imputada y que la detección de esta es alta y frágil, lo cual debe considerarse al aplicar la multa. En ese sentido, la DPDP indica que la administrada implementa el mecanismo de obtención del consentimiento y satisface el requisito de validez de ser libre, puesto que los usuarios pueden manifestar su voluntad.

La DPDP también se pronuncia respecto al requisito de informar sobre la identidad de los destinatarios, lo cual no habría cumplido la administrada; sin embargo, en su análisis indica

que la transferencia que se realiza a estos destinatarios, se restringe para fines de atención médica o para consultas sobre sus servicios, lo cual ingresa en el supuesto del numeral 5 del art. 14 de la LPDP, puesto que la obligación de poseer el consentimiento no la exime (administrada) de informar el cumplimiento del art. 18 de la LPDP. Asimismo, la DPDP indica que la mención sobre el grupo "Red Med Cayetano" está dirigida a esclarecer la finalidad del tratamiento de la administrada, es decir, la remisión de información sobre servicios y productos de la propia empresa que integra la red, lo cual no implica una transferencia. Para la DPDP, la administrada tiene responsabilidad por no obtener el consentimiento de manera libre, ya que dicha información requerida no contaba con una previsión de ser transferida ni destinatarios a los que informar. Por todo ello, la DPDP encuentra responsable a la administrada por incumplir con una infracción leve y su accionar de enmienda se toma en cuenta al momento de evaluar su sanción.

3° Hecho infractor: antes de pronunciarse sobre las dos infracciones a los numerales 1 y 2 del art. 39° de la RLPDP, la DPDP incoa el art. 9 de la LPDP que se refiere al principio de seguridad y el art. 16 del mismo cuerpo normativo que establece la obligación que, en este caso, tiene la administrada para adoptar medidas de seguridad para tratar datos personales.

- **A:** la DPDP inicia su análisis señalando el art. 39, numeral 1 del RLPDP e indica que el artículo en mención refiere la obligación de definir los procedimientos de gestión de privilegios y el acceso de los usuarios al sistema. Asimismo, enfatiza en el proceso de verificación que debe realizarse sobre esos privilegios; es decir, establecer los procesos de baja, altas y modificaciones que se puedan dar de los datos, así como de los usuarios o de los privilegios que constan en el sistema. Sobre el caso, la DPDP señala que, de los informes presentados, se acredita que la administrada no implementó las medidas de seguridad para tratar los datos sensibles, esto sobre documentos como la gestión de accesos, privilegios y la revisión periódica, lo cual reviste como infracción. La DPDP

indica que la administrada presentó sus descargos y reconoce que durante la fiscalización no contaba con la documentación correspondiente, pero habría subsanado ello. Así, la DPDP indica que, efectivamente, la administrada, si bien con fecha posterior acredita el cumplimiento del art. 39, numeral 1 de la RLPDP, esto constituye una acción de enmienda.

- **B:** la DPDP inicia su análisis señalando el art. 39, numeral 2 del RLPDP e indica que es obligatorio mantener y generar registros que evidencien las interacciones que se tienen con el sistema, incluyendo información de cuentas de usuarios que tienen acceso, trazabilidad, los horarios de inicio y cierre de sesión, así como toda acción significativa. Así, la DPDP, luego de analizar los informes y el descargo brindado por la administrada, concluye que esta última tiene responsabilidad por la infracción imputada, lo cual admite en un primer momento, puesto que, cuando se realiza la fiscalización, no contaba con documentación idónea requerida, pero posteriormente subsana ello; en consecuencia, dicha acción cuenta como enmienda, operando la atenuación sobre la sanción.

Décimo tercero Exp. N.º 150-2018-JUS/DGTAIPD-PAS

RD N.º 1529-2020-JUS/DGTAIPD-DPDP (1° instancia)

1° Hecho infractor: la DPDP inicia su análisis incoando el art. 5 de la LPDP, respecto al principio de consentimiento, así como el art. 13 del mismo cuerpo normativo, por el cual se expresa que los datos personales serán tratados cuando el consentimiento brindado por el titular haya sido realizado de manera previa, expresa, inequívoca e informada. También se señala que el art. 12 del RLPDP establece los presupuestos para que se otorgue un consentimiento válido; no obstante, también se indican las excepciones en las que no se requiere consentimiento, lo cual se encuentra regulado en el art. 14 de la LPDP. Respecto al hecho imputado, la DPDP señala que, si bien la administrada ha presentado sus descargos, observa que, en su documento

de autorización respecto al uso de imagen, este cumple con ser expreso, inequívoco, previo y libre, pero no informa lo establecido en el art. 12, numeral 4 del RLPDP, por lo que las imágenes recabadas de los médicos que son difundidas en su sitio web no cumplen con todos los criterios establecidos por el art. 12, al no informarse el domicilio del titular del banco de datos personales, la existencia del banco de datos donde se almacenará la información, si existe transferencia internacional o nacional, el tiempo de conservación de la información, sobre los derechos ARCO y todo lo idóneo al respecto.

Por otro lado, respecto a las otras imágenes difundidas, la DPDP indica que la administrada señaló que fueron extraídas de la página "shutterstock", y este sitio admite realizar descargas gratuitas. La DPDP ingresó a dicha página para comprobar ello, verificando que existen estas imágenes y contienen un sello de agua con el nombre del proveedor (shutterstock); sin embargo, las imágenes utilizadas por la administrada no tienen dicho sello de agua, y no han proporcionado el link desde el cual se realizó la descarga de imagen; por ello, la DPDP culmina señalando que, para el tratamiento de imágenes, se ha necesitado el consentimiento de sus titulares; no obstante, sobre los contratos donde se adjuntó el consentimiento para el uso de imagen, la DPDP pudo advertir el tratamiento que se realizó, referente a la publicidad, lo cual se establece como una finalidad de la celebración del contrato que está dentro de los presupuestos de las excepciones al consentimiento.

En esa misma línea, la DPDP indica que la administrada presentó sus descargos, siendo un total de seis; a ello, señala que los adjuntados en el número dos cumplen con informar lo que el art. 12, numeral 4 del RLPDP establece. Además, sobre el uso de las imágenes de artistas, la DPDP comparte el criterio ya brindado de la DFI, puesto que el tema del tratamiento realizado por la administrada está contemplado como una finalidad que el contrato celebrado poseía, encontrándose dentro de las limitaciones para solicitar el consentimiento; en consecuencia, la DPDP señala que debe evaluar la fecha que se debe considerar para subsanar

el incumplimiento. Así, la DPDP incoa el art. 245 del Código Procesal Civil sobre fecha cierta e indica que lo presentado por la administrada respecto a las imágenes de artistas, no posee certificación de fecha cierta, legalización de firmas o una difusión en una fecha que se pueda determinar, por lo que se considera como cierta la fecha que consta al adjuntarse su escrito. En ese sentido, la DPDP añade que, a razón del principio de presunción de veracidad, es indispensable que la información brindada por la administrada cuente con lo establecido por el art. 67 de la LPAG. Luego de una revisión, finaliza señalando que la declaración de la administrada no tiene sustento en documento de fecha cierta sobre la obtención del consentimiento y que lo considerará como acciones de enmienda para atenuar la responsabilidad de la administrada al ser presentada con posterioridad al inicio del PAS.

Asimismo, la DPDP se pronuncia sobre los demás documentos obrantes en el expediente, indicando que la DFI imputa que la administrada recopilaba datos en soportes no automatizados de sus pacientes mediante diversos formatos, sin contar con el consentimiento válido, y que, en concreto, se refiere a dos documentos específicos denominados A y B. Respecto al documento A, se recaba el consentimiento para fines adicionales que no se vinculan a su prestación de servicios, respecto al servicio de salud y hospitalario. En ese sentido, se tiene que el consentimiento requerido no es libre, al inducir al error al solicitar en bloque, respecto a la ejecución de la relación contractual como aquella que no es, no brindando la opción al paciente/usuario de aceptar o no que se traten sus datos personales para fines que no correspondan a la relación contractual, y que tampoco es expreso ni inequívoco porque en su sitio web no brinda el mecanismo a su usuario de que otorgue su consentimiento de manera afirmativa para tratar sus datos, máxime que tampoco se obtiene un consentimiento informado de parte de la administrada porque no comunica quién o quiénes serán destinatarios de los datos personales, ni respecto a la transferencia nacional o internacional, ni el tiempo de conservación de la información. Por ello, la DPDP indica que la administrada trata los datos personales sin

tener consentimiento libre, informado y expreso. Sobre el documento denominado B, la DPDP señala los argumentos indicados para el documento A; no obstante, añade que la administrada, antes del inicio del PAS, modifica los documentos para obtener el consentimiento y la DPDP, al verificarla, señala que la nueva fórmula cumple con todo lo indicado por el art. 12 del RLPDP. Sobre la fecha cierta, la considera siguiendo el razonamiento expresado previamente e indica que, al no contar con esta ni con documentación pertinente, entonces es una acción de enmienda al ser presentada con fecha posterior al inicio del PAS.

Para finalizar con el hecho infractor primigenio, la DPDP, sobre los descargos presentados por la administrada, respecto a aceptar su responsabilidad e indicar que ha realizado acciones de subsanación, refiere que no acredita haber realizado las acciones de enmienda antes de la notificación de la resolución que da inicio al procedimiento, pero su accionar se tomará en cuenta. Concluye indicando que la administrada realiza el tratamiento de datos personales sin obtener un consentimiento válido.

2° Hecho infractor: La DPDP incoa el art. 18 de la LPDP señalando que para tratar los datos personales se debe informar al titular previamente, enfatizando que el artículo en mención presenta una obligación que el titular o responsable del banco de datos personales debe realizar en los casos que el consentimiento sea necesario de requerir, lo cual se relaciona con el art. 5 del mismo cuerpo normativo, así como considerar las excepciones al consentimiento, como lo expresa el art. 14. Respecto a la infracción, la DPDP señala que, si bien se imputa que la administrada recaba información (datos personales) a través de soporte automatizado y por formularios físicos sin informar lo que indica el art. 18 de la LPDP, la DPDP señala que no hay certeza de una revisión de autos, cómo es la forma en que se da la recopilación, cómo se ingresan, no pudiéndose imputar una falta de información. Sobre los formularios que son soportes no automatizados, como lo refiere la DPDP, se señala por el despacho a cargo que, en un inicio (primera vez), se debe informar al paciente sobre la

recopilación que se hace de sus datos personales, no así en cada formato que vaya a rellenar, esto en relación a su historia clínica. Además, la administrada, en su descargo, incorpora para ambos sistemas el consentimiento informado y las políticas de privacidad, indicando que realizó acciones correctivas, las cuales se ejecutaron antes del inicio del PAS. Al respecto, la DPDP, luego de revisado el documento, verifica que la administrada no cumple con informar la finalidad de uso de los datos personales, no trasladando la información completa que regula el art. 18 de la LPDP; sin embargo, presenta descargos. Así, el despacho, revisados los documentos de políticas de privacidad, verifica que la nueva fórmula cumple con todo lo establecido en el art. 18 de la LPDP y entiende que su accionar se debe considerar porque modifica sus procedimientos, considerándolo responsable por lo que se le imputa: realizar el tratamiento de datos personales sin cumplir con su deber de informar.

3° Hecho infractor: la DPDP incoa el art. 2 de la LPDP respecto a la definición de qué es flujo transfronterizo y respecto a la obligación que la administrada tiene de comunicar sobre este, el cual regula el art. 26 del RLPDP, sosteniendo que el flujo transfronterizo de datos personales se debe comunicar a la DGTAIPD para que esta supervise que cumple con las exigencias legales. De lo imputado, la DPDP señala que la administrada recopila datos personales por su página y que su servidor físico, donde se aloja esta información, se encuentra en Estados Unidos. Al respecto, se señala que la administrada dio sus descargos indicando que presentaron su solicitud ante la RNPDP antes de que se inicie el PAS, pero les realizaron observaciones que no fueron resueltas porque la empresa proveedora demoró en entregar la información, siendo una inobservancia de fuerza mayor, debiéndose aplicar la eximente contemplada en el art. 257, numeral 1, literal a) del TUO de la LPAG; sin embargo, el despacho indica que no es un caso de fuerza mayor, pues es un caso que obedece a la gestión de la administrada, y no adjunta medio probatorio que ratifique su dicho; también, la DPDP señala que la administrada en otro descargo acepta su responsabilidad por escrito y de manera expresa,

alegando subsanar voluntariamente la infracción antes de que se emita resolución final, y reitera la inscripción del flujo transfronterizo e indica que borró los datos personales que se hubiesen recibido antes de resolverse el tema de la inscripción del flujo transfronterizo. La DPDP, conforme la RNPDP, señala que se modifica el código de la inscripción del banco de datos personales y se comunica la realización de flujo transfronterizo, además de la solicitud de modificación del banco de datos personales; sin embargo, no se acredita que la administrada haya cumplido con comunicar a la RNPDP que realizó flujo transfronterizo, pero sí lo subsanó con posterioridad al inicio del PAS, siendo una atenuante a considerarse. Asimismo, la DPDP finaliza indicando que tomará en consideración las acciones de enmienda que haya realizado la administrada.

4° Hecho infractor: la DPDP señala el art. 39 de la LPDP respecto a la seguridad para el tratamiento de la información digital, tal como lo indica su título, y añade que uno de los bancos de datos que no posee condiciones de seguridad es aquel que recopilaba datos personales, incluyéndose datos sensibles, siendo que no generaba ni mantenía registros de interacciones lógicas adecuadas al banco de datos personales que estaban en soportes automatizados, lo cual establece el numeral 2 del artículo ya indicado. Además, el despacho precisa que uno de esos bancos de datos almacenaba información de salud, religión e idónea que es considerada como información (datos) sensible, según la definición que brinda el art. 2, numeral 5 de la LPDP; y si bien mediante informe técnico N.º 215-2018 se ha indicado dicho incumplimiento por parte de la administrada al art. 39, numeral 2 del RLPDP, la administrada ha indicado que ha implementado las medidas de seguridad para el tratamiento de datos personales, incluyéndose los datos sensibles, al mantener y generar un registro de interacción lógica adecuada respecto al soporte automatizado, adjuntando documentos idóneos. Ante ello, mediane informe técnico N.º 0177-2019, se señala que sí cumple con lo indicado, por lo cual

la DFI recomienda archivar dicho extremo, encontrándose el despacho de acuerdo con esta decisión.

Décimo cuarto Exp. N.º 143-2019-JUS/DGTAIPD-PAS

RD N.º 1944-2021-JUS/DGTAIPD-DPDP

1° Hecho infractor: el despacho resolutor inicia precisando lo establecido por la norma madre en su art. 2, numeral 6, lo cual se relaciona con la autodeterminación informativa. Así, para dar un concepto sobre ello, incoan lo que el TC indica en su STC N.º 04739-2007, y siguiendo dicho razonamiento, especifica que no se puede tener un control idóneo respecto a la información personal sin que se conozca cómo se van a utilizar los datos que se recopilen, el tratamiento a brindarles y con quién o quiénes se comparte. Al respecto, señalan que la LPDP, en su art. 1a, reconoce la protección de los datos personales y se relaciona con el artículo indicado de la norma madre en un inicio. Además, en el Título III se señalan los derechos que ostenta el titular de la información (datos personales), regulado del art. 18 al art. 22 de la LPDP. Al respecto, la DPDP se enfoca en indicar que el art. 18 de la LPDP regular el deber-derecho que la administrada tiene de informar al titular de los datos personales sobre el uso de este, y que se debe realizar una especificación de cómo, quiénes, el domicilio del titular, la finalidad e información pertinentes que lleve a cabo lo establecido por el art. 18 de la LPDP. El despacho agrega que, si bien este artículo se une al art. 5 de la LPDP, sobre el consentimiento, también es de considerarse los supuestos en los cuales no es necesario su requerimiento, tal cual lo regula el art. 14 de la LPDP, agregando que este artículo solo exonera al titular del bando de datos de solicitar el consentimiento, debiéndose cumplir los demás aspectos regulados en otros artículos de la LPDP y RLPDP. Asimismo, añade que, para el cumplimiento del art. 18 de la LPDP, si bien se conecta con casos en los cuales se requiere el consentimiento del titular, como el art. 5 de la LPDP refiere, también habrá excepciones en las cuales no se requiere, como el art. 14 del mismo cuerpo normativo indica; sin embargo, eso no significa que no se deba

cumplir con los demás requisitos. Asimismo, para el cumplimiento del art. 18 de la LPDP, se debe informar de manera previa el tratamiento a darse a la información, siendo que el cumplimiento de dicho artículo es una infracción grave, como lo indica el art. 132, numeral 2, literal a), a razón de que se vulnera un bien jurídico protegido al impedir al titular de conocer cómo se usará su información, impidiendo que tenga control al respecto. Se enfatiza que el hecho de no informar de manera previa lo requerido por el art. 18 de la LPDP ya impide u obstaculiza el ejercicio del derecho de información del titular de la información.

Respecto a lo imputado, el despacho indica que la administrada realizaba el tratamiento de los datos personales en sistemas no automatizados, pero no informaba a los titulares de los datos personales, lo indicado en el art. 18 de la LPDP, lo cual realizaba a través de sus formularios. Así, mediante acta e informe de fiscalización, se indica el hecho infractor, a lo que la administrada señala que sí informa a los titulares de lo requerido por el artículo en mención, esto a través de su cláusula de política de información y consentimiento, de manera expresa e inequívoca. Luego de analizar ello, la DFI, en el PAS, resalta que, en el documento incoado, no se informa de la existencia del banco de datos personales ni del plazo de conservación, a lo que la administrada responde señalando que realizó modificaciones e incorporó la existencia del banco de datos, su tiempo de conservación, y que ello se acoge al art. 126, respecto a acciones de enmienda, lo cual evaluó la DFI mediante su informe, pero indica que la administrada no acredita que se haya implementado de manera adecuada las enmiendas. Sobre ello, la DPDP señala que no hay más descargos presentados por la administrada y que, efectivamente, esta trata los datos personales en soporte no automatizado mediante diversos formularios físicos, pero que sí ha realizado acciones de enmienda para el cumplimiento del art. 18 de la LPDP. Al respecto, denota que, respecto a los formularios, no se cumple con informar las condiciones del artículo que se viene infringiendo ni con el plazo de conservación de los datos; por otra parte, sí cumplen con indicar qué datos se almacenarán y en donde,

considerando el despacho que, sobre dicho extremo, debe declararlo infundado, pero se indica que hay una finalidad sobre publicidad, debiéndose suprimir porque esta requiere el consentimiento del titular según lo dispone la LPDP y el RLPDP. Por ello, se encuentra responsabilidad en la administrada.

2° Hecho infractor: al respecto, el despacho resolutor inicia indicando lo que el art. 34 de la LPDP refiere sobre las finalidades de inscripción de los bancos de datos personales, ya sea de administración pública o privada. Además, permite que los ciudadanos puedan solicitar información sobre la finalidad y existencia de los bancos de datos personales inscritos, y acerca de la identidad y domicilio de los titulares. Añaden que el art. 78 del RLPDP señala la obligatoriedad de inscribir el banco de datos. Sobre ello, si bien en la fiscalización la DFI imputa a la administrada no haber inscrito en el RNPDP el banco de datos personales, la administrada indica que no era necesaria dicha acción porque no cuenta con proveedores directos. En respuesta, la DFI señala que, al recopilarse datos de personas jurídicas, la inscripción no corresponde; por tanto, la DPDP declara infundado dicho extremo infractor.

Décimo quinto Exp. N.º 134-2018-JUS/DGTAIPD-PAS

RD N.º 418-2021-JUS/DGTAIPD-DPDP

Hecho infractor: primero, la DPDP incoa el ar. 18 de la LPDP e indica que los titulares de los datos personales tienen el derecho que se les informe sobre el tratamiento de su información, por qué se recopila y dónde se almacenará en caso de existir un banco de datos, si este es nacional o internacional, el tiempo de conservación, quién se encargará de administrar la información y los terceros destinatarios en caso hubiere. Así, mediante dos actas de fiscalización e informe correspondiente, la administrada estaría tratando datos personales sin informar a sus titulares del artículo indicado, lo cual es una infracción grave estipulada en el art. 132, numeral 2 del RLPDP; por ello, el despacho indica que, al momento de las fiscalizaciones, la administrada no realizaba lo indicado por el art. 18 de la LPDP.

Al respecto, la DFI solicitó a la administrada indicar cómo recopilaba los datos personales de los pacientes en su sistema denominado SIGASA. La administrada señaló que proporcionaba a los pacientes un formulario virtual, por ello la DFI, mediante su informe, señala que la administrada recopilaba esta información de sus titulares de manera directa, sin poner a disposición de ellos la información señala en el art. 18 de la LPDP. Mediante otro descargo, la administrada señala que su sistema cuenta con política de privacidad. En ese sentido, la DPDP señala que el formulario es físico y los pacientes lo rellenan, y la información es ingresada al sistema (Sigasa) por el personal de la entidad; es decir, los datos ingresados no se proporcionan de manera directa por el titular de la información. Así, el despacho declara infundado este extremo. Sobre el tratamiento a datos personales por medio de formularios físicos sin cumplir con el art. 18 de la LPDP, la DPDP indica que, si bien no es una obligación de la administrada el solicitar el consentimiento, sí debe cumplir con informar a los titulares de los datos personales respecto a las condiciones del tratamiento; y en la misma línea, la administrada presenta sus descargos e indica que sí informa a los titulares respecto a lo que establece el art. 18 de la LPDP, y lo realiza antes que sus clientes o usuarios contraten el servicio. Asimismo, indica que posee un formato de consentimiento que se exhibe en sus paneles informativos, entregándose el documento en recepción y caja antes de la cancelación del costo del servicio; adjunta, además, medios de prueba que son fotografías sobre lo que aduce. En este sentido, la DPDP indica que el derecho de información es un derecho que toda persona natural tiene, puesto que se realiza el tratamiento sobre datos que la identifican o permiten hacerlo/a identificable. Ello le permite conocer el fin para el cual se recopilan sus datos, así como a quién le serán transferidos, la forma y modo, y frente a quién pueden ejercer sus derechos ARCO.

Toda esta información sobre las condiciones del tratamiento de datos personales debe ser accesible e identificable de manera priva a su recopilación. Luego de una revisión a las

fotografías, la DPDP constata que, por la distancia de la toma, no se puede dar una lectura del contenido, y por ello se solicita a la administrada, en un plazo de cinco días, presentar el documento incoado; y a dicha respuesta, la administrada presentó su formato de privacidad y consentimiento; sin embargo, la DPDP señala que el objetivo del documento es informar sobre el tratamiento de sus datos personales a los titulares, por lo que los verbos rectores deben ser "informar" y no "consentimiento". Además, en el mismo documento se observan diversas finalidades indicadas, y una de ellas no se vincula con la prestación de servicios que realiza; aun así, la administrada debe cumplir con indicar los requisitos y características que señala la LPDP y el RLPDP sobre el consentimiento, en caso contrario, debe suprimir dicha finalidad porque la administrada debe indicar aquellas a fines a su prestación de servicio o, como indica la DPDP, solicitar el consentimiento.

La DPDP señala que, respecto a las transferencias y destinatarios, la administrada tiene que indicar a qué empresa se envía la información, su denominación, los encargados, la finalidad, si es empresa nacional o internacional, país destinatario, cuál es el medio de almacenamiento, ubicación geográfica, tiempo de conservación y demás datos pertinentes, ya que la administrada indica que los datos personales se enviarán a terceros nacionales, pudiendo ser empresas que son parte de esta. La DPDP enfatiza que, respecto al cumplimiento del art. 18 de la LPDP, se publicó una guía para que pueda cumplir con todos los requisitos necesarios expresados en este artículo.

En concordancia con lo indicado, la DPDP señala que la administrada genera riesgo en los titulares de la información (datos personales), puesto que no cumple con informar ni dispone a los titulares con información completa respecto al tratamiento que brinda a sus datos personales. Además, sobre la exhibición que la administrada alega realizar sobre su formato de privacidad y consentimiento en todos sus pisos e instalaciones, la DPDP indica que no

cuestiona la forma, siempre que haya una accesibilidad de forma previa a la recopilación de información (datos personales).

Respecto a otro punto a tomar en cuenta, la administrada en su descargo indicó que realizó mejoras sugeridas; sin embargo, la DPDP indica que la DFI precisó que no se cumplió con informar la finalidad del tratamiento de los datos ni el tiempo de conservación, no cumpliendo con subsanar de manera completa lo requerido.

Respecto al sitio web de la administrada, la DPDP señala que, a través de su formulario "contacto", no se observa que informe lo que indica el art. 18 de la LPDP, y si bien la DFI mediante la RD N.º 025-2020 señala que el sitio web cuenta con un aviso, no informa el fin del tratamiento ni el tiempo de conservación de los datos personales, ni tiene un título, por lo que se inicia el PAS. Posterior a ello, la DFI emite su informe e indica que la administrada no realiza enmienda alguna, y sigue sin informar a los titulares de los datos personales el fin y tiempo de conservación de sus datos. Así, la administrada en su escrito reconoce que dicha omisión se dio de manera involuntaria, pero rectifica en el reinicio de sus actividades, además de haber colaborado con el procedimiento de fiscalización y realizar acciones de enmienda.

La DPDP también se pronuncia sobre lo imputado y las investigaciones que realizó la DFI. De esta manera, el despacho resolutor ingresó a la página web de la administrada para evaluar la finalidad que expresa su política de privacidad respecto al formulario "contacto". El despacho expresó que, en el documento, se indican las finalidades adicionales a su prestación de servicio, las cuales requieren del consentimiento del titular de la información (datos personales), debiendo suprimirse o, en todo caso, solicitar el consentimiento para estas. Asimismo, si bien emite pronunciamiento, la DPDP señala que no fue imputada, por tanto, no puede ser materia de sanción.

Respecto a las transferencias y destinatarios, el despacho señala que la administrada, dentro de sus políticas de privacidad, indica que los datos personales serán enviados a empresas

que son afiliadas, socios y terceros; el listado se encuentra en su sitio web, pero la DPDP señala que la administrada ha debido señalar detalladamente cada uno de esos puntos, y que, al ingresar al link, este remite a la web donde se detallan los servicios médicos que brinda y no al listado incoado. En esta misma línea, el despacho indica que, de ubicarse los datos personales en la nube, se debe indicar la empresa, ubicación geográfica del servidor, sí la transferencia es nacional o internacional, la denominación de existir un bando de datos y demás información idónea.

Sobre el tiempo de conservación, la DPDP indica que la administrada refirió que los datos serán conservados por el tiempo necesario para que se cumpla con las finalidades que la norma indica; así, el despacho señala que se debe precisar qué norma regula ello y señalarse, como recomendación, el lapso de tiempo de conservación.

Por todo ello, la DPDP concluye que la administrada no cumple con el art. 18 de la LPDP, según lo que dispone, debiendo modificar las políticas de privacidad, ya que la administrada reviste de responsabilidad al tratar los datos personales a través de su sitio web por diversos formularios.

Décimo sexto Exp. N.º 139-2019-JUS/DGTAIPD-PAS

RD N.º 1981-2020-JUS/DGTAIPD-DPDP

1° Hecho infractor: el despacho comienza indicando lo establecido por el art. 18 de la LPDP, el cual tiene por expresado que los titulares de los datos personales deben ser informados respecto al tratamiento que se le brindará a estos; es decir, deben saber sobre qué tratamiento se dará, el fin de la recopilación, el almacenamiento, si existe un banco de datos, si está en el país o fuera de este, el tiempo de su conservación, las personas encargadas, así como los terceros destinatarios que podrán estar dentro o fuera del país. Así, mediante tres actas de fiscalización, la DFI dejó constancia que la administrada, en su banco de datos personales de sus pacientes, realizaba tratamiento a la información en soporte, tanto automatizados como no

automatizados. Asimismo, contaban con un ambiente de videovigilancia a cargo de la jefa de mantenimiento; por último, se verificó que tenían ordenadas de forma ascendente las historias clínicas por sus números, por lo que, a través del informe de fiscalización, se concluye que la administrada realizaba tratamiento de datos personales sin informar a sus titulares lo que señala el art. 18 de la LPDP, vulnerando el derecho de información y siendo una infracción grave. Son tres los medios a partir de los cuales se realiza el hecho infractor, y se exponen en el siguiente análisis:

- Sobre el sistema cliente/servidor, la administrada no presentó en sus descargos evidencia con argumentos específicos sobre el tratamiento que brinda a los datos personales que se almacenan en dicho medio, y la DFI se pronunció indicando que no figuran medios probatorios por los cuales se informe a los titulares lo que dispone el artículo que se postula infringido. Luego, la administrada vuelve a presentar descargos, pero no son específicos los argumentos sobre el tratamiento realizado en este servidor. De consignada el acta de fiscalización emitida por la DFI, así como capturas de pantalla y documentación pertinente obrante en el expediente, la DPDP afirma que, si bien la administrada realiza tratamiento de datos por medio de dicho sistema, no se acredita que la información se seleccione de los formularios para ser ingresada ni cómo se da la recopilación de manera directa del paciente; al no tener certeza de esto, no se puede afirmar el incumplimiento del artículo incoado, declarándose infundado este extremo.
- Se imputa que la administrada trata información mediante formularios físicos. De los descargos presentados, la DPDP indica que el derecho de información es importante porque toda persona natural lo posee cuando se trata de sus datos personales, puesto que así se conoce la finalidad de la recopilación, a quién o a quiénes se transfiere esta, la forma y modo, y ante quién ejercerá sus derechos ARCO; por lo que dicha información expresada debe ser accesible e identificable de manera previa a su

recopilación. Por lo tanto, y en conexión con el art. 18 de la LPDP, todo titular o responsable del banco de datos debe poner a disposición de los titulares de los datos la información idónea que se vincula al tratamiento que darán.

La DPDP analizó la política de privacidad que maneja la administrada, y da cuenta que esta no cumple con indicar la transferencia de los datos personales, el nivel, si son internacionales o nacionales las empresas destinatarias, el fin de estas, la denominación de la entidad, y en caso fuese internacional, el país y la finalidad; así, añade que se debe precisar el tiempo de conservación. Asimismo, si bien indican de manera genérica que la conservación se da con base en la normativa vigente y dentro de lo establecido en la Ley N.º 26842, la DPDP señala que se debe indicar la norma técnica que la dispone; posteriormente, la administrada presenta sus descargos.

Al respecto, el despacho ha indicado que sobre la materialización para cumplir con el deber que le atañe a la administrada de informar, esta cuenta con un documento de política de privacidad, que se ubica en lugares diversos, siendo visibles y de fácil acceso para el público que se apersona a la entidad, quedando sus argumentos estimados. Además, para que se cumpla con lo dispuesto por el art. 18 de la LPDP, en tanto se perfeccione de manera correcta el deber de informar, implementar sus carteles es idóneo porque la naturaleza dinámica que tienen los servicios que prestan las entidades lo amerita. La DPDP finaliza indicando a la administrada que incluya las transferencias nacionales e internacionales en su documento de privacidad.

- Sobre las cámaras de vigilancia, se tiene que la administrada cuenta con estas de manera interna y externa, debiéndose implementar un canal donde el titular de los datos tenga conocimiento de estas zonas; al respecto, la administrada presenta fotos de la ubicación de los letreros que informan ello, y alega la implementación de la política de privacidad y adjunta fotografías; sin embargo, la DFI señala en su informe que la administrada no cumple con informar de manera total lo dispuesto por el art. 18 de la LPDP al no referir

el tiempo de conservación. La administrada ha precisado que los fiscalizadores no han considerado dichos carteles distribuidos en diversas áreas de sus instalaciones, para lo cual adjunta evidencia. El despacho señala que el tratamiento de datos que se dan por medio de cámaras de vigilancia reviste de particularidades en su cumplimiento, y consideran que recién la ANPD, a través de su directiva, ha desarrollado disposiciones para la obligación que recae en la administrada. No se le puede exigir el cumplimiento al momento de fiscalizarla, solo es necesario que la administrada comunique a los titulares de los datos que estaban siendo grabados, lo cual se debió exigir. De verificado los medios probatorios, la DPDP indica que la administrada cumple con informar a los titulares de la información respecto a qué zonas contaban con cámaras de vigilancia, y que dichas fotografías presentadas por la administrada se realizaron con anterioridad a la imputación de cargos, siendo una eximente de responsabilidad.

Para concluir, el despacho indica que la administrada debe implementar el cartel informativo, como lo ha señalado la directiva, modificando así el documento de política de privacidad, como lo ha indicado la DPDP. Asimismo, la administrada debe considerar lo dispuesto por la DGTAIPD en su directiva implementada para que informen sobre el tratamiento de los datos personales, tal cual indica el art. 18 de la LPDP. Sobre la política de privacidad de los documentos físicos, la DPDP señala que los pacientes completan estos documentos cuando ya han visto las políticas de privacidad, siendo una buena práctica, no asumiéndose que no están informados. Sin embargo, el defecto radica en que no informan sobre las transferencias; por lo tanto, la administrada es responsable de cometer esta infracción grave.

2° Hecho infractor: se imputa a la administrada haber infringido el numeral 1 y 2 del art. 39 de la RLPDP; así, la DPDP incoa al art 9 del mismo cuerpo normativo como uno de los principios rectores sobre la protección de datos, y señala al art. 16 de la misma ley que indica la obligación de que se adopten medidas de seguridad para tratar los datos personales; por tanto,

el despacho desarrolla su análisis respecto a ambos numerales de manera separada, sugiriendo lo siguiente:

- Respecto al numeral 1 del art. 39 de la RLPDP, el despacho inicia refiriendo lo que este artículo señala, indicando la obligatoriedad que se debe realizar sobre procedimientos y documentos de gestión de privilegios y acceso de los usuarios al sistema, la identificación de estos, el proceso de verificación periódica de esos privilegios, establecerse el proceso para la baja, alta y/o modificación que pueda darse, modificar usuarios, así como los privilegios en el sistema. De esta manera, la DFI, a través de su acta de fiscalización, deja constancia que se verifica que la administrada no cuenta con procedimientos documentados de la gestión de privilegios, accesos y la verificación periódica; y después se emite el informe de fiscalización; por ello, el despacho señala que la administrada no habría cumplido con implementar las medidas de seguridad, incluyéndose como supuesto infractor imputado lo dictaminado en la RD N.º 149-2019. Posterior a ello, la administrada presenta diversos descargos a los cuales la DFI emite sus informes técnicos como respuesta, señalando que no cumple con el artículo que se le imputa; sin embargo, en el último descargo realizado, donde incluye medios probatorios que obran en autos, la DPDP constata que la administrada cumple con implementar el numeral 1 del art. 39 de la RLPDP y lo hace con anterioridad al inicio del PAS, siendo causal de eximente y estimando los argumentos que la administrada presentó respecto a la implementación sobre la gestión de accesos.

Por otra parte, la DPDP sí indica que, respecto a la gestión de privilegios, sí se cumple con lo dispuesto por el artículo que se le imputa; y de revisado los medios probatorios, siguiendo la misma idea, cumplen con enmendar lo que se les requirió con anterioridad a la imputación de cargos, eximiéndose de responsabilidad a la administrada. Ahora, lo que no se acredita es que la administrada no documenta su procedimiento de verificación periódica de

privilegios asignados ni indica la frecuencia de la periodicidad; por tanto, es responsable de incumplir con el art. 39, numeral 1 de la RLPDPD.

- Sobre el incumplimiento al numeral 2 del art. 39 de la RLPDP, se tiene que dicho artículo desprende que es obligatorio que se cuente con un control de acceso desde el registro del usuario, la gestión de la identificación y privilegios del usuario con el sistema. Además, se deben generar y mantener registros que provean evidencia respecto a las interacciones que se hagan con el sistema. La DFI, así como la administrada, ha presentado sus reportes; de todo ello, el despacho concluye que la administrada no implementa las medidas de seguridad que se le requiere, puesto que no genera ni mantiene registros de interacción lógica con su banco de datos de pacientes; y si bien la administrada brinda su descargo, al final la DPDP señala que no cumple con presentar medios de prueba que demuestren dicha implementación, siendo responsable de la imputación que se le realiza.

Décimo séptimo Exp. N.º 111-2019-JUS/DGTAIPD-PAS

RD N.º 313-2021-JUS/DGTAIPD-DPDP

1° Hecho infractor: la DPDP inicia señalando lo regulado por el art. 18 de la LPDP y señala que es necesario brindar la información respecto al tratamiento de datos personales al titular de la información y deber ser de manera previa; es decir, los titulares tienen el derecho de estar debidamente informados sobre qué tratamiento se le dará a su información, la identidad y domicilio del banco de datos, el fin de recopilación de sus datos, las consecuencias de brindar sus datos, cómo pueden ejercer sus derechos ARCO, el tiempo de conservación de los datos y todo lo demás pertinente. Asimismo, enfatiza que dicho artículo presenta una obligación que el titular o responsable del banco de datos debe cumplir, ya sea si es necesario tener el consentimiento del titular o si no se requiere.

Respecto al hecho imputado, se tiene que la administrada no informaba a los titulares de la información lo requerido por el artículo ya indicado, pero daba tratamiento a datos personales a través de su formulario en su página web, resaltándose que no contaba con políticas de privacidad, pero en la parte baja había una página semejante que no cumplía con lo requerido. La administrada presentó sus escritos, brindando sus descargos y consideraciones, a lo cual el despacho brindó el siguiente análisis: la administrada postula una afectación al principio de licitud y otros; al respecto, la DPDP señala que, desde que se dio inicio a las actuaciones previas, así como durante el desarrollo del procedimiento sancionador, la DFI no admitió ningún hecho como si se hubiese probado. Asimismo, arriba a sus conclusiones luego de evaluar y recabar sus pruebas de oficio, así como documentales ofrecidos por los administrados, no presumiendo un actuar ilícito por parte de la administrada, debiéndose entender que la DFI realiza acciones indagatorias previas a la emisión de algún juicio de valor.

Así, al fiscalizar se ha determinado que, mediante su sitio web, no se informaba de manera completa lo indicado por el art. 18 de la LPDP, lo cual se notificó a la administrada para que pueda defenderse. En ese sentido, se expresa lo regulado por el art. 248, inciso 10 del TUO de la LPAG, por el cual se tiene que la responsabilidad administrativa es subjetiva, caso contrario señalado por ley o decreto legislativo que la disponga de manera objetiva, por lo que el art. 328 de la LPDP establece que los administrados tienen responsabilidad objetiva cuando incumplen con las normas sobre protección de datos personales; por ello, existe una norma que impide la aplicación de exigirse que se acredite que el sujeto infractor actúa de manera negligente o dolosa, y el análisis se restringe a configurarse la conducta típica; es decir, para poder demostrarse la responsabilidad de la administrada basta con que se acredite que comete la conducta típica sin necesidad de demostrarse el dolo o la culpa.

Así, la DPDP señala que, luego de revisado el sitio web de la administrada, se constata que en la parte inferior de la venta se tiene un enlace que lleva a la política de privacidad y al

ingresar remite a un documento. El despacho indica que procederá a analizar, respecto al tiempo de conservación de datos, si este se informa a los titulares de los datos personales, por lo que advierten que existe una política de privacidad que ha estado vigente desde el 01 de agosto de 2019, y también se tiene otra que rige desde el 05 de marzo de 2020, ambas publicadas en el sitio web de la administrada y ambas contienen la misma redacción respecto al tiempo de conservación de la información (datos personales). Asimismo, la DPDP enfatiza que no se discute si la administrada cuenta o no con política de privacidad, sino que cumple con lo dispuesto por el art. 18 de la LPDP, por lo que hay una necesidad de realizar un examen de inteligibilidad y un examen legal respecto a la redacción que yace en esta. Al ser materia de análisis por la DFI, se dispuso que no cumplía con informar de manera clara lo dispuesto por el artículo en mención; sin embargo, la DPDP advierte que, si bien el tiempo no se establece en meses, años, días, se entiende que la conservación se dará por el tiempo que se atienda la solicitud, entregándose una información idónea al titular de los datos.

4.4. ¿Cuál es la Finalidad e Importancia de Graduar las Sanciones y el Cálculo de la Multa en los Fallos de las Resoluciones Emitidas por la ANPD en los Años 2020 y 2021?

Mediante el proceso administrativo se llega a determinar la comisión de una infracción. Es mediante las sanciones administrativas que se sanciona administrativamente mediante multas pecuniarias y suspensión de autorización al infractor.

La finalidad de la sanción es disuadir y castigar una conducta ilícita. Mediante la sanción, la Administración ejerce coerción en los individuos para que se ciñan al cumplimento de las leyes causando dos efectos: el primero, disuasivo, pues procura evitar que se sigan cometiendo en el futuro conductas como la sancionada por el infractor o por terceros; el segundo, correctivo, pues suspende la comisión de la conducta infractora y devuelve a la sociedad el equilibrio perdido (Gómez et al., 2010).

La comisión de la conducta sancionable no debe resultar beneficiosa al infractor, sino para cumplir con las normas infringidas, por lo que dicha sanción debe ser proporcional al incumplimiento calificado como infracción.

En cuanto a las amonestaciones, se pueden aplicar cuando la infracción resulte mínima o inexistente y en la cual se puede presentar atenuantes. La administración solo puede hacer un llamado de atención sin imponer una sanción pecuniaria. El llamado de atención pude considerase como un antecedente.

Gómez et al. (2010) mencionan que la multa es una sanción que afecta pecuniariamente al administrado, pues tendrá que realizar un pago a favor de la Administración por la transgresión, el cual se establecerá en virtud de los principios de razonabilidad y proporcionalidad.

La principal finalidad de la infracción es que el administrado no vuelva a cometer la infracción administrativa; asimismo, se busca la protección del Ordenamiento Jurídico.

¿Cuál es la limitación al graduar la multa?

De acuerdo a lo establecido en el artículo 39 de la LPDP, las sanciones se califican en tres: leves, graves o muy graves. La imposición tributaria va desde las cinco unidades impositivas tributarias hasta una multa de cien unidades impositivas tributarias; asimismo se puede dictar medidas correctivas de acuerdo al artículo 118 del RLPDP.

El art. 257° del TUO de la LPAG explica los eximentes y atenuantes de responsabilidad en el PAS, el cual menciona lo siguiente: “1. Constituyen condiciones eximentes de la responsabilidad por infracciones las siguientes: a) el caso fortuito o la fuerza mayor debidamente comprobada; b) obrar en cumplimiento de un deber legal o el ejercicio legítimo del derecho de defensa; c) la incapacidad mental debidamente comprobada por la autoridad competente, siempre que esta afecte la aptitud para entender la infracción; d) la orden obligatoria de autoridad competente, expedida en ejercicio de sus funciones; e) el error

inducido por la Administración o por disposición administrativa confusa o ilegal. La subsanación voluntaria por parte del posible sancionado del acto u omisión del imputado como constitutivo de infracción administrativa, con anterioridad a la notificación de la imputación de cargos a que se refiere el inciso 3) del artículo, constituyen condiciones atenuantes de la responsabilidad por infracciones, siendo las siguientes: a) si iniciado un PAS el infractor reconoce su responsabilidad de forma expresa y por escrito. En los casos en que la sanción aplicable sea una multa, esta se reduce hasta un monto no menor de la mitad de su importe; y b) otros que se establezcan por norma especial".

En las resoluciones analizadas se utiliza la graduación de las sanciones, las cuales son:

a) El beneficio ilícito resultante por la comisión de las infracciones.
b) La probabilidad de detección de las infracciones.
c) La gravedad del daño al interés público y/o bien jurídico protegido.
d) El perjuicio económico causado.
e) La reincidencia en la comisión de las infracciones.
f) Las circunstancias de la comisión de la infracción.
g) La existencia o no de intencionalidad en la conducta del infractor.

Cálculo de la multa correspondiente: se realiza a través de la Metodología para el Cálculo de Multas de Protección de Datos Personales, la cual se aprobó mediante Resolución Ministerial N.º 0326-2020-JUS, a fin de establecer un criterio para el cálculo del monto de la multa a aplicarse.

Tabla 2

Fórmula general para determinar la sanción

Fórmula general.	
M = Mb x F	M: Multa preestablecida correspondiente a cada caso. Se aplica cuando se producen dos situaciones: Cuando sean infracciones graves o leves y cuando no se genere ningún beneficio ilícito.
	MB: Montó base de la multa a ser impuesta. Gravedad del daño.
	F: elementos agravantes.

Componentes:

Monto Base (Mb): esto depende de la gravedad del bien jurídico protegido que vendría a ser el control de los datos personales.

- **Variable Absoluta:** es respecto al nivel de gravedad de la infracción, desde leve, grave o muy grave, de acuerdo con lo establecido en el art 132° del RLPDP.
- **Variable Relativa:** tiene dos elementos: el primero es la afectación indirecta o directa hacia el bien jurídico y el segundo es la vulneración de los principios rectores.

Los montos base de las multas prestablecidas, según las variables relativa y absoluta de las infracciones, son los siguientes:

Tabla 3

Montos de la base de multas preestablecidas

Multa UIT		Variable relativa y monto base (Mb)					Gravedad de la infracción
Min	**Max**	**1**	**2**	**3**	**4**	**5**	
0.5	5	1.08	2.17	3,25			**Leve**
5	50	7.50	15.00	22.50	30.00	37.50	**Graves**
50	100			55.00	73.33	91.67	**Muy graves**

Nota: Adaptado de Resolución Ministerial N.º 0326-2020-JUS.

Factor de agravantes y atenuantes (F)

Mediante el componente F se incorporan los criterios del art 248°, numeral 3 del TUO de la LPAG, así como los artículos 125 y 126 de la LPDP.

Por lo que el factor es el siguiente:

$$F = 1 + \Sigma_{i=1}^{n} f_i$$

F corresponde al factor (agravante o atenuante), es decir, la intencionalidad, la reincidencia, las circunstancias y el perjuicio económico; sumados dan el factor que multiplican al monto base. Se debe considerar que el perjuicio económico será tomado en cuenta, pero de manera cualitativa.

Asimismo, cada elemento atenuante o agravante tiene un valor según el cuadro establecido de la siguiente manera:

Valores de factores agravantes y atenuantes

Figura 8

Valores de factores agravantes y atenuantes

Valores de factores agravantes y atenuantes

f_n	Factores agravantes o atenuantes	Valor
f_1	**(d) Perjuicio económico causado**	
$f_{1.1}$	. No existe perjuicio.	0.00
$f_{1.2}$	. Existiría perjuicio económico sobre el denunciante o reclamante.	0.10
f_2	**(e) Reincidencia**	
$f_{2.1}$	. No hay reincidencia.	0.00
$f_{2.2}$	. Primera reincidencia.	0.20
$f_{2.3}$	. Dos o más reincidencias.	0.40

f_n	Factores agravantes o atenuantes	Valor
f_3	**(f) Las circunstancias**	
$f_{3.1}$	. Cuando la conducta infractora genere riesgo o daño a una persona.	0.10
$f_{3.2}$	. Cuando la conducta infractora genere riesgo o daño a más de dos personas o grupo de personas.	0.20
$f_{3.3}$	. Cuando la conducta infractora haya afectado el interes público.	0.30
$f_{3.4}$	. Cuando la infracción es de carácter instantáneo y genera riesgo de afectación de otros derechos.	0.15
$f_{3.5}$		
$f_{3.6}$	. Cuando la duración de la infracción es mayor a 24 meses.	0.25
$f_{3.7}$	. Entorpecimiento en la investigación y/o durante el procedimiento.	0.15
	. Reconocimiento de responsabilidad expreso y por escrito de las imputaciones, después de notificado el inicio del procedimiento sancionador.	-0.30
$f_{3.8}$	. Colaboración con la autoridad y acción de enmienda parcial, después de notificado el inicio del procedimiento sancionador.	-0.15
$f_{3.9}$	. Colaboración con la autoridad, reconocimiento espontáneo y acción de enmienda, después de notificado el inicio del procedimiento sancionador.	-0.30
f_4	**(g) Intencionalidad**	
$f_{4.1}$	. Se advierte conocimiento y voluntad de cometer la conducta infractora	0.30

Nota: Adaptado de Resolución Ministerial N.º 0326-2020-JUS.

El valor de F se calculará a parte de los factores atenuantes y agravantes, de la siguiente manera:

$$F = 1 + \sum_{i=1}^{n} f_i = 1 + f_1 + f_2 + f_3 + f_4$$

Una vez sean definidos los valores de F y Mb, se realiza la cuantía de la multa de acuerdo con la fórmula general.

Tabla 4

Aplicación de la fórmula del cálculo de la multa en las RD

RD: 3039-2021-JUS/DGTAIPD-DPDP **FÓRMULA DEL CÁLCULO DE LA MULTA**
MB: 15.00 UIT
F: 0.85
Valor de la multa: 12.75 UIT
RD: 1436-2021-JUS/DGTAIPD-DPDP **FÓRMULA DEL CÁLCULO DE LA MULTA**
MB: 22,50 UIT
F: 0.80
Valor de la multa: 18 UIT
RD: 418-2021-JUS/DGTAIPD-DPDP **FÓRMULA DEL CÁLCULO DE LA MULTA**
MB: 7.5UIT
F: 1.60
Valor de la multa: 12 UIT
RD: 1944-2021-JUS/DGTAIPD-DPDP **FÓRMULA DEL CÁLCULO DE LA MULTA**
MB: 7.50 UIT
F: 0.75
Valor de la multa: 5.63 UIT

Nota. Elaboración propia.

Tabla 5

Graduación de sanciones en las resoluciones administrativas

GRADUACIÓN DE SANCIONES EN LAS RESOLUCIONES ADMINISTRATIVAS

R.D. N° 1885-2020-JUS/DGTAIPD-DPDP **Exp. N.º 143-2018-JUS/DGTAIPD-PAS**	
A: La administrada no se beneficia ilícitamente. **B:** La infracción es baja. **C:** Se vulnera el derecho a la protección de datos, específicamente el principio de consentimiento. **D:** No existe perjuicio económico.	**E:** La administrada no es reincidente. **F:** Respecto a la obtención del consentimiento de los usuarios. **G:** La administrada es responsable de la infracción imputada.
R.D. N.° 1045-2020-JUS/DGTAIPD-DPDP **Exp. N.º 127-2018-JUS/DGTAIPD-PAS**	
A: Respecto al primero, segundo y tercer hecho infractor, no se evidenció beneficio ilícito. **B:** Sobre los hechos infractores primero y segundo: las infracciones realizadas por la administrada son altas. Respecto al tercer hecho infractor, es medio. **C:** Primer hecho infractor: no cumplió con la política de privacidad respecto al flujo transfronterizo. Segundo hecho infractor: el acceso al RNPDP es de manera pública en el sistema web. Tercer hecho infractor: la administrada realizó acciones de enmienda. **D:** Primer hecho infractor: no existe perjuicio económico por la infracción. Segundo y tercer hecho infractor: sí se evidencia un perjuicio económico.	**E:** Primer, segundo y tercer hecho infractor: la administrada no es reincidente **F:** Primer hecho infractor: se tomó en consideración las enmiendas realizadas por parte de la administrada. Segundo hecho infractor: no realizó acciones de enmienda. Tercer hecho infractor: realizó acciones de enmienda. **G:** Primer hecho infractor: queda probada la responsabilidad por parte de la administrada. Segundo hecho infractor: queda probada la responsabilidad. Tercer hecho infractor: queda probada la infracción; se considera atenuante el no realizar enmienda efectiva.
R.D. N.º 1049-2020-JUS/DGTAIPDP-DPDP **Exp. N.º 141-2018-JUS/DGTAIPD-PAS**	
A: No existe beneficio ilícito a favor de la administrada. **B:** La infracción es media. **C:** No cumplió con el deber de informar. **D:** No se evidencia perjuicio económico.	**E:** No fue sancionada anteriormente. **F:** Realizó acciones de enmienda. **G:** Queda probada ha responsabilidad.
R.D N.° 1580-2020-JUS/DGTAIPD-DPDP. **Exp. N.º 142-2018-JUS/DGTAIPD-PAS**	
A: No existe beneficio ilícito a favor de la administrada. **B:** La infracción es alta. **C:** Afecta al derecho a la protección de datos personales. **D:** No se evidencia un perjuicio económico.	**E:** No fue sancionada anteriormente. **F:** La omisión de la inscripción ante el RNPDP al banco de datos no es un procedimiento ni complejo ni oneroso. **G:** La administrada realizó acciones de enmienda.

R.D. N.° 3292-2019-JUS/DGTAIPD-DPDP **Exp. N.º 74-2018-JUS/DGTAIPD-PAS**	
A: No existe beneficio ilícito a favor de la administrada. **B:** La probabilidad de detección de la infracción es alta, ya que se incumplió con lo dispuesto en el art 18 de la LPDP. En cuanto al no inscribir en el RNPDP los datos personales, se estaría ante una infracción alta. En cuanto al no cumplir con las medidas de seguridad, se está ante una inflación baja. **C:** El no haber realizado las medidas de seguridad adecuadas. **D:** No se evidencia un perjuicio económico.	**E:** No fue sancionada anteriormente. **F:** No realizó acciones de enmienda. **G:** Se puede evidenciar el desconocimiento de la entidad sobre el RLPDP y la LPDP, específicamente en el tema de las medidas de seguridad.
R.D. N.° 2077-2020-JUS/DGTAIPD **Exp. N.º 154-2019-JUS/DGTAIPD-PAS**	
A: La infracción no genera beneficio ilícito a la administrada. **B:** La conducta infractora es alta. **C:** No garantizó la protección de los datos sensibles al no contar con las medidas de seguridad y el respaldo de confidencialidad. **D:** No se evidencia perjuicio económico.	**E:** No fue sancionada anteriormente. **F:** La administrada no realizó acciones de enmienda respecto a las conductas infractoras realizadas. **G:** Queda probada la responsabilidad de las infracciones imputadas a la administrada.
RD N.º 515-2019-JUS/DGTAIPD-DPDP **Exp. N.º 068-2018-JUS/DPDP-PS**	
A: No se evidencia beneficio ilícito. **B:** Respecto a la primera y segunda infracción, se tiene que son de alta probabilidad de detección. En cuanto a la tercera infracción, es baja. **C:** Afecta al derecho a la protección de datos personales. **D:** No se evidencia perjuicio económico por la comisión de la infracción.	**E:** La administrada no es reincidente. **F:** Respecto a la primera, segunda y tercera infracción, la administrada realizó acciones de enmienda. **G:** No se acredita la intencionalidad para la comisión de las infracciones.
R.D N.° 1529-2020-JUS/DGTAIPD-DPDP **Exp. N.º 150-2018-JUS/DGTAIPD-PAS**	
A: Si se evidencia beneficio ilícito de la comisión de la infracción. **B:** Respecto a las conductas sobre el consentimiento y el deber de informar, es baja. Respecto a la no comunicación del flujo transfronterizo en el RNPDP, es alta. **C:** Se incumplió con el principio de consentimiento. Asimismo, la autodeterminación informativa y, por último, no se cumple con lo establecido en la normativa por haber omitido la inscripción a la RNPDP. **D:** No se evidencia perjuicio económico.	**E:** La administrada no es reincidente. **F:** La obtención del consentimiento y el deber de información se debe realizar mediante lo dispuesto por la norma. En cuanto a la omisión de la inscripción del flujo transfronterizo, no es un procedimiento difícil ni completo a realizar. **G:** La administrada realizó acciones de enmienda.
RD: 1180-2020-JUS/DGTAIPD-DPDP **Exp. N.º 07-2019-JUS/DGTAIPD-PAS**	

A: No se evidencia beneficio ilícito. **B:** El primer hecho infractor es medio. La infracción del segundo y tercero es alta. **C:** Se vulnera la protección de datos personales, específicamente el art 18° de la LPDP y el no haber realizado la inscripción en el RNPDP del banco de datos. **D:** No se evidencia perjuicio económico.	**E:** No es reincidente. **F:** Respecto al incumplimiento del art 18 de la LPDP, no se observaron acciones de enmienda. En cuanto al incumplimiento de inscripción al banco de datos, sí se realizó acción de enmienda. La administrada reconoció los hechos imputados. **G:** Se mostraron acciones de enmienda.
RD: 1981-2020-JUS/DGTAIPD-DPDP **Exp. N.º 139-2019-JUS/DGTAIPD-PAS**	
A: No se evidencia beneficio ilícito. **B:** Se incumple lo dispuesto en el art 18, por lo que se estaría ante una infracción media. No cumple con las medidas de seguridad, por lo que la infracción es baja. **C:** Afecta la protección de datos personales tipificada en la Constitución. Incumplió lo dispuesto en el art 18 de la LPDP. El no aplicar las medidas de seguridad del tratamiento de datos personales en el banco de datos, incrementa el riesgo de vulneración de datos sensibles. **D:** No se evidencia perjuicio económico**.**	**E:** **E:** La administrada no es reincidente. **F:** El incumplimiento del art 18 de la LPDP no es complejo, ni oneroso. **G:** Se evidenciaron acciones de enmienda.

Nota. Elaboración propia.

4.4.1. ¿Cuáles son las Decisiones o Fallos de las Resoluciones Emitidas por la ANPD en los Años 2020 y 2021?

La importancia de las decisiones o fallos: toda decisión debe de estar debidamente motivada y deben sustentarse las razones que han conducido a adoptar esa decisión. No solo es expresar una norma legal, sino fundamentar, exponer las razones y sustentar jurídicamente la decisión tomada.

Las sanciones administrativas y su importancia: las sanciones administrativas son un tipo de acto administrativo que constituye una sanción de aspecto punitivo, ya sea por una conducta ilegal o poco ética de parte del administrado. Se inicia con una infracción realizada a la administración, lo que conlleva a un procedimiento administrativo.

El gravamen que se le impone suele ser comúnmente por realizar conductas lesivas a un bien jurídico protegido, por lo que se impone una infracción. Las autoridades administrativas imponen estas sanciones de acuerdo a los principios y normas.

Tabla 6

Resumen de las sanciones impuestas en las 17 resoluciones

RD	INSTANCIA	DECISIÓN	SANCIÓN IMPUESTA
RD: 1885-2020-JUS/DGTAIPD-DPDP	Primera Instancia- DPDP	Sancionar a ONCOLOGIA S.A.C por usar los datos personales de los pacientes para otras finalidades.	• 5,01 UIT
RD: 1436-2020-JUS/DGTAIPD-DPDP	Primera Instancia- DPDP	Sancionar a Clínica San Pablo S.A.C por haber incumplido la obligación de confidencialidad.	• 18,00 UIT
RD:1045-2020-JUS/DGTAIPD-DPDP	Primera Instancia-DPDP.	Sancionar a Servicios de Salud Montefiori S.A.C, al infringir lo tipificado en el literal a) del numeral 2 del art 132 del RLPDP; asimismo, sancionar por lo tipificado en el literal e), numeral 1, del art. 132° de RLPDP; Sancionar por la comisión de la infracción grave tipificada en el literal c) del numeral 2 del art. 132 del RLPDP.	• 7 UIT, • 1,5 UIT, • 6,5 UIT
RD: 1459-2020-JUS/DGTAIPD-DPDP	DGTAIPD	Infundado el recurso de apelación por Clínica Mundo Salud S.A.C. Confirmar la RD N°1459-2020-JUS/DGTAIPD-DPDP.	• 5,1 UIT
RD: 3454-2021-JUS/DGTAIPD-DPDP	DPDP – Competente en impulso, admisión, etc.	Improcedente la solicitud presentada por la persona XXX contra el Seguro Social de Salud-ESSALUD.	• -
RD: N.º 3292 -2019-JUS/DGTAIPD-DPDP	En Primera Instancia - DPDP. Se presentó recurso de Apelación mediante RD:16-2021-JUS/DGTAIPD, el cual fue declarado infundado.	Sancionar a Clínica del Pacifico S.A por incurrir en una infracción grave tipificada en el art 132 numeral 2 literal a del RLPDP. Asimismo, por incurrir en una infracción grave tipificada en el art 132° numeral 1 literal e) del RLPDP. Por último, por incurrir en una infracción leve tipificada en el art 132 numeral 1 literal a) del RLPDP.	• 6,5 UIT • 1,5 UIT • 8 UIT

RD: N.º 1049-2020-JUS/DGTAIPD-DPDP	Primera Instancia. DPDP	Sancionar a Clínica Santa Martha del Sur S.A.C	• 5,1 UIT
RD: 1180-2020-JUS/DGTAIPD-DPDP	Primera Instancia- DPDP	Declaró infundado la imputación a Centro Médico Ohi S.A.C. respecto a la comisión de la infracción grave del art 132, numeral 2, literal b). Sancionar a la administrada por haber incurrido en una infracción grave al no haber cumplido con lo dispuesto en el art 18 de la LPDP. Asimismo, incurrió en una infracción leve por no cumplir con lo establecido en el art 132, numeral 1, literal e) del RLPDP. Por último, por haber incurrido en una infracción leve por no cumplir con lo tipificado en el art 132, numeral 1, literal e) del RLPDP.	• 6 UIT • 1 UIT • 0,5 UIT
RD:1580-2020-JUS/DGTAIPD-DPDP.	Primera Instancia- DPDP	Sancionar a Clínica La Luz S.A.C. por haber incurrido en una infracción grave por no haber cumplido lo dispuesto en el art 132, inc 2, literal a). Asimismo, por haber incurrido en una infracción leve por no cumplir lo tipificado en el art 78 del RLPDP. Por último, por incurrir en una infracción leve tipificada en el art 132, inc 2, literal c), del RLPDP.	• 10 UIT • 5 UIT • 1 UIT • 10 UIT
RD: N° 3039-2021-JUS/DGTAIPD-DPDP	Primera Instancia-DPDP.	Sancionar a Genetics S.A.C. por no haber cumplido con lo establecido en el art 18° de la LPDP, incurriendo en una infracción grave	• 9,86 UIT
RD:2077-2020-JUS/DGTAIPD-DPDP	Primera Instancia-DPDP. Se presentó recurso de Apelación mediante RD:13-2020-JUS/DGTAIPD,	Sancionar al Hospital de Emergencias José Casimiro Ulloa por haber incurrido en una infracción grave tipificada en el art 132 numeral 2, literal g del RLPDP.	• 25 UIT

	el cual fue declarado infundado.		
RD:515-2019-JUS/DGTAIPD-DPDP	Primera Instancia- DGTAIPD. Se presentó recurso de Apelación mediante RD:13-20202-JUS/DGTAIPD, el cual fue declarado infundado.	Sancionar a Clínica Médica Cayetano Herida S.A, por incurrir en una infracción leve establecida en el art 38° numeral 1, literal b de la LPDP. Asimismo, por incurrir en una infracción leve tipificada en el art 38° numeral 1, literal a. Por último, por incurrir en una infracción grave tipificada en el art 38°, numeral 2, literal a.	• 2 UIT • 1,5 UIT • 4,5 UIT
RD: 1529-2020-JUS/DGTAIPD-DPDP	Primera Instancia- DPDP	Sancionar a Clínica Morillas S.A. por incurrir en una infracción grave estipulada en el art 13 inc. 13.5 de la LPDP y en el art 12 del RLPDP. Asimismo, por incurrir en una infracción grave de acuerdo con lo estipulado en el art 18.b de la LPDP. Por último, por incurrir en una infracción leve por incurrir en lo establecido en el art 26 del RLPDP.	• 2 UIT • 2 UIT • 0,5 UIT
RD:1944-2021-JUS/DGTAIPD-DPDP	Primera Instancia- DPDP	Sancionar a Policlínico Los Naranjos E.I.R.L. respecto a la infracción del art 132°, numeral 2, literal a) del RLPDP.	• 5,63 UIT
RD: 418-2021-JUS/DGTAIPD-DPDP	Primera Instancia- DPDP	Infundada en parte a Especialidades Médicas Universales S.A. respecto a la infracción del art 18° de la LPDP. Fundada al haber incumplido con lo dispuesto en el art 18° de la LPDP, incurriendo en una infracción grave.	• 12 UIT
RD: 1981-2020-JUS/DGTAIPD-DPDP	Primera Instancia- DPDP	Eximir a Centro médico San Judas Tadeo S.A. respecto a la imputación del tratamiento de las cámaras de video vigilancia. Sancionar a la administrada por infringir los dispuesto en el art 18 de la LPDP. Asimismo, sancionar a la	• 5,01 UIT • 1,5 UIT

		administrada por no cumplir con las medidas de seguridad.	
RD: 313-2019-JUS/DGTAIPD-DPDP	Primera Instancia- DPDP	Infundada la imputación hacia Ópticas GMO Perú S.A.C.	-

Nota. Elaboración propia.

Capítulo V. Discusión

Tabla 7

Resumen de los 17 casos analizados en la investigación

Resol.	Entidad	Hechos	
1885-2020-JUS/DGTAIPD-DPDP	ONCOLOGIA S.A.C.	No tener el debido consentimiento para el uso o trato de los datos personales. No informar al titular de los datos personales de cómo estos serán tratados. Motivación 1° Hecho Infractor: la DPDP determina que la imputación se da por la evaluación que realiza la DFI del documento "autorización de uso de datos personales en historia clínica", ya que induce al error al interesado. La administrada no informa de manera correcta la finalidad del tratamiento cuando consigna en un apartado el término "entre otros"; la DPDP menciona que la administrada, en su primer descargo, adjunta un documento sin modificación de la "autorización de uso de datos personales en historia clínica"; la DPDP determina que, de analizado el documento, se retira la finalidad del para qué era necesario el consentimiento; no teniendo fecha cierta según lo establece el art. 245 del Código Procesal Civil, se consideró la data de su escrito donde se adjunta este medio probatorio; aunado a ello, la DPDP considera dicho documento como una acción de enmienda en la responsabilidad que le atañe a la administrada, por ser de fecha posterior a la notificación del PAS de inicio, lo cual reitera en sus fundamentos expresados respecto al descargo posterior que realiza la administrada, siendo responsable por el hecho infractor y poseyendo a su favor las acciones de enmienda. 2° Hecho infractor: la DPDP indica que, mediante dos actas de fiscalización, constata que la administrada recopila datos personales mediante su sistema y/o aplicativo, pero que no está en la obligación de solicitar el consentimiento para ello; eso no la exime de informar respecto al tratamiento que brindará a estas, lo cual la administrada prueba que realiza mediante su descargo de fecha 15 de agosto del 2019, cumpliendo con el art. 18 de la LPDP; y ello lo realiza con anterioridad a la notificación de la resolución que da inicio al proceso administrativo sancionador, por lo que se le debe eximir de responsabilidad. Decisión Sancionar a Oncología S.A.C.	Sanción impuesta Se impone una multa de 5.01 UIT por utilizar los datos personales de los pacientes para fines no relacionados con la prestación

		Eximir a Oncología S.A.C. respecto a la responsabilidad administrativa de la infracción grave tipificada en el literal a), numeral 2, del art. 132 del Reglamento de la LPDP.	del servicio, sin obtener válidamente el consentimiento del titular de los datos.
1436-2021-JUS/DGTAIPD-DPDP	CLÍNICA SAN PABLO S.A.C.	Hechos No hubo confidencialidad de los datos personales por parte del encargado. Motivación La DPDP afirma que la DFI imputa a la administrada haber brindado datos personales de su paciente a Avianca S.A., indicando que fue un error y sancionan a su colaboradora quien remite dicha información. La administrada presenta sus descargos, indicando que no se determina el beneficio ilícito que poseen por cometer la infracción, el perjuicio económico o confiscatoria, entre otros; asimismo, señala que su conducta fue corregida voluntariamente y con anterioridad a la emisión de la resolución de sanción. La DPDP indica que la DFI no imputa como una agravante que la información compartida haya sido sensible, sino que el hecho infractor se basa en la falta de confidencialidad de la administrada con su paciente sobre sus datos personales, y que su accionar fue instantáneo porque se configuró cuando se transfiere la información sin consentimiento del titular, no pudiendo ejercer acción de enmienda la administrada porque ya Avianca poseía la información, sin perjuicio de que la administrada realice acciones idóneas para no repetir el hecho infractor.	
		Decisión	Sanción impuesta
		Sancionar a Clínica San Pablo S.A.C.	Se aplica una multa de 18.00 UIT debido a la realización de tratamiento de datos personales sin cumplir con la obligación de confidencialidad.
1045 - 2020-JUS/DGTAIPD-DPDP	SERVICIOS DE SALUD MONTEFIORI S.A.C	Hechos No tener el debido consentimiento para el uso o trato de los datos personales. No informar al titular de los datos personales de cómo estos serán tratados. No inscripción de banco de datos en el RNPDP. No informar a la DGTAIPD del flujo transfronterizo que se realiza de los datos personales. No presenta medidas de seguridad apropiadas para el tratamiento de datos personales, que incluyen datos sensibles. Motivación 1° Hecho infractor: la DPDP señala que un hecho infractor debe ser detectado, indagándose sobre este; es decir, no solo basta con verificar o visualizar el contenido o la composición de la página web de la administrada, sino la importancia radica en si la divulgación de las imágenes ha sido autorizada por sus propietarios. La DPDP indica que, de autos, no se acredita dicho accionar; además, en la etapa previa al inicio del proceso sancionador, solo se da a conocer la difusión de imágenes, por tal motivo la DPDP no propugna como objeto de sanción este hecho infractor. 2° Hecho infractor: primero, la DPDP indica la obligación que posee el responsable del tratamiento de los datos personales de proporcionar información detallada al titular de los datos, sobre cómo se utilizarán estos, cómo se recopilarán y su	

		tratamiento, pues la referencia del art. incoado va más allá del simple consentimiento, generando que el titular pueda ejercer sus otros derechos de manera efectiva. 3° Hecho infractor: la administrada en sus descargos indica que solo tiene pendiente la inscripción del banco de datos de médico. La DFI se pronuncia mediante su informe final de instrucción, brindando como recomendación que se archive en este extremo el PAS. la DPDP indica estar de acuerdo con lo expresado por la DFI, por lo que se confirma el archivamiento definitivo. 4° Hecho Infractor: La DPDP señala que, si bien existe una solicitud de la administrada para la inscripción del flujo transfronterizo, esta fue observada, pero no se realizaron las subsanaciones incoadas; por tanto, la administrada tiene responsabilidad al respecto. 5° Hecho infractor: se realizó el análisis de dos hechos respecto a: i) no registrar los procedimientos para gestionar los privilegios y realizar verificaciones periódicas de los privilegios asignados, así como de ii) no realizar el cierre de sesión de los usuarios como resultado de su actividad en los sistemas que registran el tratamiento de datos personales. Mediante informe técnico, la DFI indicó que la administrada presenta documentación adicional donde se advierte que sí cumple con el punto i) y ii). La DFI indica que la administrada no dispone de las medidas de seguridad idóneas en su "centro de datos. Al respecto, la DPDP señala que la administrada ha cumplido con implementar todo ello, puesto que brinda sus descargos. Decisión — Sanción impuesta Eximir de responsabilidad a Servicios de Salud Montefiori S.A.C. Sancionar a Servicios de Salud Montefiori S.A.C. — Se establece una multa de 7 UIT por obstruir el ejercicio de los derechos del titular de datos personales; 1.5 UIT por no registrar o actualizar en el RNPDP; y 6.5 UIT por tratar datos personales sensibles sin cumplir con las medidas de seguridad. Imponer medidas correctivas a Servicios de Salud Montefiori S.A.C.
RD N° 1459-2020-JUS/DGTA IPD-DPDP	Clínica Mundo Salud S.A.C.	Hechos No tener el debido consentimiento para el uso o trato de los datos personales. Motivación 1° Análisis: la DPDP inicia incoando al art. 219 de la LPAG, el cual indica que el recurso de reconsideración se interpone ante el mismo órgano que ya emitió pronunciamiento sobre el caso, siendo un requisito primordial el presentar nueva prueba para que la autoridad pueda sustentar y emitir un nuevo criterio; es decir, al presentarse dicho recurso, el administrado busca que la autoridad varié su criterio y solo se dará ese supuesto cuando se evalúe que haya un nuevo hecho o prueba que no fue presentada o que su actuación no se solicitó por desconocimiento de su existencia o que, en su momento, había imposibilidad de obtenerla y no fue valorada; sin embargo, no todos los elementos probatorios nuevos son idóneos para una reconsideración. 2° Análisis: del escrito presentado por la administrada, la DPDP no advierte medios probatorios que brinden indicios de hechos novedosos o que no hayan sido conocidos por la administrada ni por la autoridad resolutoria, por lo que no se permite brindar nuevos argumentos ni se vislumbra el requerimiento de una nueva revisión de los hechos.

		Decisión	Sanción impuesta
		Declarar IMPROCEDENTE el recurso de reconsideración interpuesto por Clínica Mundo Salud S.A.C. contra la RD N.º 11082020-JUS/DGTAIPD-DPDP.	5.1 UIT por no cumplir con informar al titular de los datos personales sobre el tratamiento que se realizará a sus datos.
3454-2021-JUS/DGTAIPD-DPDP	Seguro Social De Salud – ESSALUD	Hechos Solicitud por parte del afectado solicitando información con respecto al procedimiento de reembolso Se deriva del Tribunal de Transparencia y Acceso a la Información Pública a la DGTAIPD. Motivación 1° Análisis: la DPDP indica que el derecho fundamental a la protección de datos lo resguarda el art. 2, numeral 6 de la Constitución; es así que, a través del art. 1 de la LPDP, se hace referencia a ello, añadiendo que el objeto de creación de dicha ley radica en la protección de los datos personales que se darán cuando haya un adecuado tratamiento de estos, dentro de un marco de respeto a otros derechos fundamentales que se reconocen; además, se dará tanto en el sector público como en el privado. La DPDP menciona que los principios se encuentran en la LPDP, y su RLPDP sirve para brindar seguridad y resguardo a la protección de los datos personales. Además, el titular podrá ejercer sus derechos ARCO, encontrándose todo esto previsto en los artículos que van del 18 al 22 de la LPDP. 2° Análisis: la DPDP indica que el interesado tiene la facultad para solicitar informaciones, entendiéndose como obligado a las entidades; además, la DPDP precisa que el derecho de petición podrá incluir información o no de los propios administrados, y si fuese así, no es motivo para que se niegue la atención al ejercicio de este derecho; en consecuencia, se concluye que se debe atender al administrado en ejercicio de su derecho de petición, lo cual queda fuera de su ámbito de aplicación al ser incompetente en razón de la materia.	
		Decisión	Sanción impuesta
		Declarar improcedente la solicitud presentada por el administrado en el Exp. N.º 3435-2021 contra el Seguro Social de Salud- ESSALUD, por resultar la DPDP incompetente debido a la materia.	No se impuso una sanción
3292-2019-JUS/DGTAIPD-DPDP	Clínica del Pacifico S.A.	Hechos No informar al titular de los datos personales de cómo estos serán tratados. No inscripción de banco de datos en el RNPDP. No informar a la DGTAIPD del flujo transfronterizo que se realiza de los datos personales. Motivación 1° Hecho infractor: el despacho señala que, mediante RD, se imputa a la administrada tratar la información de los titulares por un sistema y formularios físicos. La DPDP declara responsable a la administrada. 2° Hecho infractor: la administrada indicó que realiza la inscripción de su banco de datos, para cumplir y colaborar con la autoridad, pero la RD N.º 1802-2019 negó dicho registro sobre el sistema de vigilancia; por tanto, la administrada solo enmienda su conducta respecto a los proveedores, sin poderle aplicar la atenuación de su responsabilidad administrativa, incurriendo en una infracción leve.	

		3° Hecho infractor: al respecto, la DPDP señala el objetivo de la seguridad que se debe brindar al tratar datos personales, puesto que hay medidas organizativas, técnicas y legales a adoptarse, y que se debe evitar la pérdida, alteración, acceso o tratamiento que no se autorice respecto a los datos personales. La DPDP añade que a la administrada se le detecta que brinda un tratamiento automatizado a datos personales sensibles, y brinda la definición establecida en el art. 2 de la LPDP, imputándosele la comisión del art. 132, numeral 2, literal c) del RLPDP: una infracción grave. Decisión Infundado el recurso de apelación por Clínica Mundo Salud S.A.C.	Sanción impuesta Se establece 5.1 UIT por no cumplir con informar al titular de los datos personales sobre el tratamiento que se realizará a sus datos.
1049-2020-JUS/DGTAIPD-DPDP	Clínica Santa Martha del Sur S.A.C.	Hechos No tener el debido consentimiento para el uso o trato de los datos personales. No informar al titular de los datos personales de cómo estos serán tratados. No inscripción de banco de datos en el RNPDP. Motivación 1° Hecho infractor: la DPDP señala que, de revisado el informe técnico de la DFI, se concluye que la administrada no cuenta con su sitio web activo, no realizando un tratamiento de datos personales; sin embargo, la DPDP identifica que la DFI imputa este hecho a un sitio web incorrecto, debiendo ser otro que también posee como titular a la administrada, indicando, de oficio, que se puede realizar la fiscalización y que, sin perjuicio de ello, la administrada tenga sus documentos con las autorizaciones correspondientes. 2° Hecho infractor: la DPDP indica que, si bien el art. 18 de la LPDP se relaciona con el consentimiento, su finalidad en sí es que al titular se le informe sobre el tratamiento que se les brindará a sus datos personales; ahora bien, se le impone como hecho infractor tres puntos esenciales: el tratamiento de datos que se recopilan por el “sistema clínico”, así como a través de formularios físicos y a través de su sitio web. Sobre el sitio web, se archiva este extremo, ya que la página web incoada se encuentra deshabilitada con anterioridad. 3° Hecho infractor: la administrada presenta su inscripción correspondiente, teniendo su código señalado mediante RD y, de revisada la web de la RNPDP, todos los bancos de datos que constan en dicha resolución están debidamente inscritos bajo la titularidad de la administrada, quien ha señalado que está realizando cambios a su denominación social y nombre. La DPDP advierte que varía el nivel de declaración respecto al nombre comercial ante la SUNAT, no siendo este relevante para la inscripción o modificación del banco de datos personales ante la RNPDP, considerándose una eximente de responsabilidad; además, se exige que dicho cambio de denominación social se actualice para que todo procedimiento sea transparente. Decisión	Sanción impuesta

			Sancionar a Clínica Santa Martha del Sur S.A.C.	Se establece una multa de 5.1 UIT por obstruir el ejercicio de los derechos del titular de datos personales.
1180-2020-JUS/DGTAIPD-DPDP	CENTRO MÉDICO S.A.C.	OHI	Hechos No tener el debido consentimiento para el uso o trato de los datos personales. No informar al titular de los datos personales de cómo estos serán tratados. No inscripción de banco de datos en el RNPDP. No informar a la DGTAIPD del flujo transfronterizo que se realiza de los datos personales. Motivación 1° Hecho infractor: se le imputa a la administrada la disfunción de imágenes de personas en su página web sin previo consentimiento para ello; sin embargo, la DPDP indica que, en estos casos, para poder constatar el carácter ilícito, se debe constatar que cada imagen cuente con el consentimiento de su titular, y que del expediente administrativo se tiene solo las imágenes, pero no una constatación de cómo se obtuvo para su difusión, no demostrándose la comisión de la infracción, por lo que no es pasible de ser objeto de sanción. 2° Hecho infractor: la DPDP menciona que el cambio realizado era más de forma que de fondo; asimismo, precisa que no se trata de poner bajo qué política y protección se tratan los datos personales o conceptos que dispone la LPDP, sino que lo importante reside en informar detalladamente las condiciones de tratamiento de estos. Por todo ello, la DPDP concluye que la administrada es responsable por no realizar su obligación de informar a los titulares de los datos personales respecto al tratamiento de estos. 3° Hecho infractor: la administrada no habría inscrito los bancos de datos con el informe correspondiente; en la motivación que brinda la DPDP, refiere que la administrada era titular del banco de datos, por lo que tenía que registrar estos en el RNPDP, y que, si bien la administrada presenta su descargo, no consta alegato que desvirtué lo que se le viene imputando; sin embargo, mediante otro informe, la DFI indica que la administrada ya no recopilaba datos personales en su sitio web, por lo que ya no se le exigía la inscripción, lo cual es comprobado por la DPDP; asimismo, en su segundo descargo, la administrada presenta la solicitud de inscripción que realiza, y se verifica en el RNPDP que efectivamente consta esta, cumpliéndose con el deber que se le imputa como infracción. 4° Hecho infractor: se tiene que la administrada realiza tratamiento de datos personales a través de su sitio web y que el servidor que almacena está información se encuentra en Canadá. La administrada no realizaba flujo transfronterizo y ello es constatado por la DPDP. Es importante mencionar que la DPDP determina que la administrada cesa el tratamiento de los datos personales con posterioridad a la notificación, siendo esto una atenuante de la responsabilidad. Decisión Se declara infundado la imputación a Centro Médico Ohi S.A.C. respecto a la comisión de la infracción grave respecto al art 132, numeral 2, literal b). Sancionar a la administrada por haber incurrido en una infracción grave al no haber cumplido con lo dispuesto en el art 18 de la LPDP. Asimismo, incurrió	Sanción impuesta Se impone una multa de 6 UIT por no informar al titular de los datos personales sobre el tratamiento que se realizará a sus datos. Además, se establece una multa de 1

		en una infracción leve por no cumplir con lo establecido en el art 132, numeral 1, literal e) del RLPDP. Por último, por haber incurrido en una infracción leve por no cumplir con lo tipificado en el art 132, numeral 1, literal e) del RLPDP.	UIT por no inscribir en el RNPDP el banco de datos personales de pacientes y trabajadores. Asimismo, se establece una multa de 0.5 UIT por no comunicar al RNPDP la realización de flujo transfronterizo de los datos personales.
1580-2020-JUS/DGTAIPD-DPDP	Clínica La Luz S.A.C.	Hechos No informar al titular de los datos personales de cómo estos serán tratados. No inscripción de banco de datos en el RNPDP. No informar a la DGTAIPD del flujo transfronterizo que se realiza de los datos personales. No presenta medidas de seguridad apropiadas para el tratamiento de datos personales que incluyen datos sensibles. Motivación La DPDP investigó varias infracciones cometidas por una entidad en el manejo de datos personales. En primer lugar, la entidad no informó adecuadamente a los clientes sobre cómo se tratarían sus datos sensibles, lo que constituyó una violación grave del deber de información establecido en la LPDP. Además, se encontró que la entidad recopilaba datos de manera inadecuada a través de varios documentos y formularios, sin cumplir con los requisitos legales de transparencia y consentimiento. Esto se consideró como una infracción adicional debido a la naturaleza sensible de los datos recopilados. En segundo lugar, la entidad no registró adecuadamente su banco de datos de proveedores ante la autoridad competente, lo que constituyó otra infracción. Además, no informó a la autoridad sobre el flujo transfronterizo de datos personales, lo que también fue considerado como una violación de las normas de protección de datos. Finalmente, la entidad no implementó adecuadamente medidas de seguridad para proteger la información digital de los pacientes, lo que constituyó múltiples violaciones de los requisitos de seguridad establecidos en la LPDP. Aunque la entidad tomó medidas correctivas en algunos aspectos, como la implementación de medidas de seguridad adicionales, estas acciones se llevaron a cabo después de que se iniciara el PAS, lo que resultó en una responsabilidad parcial por parte de la entidad.	
		Decisión Sancionar a Clínica La Luz S.A.C. al haber incurrido en una infracción grave por no haber cumplido lo dispuesto en el art 132, inc 2, literal a). Asimismo, por haber incurrido en una infracción leve por no cumplir lo tipificado en el art 78 del RLPDP. Por último, por incurrir en una infracción leve tipificada en el art 132, inc 2, literal c) del RLPDP.	Sanción impuesta Se impone una multa de 10 UIT por obstruir el ejercicio de los derechos del titular de datos personales. Además, se establece una multa de 0.5 UIT por no inscribir en el RNPDP, y 1 UIT por no comunicar al RNPDP la realización de flujo transfronterizo de los datos personales. También se aplica una multa de 10 UIT por

			no proporcionar medidas de seguridad para el tratamiento de datos personales sensibles.
3039-2021-JUS/DGTA IPD-DPDP	GENETICS S.A.C.	Hechos No informar al titular de los datos personales de cómo estos serán tratados. No presenta medidas de seguridad apropiadas para el tratamiento de datos personales que incluyen datos sensibles. Motivación La DPDP analiza dos infracciones cometidas por una entidad en el manejo de datos personales. Primero, se incumple el deber de informar a los clientes sobre cómo se manejan sus datos, lo cual es esencial según la LPDP. Además, se encuentran deficiencias en la implementación de medidas de seguridad requeridas por la ley. Aunque la entidad intentó presentar evidencia de cumplimiento, falló en acreditar la fecha precisa de implementación de estas medidas. La DPDP concluye que estas acciones constituyen infracciones leves, pero destaca que la entidad tomó medidas correctivas, lo que mitigó la gravedad de las infracciones. Respecto a la autenticidad de los documentos presentados, aunque algunos no cumplen completamente con los requisitos legales de certificación de fecha, se consideran auténticos por el principio de veracidad y la colaboración procedimental. Decisión Sancionar a Genetics S.A.C. por no haber cumplido con lo establecido en el art 18° de la LPDP, incurriendo en una infracción grave.	Sanción impuesta Se establece una multa de 9.86 UIT por no cumplir con informar al titular de los datos personales sobre el tratamiento que se realizará a sus datos.
2077-2020-JUS/DGTA IPD-DPDP	Hospital de Emergencias José Casimiro Ulloa	Hechos No presenta medidas de seguridad apropiadas para el tratamiento de datos personales que incluyen datos sensibles. No guarda confidencialidad respecto a los datos personales otorgados por los titulares. Motivación En este caso, la DPDP analiza dos hechos infractores cometidos por una entidad. En el primer hecho, se cuestiona el incumplimiento de la obligación de implementar medidas de seguridad adecuadas en los sistemas utilizados para visualizar y programar imágenes médicas. La DPDP determina que la entidad no cuenta con mecanismos suficientes para controlar accesos y generar registros de interacción lógica, lo que constituye una infracción al artículo 39 del RLPDP. Aunque la entidad presenta un proyecto para mejorar la seguridad de los sistemas, la DPDP lo desestima al no estar finalizado ni implementado. En el segundo hecho, se aborda la divulgación de datos sensibles relacionados con la salud de un paciente. La DPDP encuentra que la entidad incumple el deber de confidencialidad al no proteger adecuadamente los datos sensibles y al no contar con acuerdos de confidencialidad con su personal. Además, la DPDP destaca que la divulgación de estos datos vulnera la dignidad humana y la normativa sobre protección de datos. Aunque la entidad argumenta que la decisión inicial de la DPDP carece de motivación adecuada, la DPDP concluye que la entidad efectivamente ha incurrido en la infracción por falta de confidencialidad de los datos personales. Decisión	Sanción impuesta

		Sancionar al Hospital de Emergencias José Casimiro Ulloa por haber incurrido en una infracción grave tipificada en el art 132, numeral 2, literal g del RLPDP.	Se impone una multa de 25 UIT por incumplir la obligación de confidencialidad.
515-2019-JUS/DGTA IPD-DPDP	CLÍNICA MÉDICA CAYETANO HEREDIA S.A.	Hechos No informar al titular de los datos personales de cómo estos serán tratados. No tener el debido consentimiento para el uso o trato de los datos personales. No presenta medidas de seguridad apropiadas para el tratamiento de datos personales que incluyen datos sensibles. Motivación La DPDP analiza tres presuntas infracciones cometidas por una entidad. En el primer hecho infractor, se cuestiona la falta de información proporcionada a los titulares de datos personales según lo establecido en el artículo 18 del LPDP. Aunque la entidad argumenta haber mejorado sus términos y condiciones en su página web, la DPDP determina que no se informó adecuadamente a los usuarios, iniciando un PAS. En el segundo hecho, se examina el incumplimiento del principio de consentimiento según el artículo 4 de la LPDP. Aunque la entidad implementa cambios en su página para permitir a los usuarios manifestar su consentimiento de manera explícita, la DPDP encuentra que no se informó adecuadamente sobre los destinatarios de los datos personales, aunque reconoce que no hubo transferencia de datos a terceros. En el tercer hecho, se aborda el incumplimiento de medidas de seguridad para el tratamiento de datos sensibles según el artículo 39 del RLPDP. La entidad reconoce la falta de implementación de ciertas medidas de seguridad, pero posteriormente subsana este incumplimiento. En ambos casos, la DPDP considera las acciones de enmienda realizadas por la entidad al evaluar la sanción correspondiente. Decisión Sancionar a Clínica Médica Cayetano Herida S.A. por incurrir en una infracción leve establecida en el art 38° numeral 1, literal b de la LPDP. Asimismo, por incurrir en una infracción leve tipificada en el art 38°, numeral 1, literal a. Por último, por incurrir en una infracción grave tipificado en el art 38°, numeral 2, literal a.	Sanción impuesta Se establece una multa de 2 UIT por no informar sobre los destinatarios de los datos personales. Además, se impone una multa de 1.5 UIT por no cumplir con el requisito de obtener un consentimiento libre. También se establece una multa de 4.5 UIT por no proporcionar medidas de seguridad para el tratamiento de datos personales sensibles.
1529-2020-JUS/DGTA IPD-DPDP	CLÍNICA MORILLAS S.A.	Hechos No tener el debido consentimiento para el uso o trato de los datos personales. No informar al titular de los datos personales de cómo estos serán tratados. No inscripción de banco de datos en el RNPDP. No presenta medidas de seguridad apropiadas para el tratamiento de datos personales que incluyen datos sensibles. Motivación	

		En el caso analizado, la DPDP examina cuatro presuntas infracciones cometidas por una entidad. En el primer hecho infractor, se cuestiona el tratamiento de imágenes de médicos sin consentimiento válido, así como la falta de información sobre el uso de imágenes obtenidas de terceros. Se destaca que la entidad presentó descargos, aunque algunos no cumplían con los requisitos legales. En el segundo hecho, se investiga la falta de información al titular sobre la recopilación de datos personales, tanto en formatos físicos como digitales. Aunque la entidad alega haber tomado medidas correctivas, la DPDP concluye que no cumplió con su deber de informar debidamente. En el tercer hecho, se aborda la falta de comunicación sobre el flujo transfronterizo de datos personales, situación que la entidad subsana posteriormente, aunque sin pruebas que respalden sus argumentos de fuerza mayor. Finalmente, en el cuarto hecho, se examina la seguridad en el tratamiento de datos sensibles, donde la entidad presenta evidencia de haber implementado medidas de seguridad adecuadas, lo que lleva a la recomendación de archivar el caso por parte de la DPDP.
		Decisión Sancionar a Clínica Morillas S.A. por incurrir en una infracción grave estipulada en el art 13, inc. 13.5 de la LPDP y en el art 12 del RLPDP. Asimismo, por incurrir en una infracción grave de acuerdo con lo estipulado en el art 18.b de la LPDP. Por último, por infracción leve por incurrir en lo establecido en el art 26 del RLPDP.
		Sanción impuesta Se impone una multa de 2 UIT por no obtener el consentimiento de los titulares de los datos personales, así como 2 UIT por obstruir el ejercicio de los derechos del titular de los datos personales. Además, se establece una multa de 0.5 UIT por no inscribir en el RNPDP.
1944-2021-JUS/DGTAIPD-DPDP	POLICLÍNICO LASER LOS NARANJOS E.I.R.L.	Hechos No informar al titular de los datos personales de cómo estos serán tratados. No inscripción de banco de datos en el RNPDP.
		Motivación La DPDP destaca la importancia del art. 18 para garantizar el derecho de autodeterminación informativa de los individuos. La empresa trató datos personales sin informar adecuadamente a los titulares, lo cual constituye una infracción grave. Aunque la empresa alega haber realizado modificaciones para cumplir con la normativa, la DPDP determina que aún persisten deficiencias en la información proporcionada a los titulares, lo que resulta en una responsabilidad por parte de la empresa. Obligación de inscribir los bancos de datos personales en la RNPDP, según lo establecido en el artículo 34 de la LPDP y el artículo 78 del RLPDP. La empresa argumenta que no era necesario inscribir el banco de datos porque no tenía proveedores directos, pero la DPDP determina que esta acción era obligatoria, aunque exonera a la empresa de responsabilidad en este aspecto debido a la naturaleza de los datos recopilados.
		Decisión Sancionar a Policlínico Los Naranjos E.I.R.L respecto a la infracción del art 132°, numeral 2, literal a) del RLPDP.
		Sanción impuesta Se establece una multa de 5.63 UIT por obstruir el ejercicio de los derechos del titular de datos personales.

418-2021-JUS/DGTAIPD-DPDP	ESPECIALIDADES MÉDICAS UNIVERSAL S.A.	Hechos No informar al titular de los datos personales de cómo estos serán tratados. Motivación La DPDP determina que la empresa no proporciona a los titulares de datos personales la información completa requerida por la ley. Se evidencia que la administrada trata los datos personales sin informar adecuadamente a los titulares sobre el tratamiento de su información, lo cual constituye una infracción grave según el reglamento de la LPDP. La DPDP destaca la importancia de informar de manera clara y accesible a los titulares sobre el tratamiento de sus datos, así como la necesidad de ajustarse a los requisitos establecidos en la normativa. Se constata que la administrada no cumplió con subsanar por completo las deficiencias señaladas por la DFI, lo que refuerza la conclusión de la DPDP sobre el incumplimiento de la empresa. Se destaca también que el sitio web de la administrada carece de información esencial sobre el tratamiento de datos, lo cual agrava la situación. La DPDP concluye que la administrada debe modificar sus políticas de privacidad para cumplir con lo establecido en el artículo 18 de la LPDP y asumir la responsabilidad correspondiente por el tratamiento inadecuado de los datos personales a través de su sitio web. Decisión: Infundada en parte a Especialidades Médicas Universales S.A. respecto a la infracción del art 18° de la LPDP. Fundada al haber incumplido con lo dispuesto en el art 18° de la LPDP, incurriendo en una infracción grave. Sanción impuesta: Se impone una multa de 12 UIT por obstruir el ejercicio de los derechos del titular de los datos personales.
1981-2020-JUS/DGTAIPD-DPDP	CENTRO MÉDICO CLÍNICA SAN JUDAS TADEO S.A.	Hechos No informar al titular de los datos personales de cómo estos serán tratados. No presenta medidas de seguridad apropiadas para el tratamiento de datos personales que incluyen datos sensibles. Motivación **1° Hecho infractor:** Se analiza el incumplimiento del deber de informar a los titulares de datos personales según lo establecido en el artículo 18 de la LPDP. La entidad en cuestión fue objeto de tres actas de fiscalización, en las cuales se constató que realizaba tratamiento de datos personales de sus pacientes sin proporcionar la información requerida por la ley. Además, se encontró que la entidad tenía un sistema de videovigilancia y ordenaba las historias clínicas sin informar adecuadamente a los titulares. Como resultado, se determinó que la entidad vulneraba el derecho de información de los titulares, constituyendo una infracción grave según la normativa. En este caso, se examina la falta de evidencia específica por parte de una entidad en relación con el tratamiento de datos personales en un sistema cliente/servidor. A pesar de presentar descargos y documentos relacionados, no se demostró claramente cómo se llevaba a cabo el tratamiento de datos en este sistema. La autoridad de fiscalización concluyó que no se acreditaba adecuadamente el cumplimiento de las normas de informar a los titulares de datos, y, por lo tanto, se declaró infundada la acusación en este aspecto. **2° Hecho infractor:** falta de implementación de medidas de seguridad en el tratamiento de datos, específicamente en la gestión de privilegios de acceso al sistema y en la generación de registros de interacción con el mismo. Tras evaluar los

		descargos y pruebas presentadas, se determinó que la entidad no cumplía totalmente con estas medidas, siendo responsable de la infracción. Decisión Eximir a Centro médico San Judas Tadeo S.A. respecto a la imputación del tratamiento de las cámaras de video vigilancia. Sancionar a la administrada por infringir los dispuesto en el art 18 de la LPDP. Asimismo, sancionar a la administrada por no cumplir con las medidas de seguridad.	Sanción impuesta Se establece una multa de 5.01 UIT por obstruir el ejercicio de los derechos del titular de los datos personales. Además, se impone una multa de 1.5 UIT por no proporcionar medidas de seguridad para el tratamiento de datos personales sensibles.
313-2021-JUS/DGTAIPD-DPDP	OPTICAS GMO PERU S.A.C.	Hechos No informar al titular de los datos personales de cómo estos serán tratados. Motivación La DPDP examina que la administrada no informaba adecuadamente a los titulares de datos personales sobre el tratamiento de su información, como lo requiere el art. 18 de dicha ley. La entidad tenía un formulario en su página web sin políticas de privacidad claras; aunque ofrecía un enlace a una página, esta no cumplía con los requisitos legales. La DPDP concluyó que basta con acreditarse la conducta típica de la infracción sin demostrarse si hubo culpa o dolo en el accionar. En ese sentido, la DPDP, de revisado el sitio web de la administrada, constata que esta cuenta con un enlace que deriva a su política de privacidad, pero se advierten dos de estas que rigen en fechas distintas, y la redacción sobre la conservación de la información era la misma, no discutiéndose esto, sino el cumplimiento del art. 18 de la LPDP, entendiéndose que la conservación se daba por el tiempo de atención a la solicitud. Decisión Infundada la imputación hacia Ópticas GMO Perú S.A.C.	Sanción impuesta No se impuso una sanción.

Nota. Elaboración propia.

Tabla 8

Tabla de criterios aplicados a las resoluciones

CRITERIOS	**C1**	**C2**	**C3**	**C4**	**C5**	**C6**
	Consentimiento del titular de los datos personales	Deber de informar sobre el tratamiento de datos personales/sensibles	Deber confidencialidad sobre los datos personales	Cumplir con registrar el banco de datos ante la RNPDP	Comunicar el uso del flujo transfronterizo a la DGTAIPD	Cumplir con las medidas de seguridad para el tratamiento de datos personales/sensibles
REGULACIÓN	Art. 13 inc. 5 de la LPDP	Art. 18 de la LPDP	Art. 17 de la LPDP	Art. 78 de la LPDP	Art. 26 del RLPDP	Art. 39 del RLPDP

Tabla 9

Aplicación de los criterios en los 17 casos analizados en la investigación

RESOLUCIÓN	ADMINISTRADA	CRITERIOS	ATENUANTE/ EXIMENTE/ NO OBJETO DE SANCIÓN (NOS)	TIPO DE INFRACCIÓN	RESPONSABLE	SANCIÓN/ MEDIDA CORRECTIVA
RD N° 1885-2020-JUS/DGTAIPD-DPDP	ONCOLOGÍA S.A.C	C1: Afectación del consentimiento del titular al solicitarle la aceptación total sobre las finalidades de la relación contractual que se buscaba establecer.	A: se consideró la enmienda del hecho infractor antes del PAS	Leve	Sí	5,01 UIT
		C2: La administrada mediante su descargo demuestra que brinda la información de tratamiento requerido	E: se demuestra que el accionar de cumplimiento se da antes del PAS	Grave	No	-
RD N° 1436-2021-JUS/DGTAIPD-DPDP	Clínica San Pablo S.A.C	C3: La administrada compartió información mediante un correo electrónico a otra entidad. La DPDP sanciona la acción realizada.	-	Grave	Sí	18,00 UIT
RD N° 1045-2020-	Servicios de Salud Montefiori S.A.C	C1: No basta que la DFI constate que la administrada difundía imágenes a través de su página web, ya que debió requerir el sustento respecto al consentimiento, no realizándolo.	NOS			

JUS/DGTAIPD -DPDP		C2: - Se advierte la responsabilidad de la administrada al no informar la transferencia internacional (EE.UU.). - La recopilación automatizada de las historias clínicas se realiza mediante Excel, el cual restringe al personal del área de archivo. - La administrada recopila información a través de un sistema utilizado por los ejecutivos del área de Admisión, los cuales solicitaban información personal de forma verbal y directa al titular sin contar con formato idóneo. - El sistema gestión y LOLCLI9000++ comparte la misma base de datos, siendo que el primero se alimenta del segundo. - La DFI no motiva su imputación, sustrayéndose el análisis de ilicitud. - La historia clínica es una reproducción de lo recopilado del sistema LOLCLI9000++.	- A: acción de enmienda - NOS - - - NOS - NOS - NOS	-	-	Medida correctiva
		C4: La DFI en el informe final recomienda que se archive dicho extremo.				
		C5: La administrada expide una solicitud para la inscripción para su uso de flujo transfronterizo, pero es observada y no realiza las subsanaciones debidas.	-	Leve	Sí	1,5 UIT
		C6: - Se advierte que la administrada cumple con gestionar los privilegios y verificaciones de estos, así como los cierres de sesión de los usuarios con posterioridad y antes del informe técnico. - La administrada no contaba con un ambiente idóneo para su centro de datos, sin embargo, lo implementó. - La DFI no cumple con acreditar que las historias clínicas estén expuestas al público en general o que no haya una restricción debida, contrarrestándose en la fase de instrucción - La DFI no evidencia la reproducción documentos de datos personales/sensibles que desprende las historias clínicas	- - - - - - - Archivar	Grave	Sí	6,5 UIT
RD N° 1459-2020-JUS/DGTAIPD -DPDP	Clínica Mundo Salud S.A.C	El despacho considera como requisito esencial para que se dé una reconsideración el tener prueba nueva o nuevo hecho del cual se desconocía su existencia o había una imposibilidad de obtenerlo, lo cual no cumple en acreditar la administrada en su escrito. Se declaró improcedente el recurso de reconsideración.				

RD N° 3454-2021-JUS/DGTAIPD-DPDP	Seguro Social de Salud- ESSALUD	La DPDP analiza la importancia de los derechos ARCO y cómo los titulares de los datos personales pueden ejercerlos; sin embargo, advierten que el administrado solicita que se le brinden información no conexa a la finalidad de la LPDP y su RLPDP. En consecuencia, se deberá atender como un derecho de petición, mas no de acceso. Se declaró improcedente la solicitud.				
RD N° 3292-2019-JUS/DGTAIPD-DPDP	Clínica del Pacífico S.A.	C2: La administrada omite el texto informativo en sus formularios físicos, no nombra a la compañía de seguros que trata la información y usa tres formularios juntos, debiéndose incluir todo el texto informativo en estos.	- -	Grave	Sí	6,5 UIT
		C4: El despacho determina que la administrada, en un intento de resarcir la omisión de la inscripción del banco de datos, solo lo realiza parcialmente.	- -	Leve	Sí	1,5 UIT
		C6: - La administrada no cumple con documentar la periodicidad de la revisión de perfiles. - La administrada no genera ni mantiene los registros de interacción lógica con la información de los pacientes. - Se da por acreditado que la administrada no asigna un personal responsable para la custodia de las historias clínicas, pero se prueba lo contrario.	- - - - A: en su descargo acredita la asignación de personal responsable, la llave y cerradura.	Grave	Sí	8 UIT
RD N° 1049-2020-JUS/DGTAIPD-DPDP	Clínica Santa Martha del Sur S.A.C	C1: La DFI examina un sitio web incorrecto por el cual imputa el hecho infractor.	NOS		Sí	5,1 UIT
		C2: 1° medio: - La administrada presenta formularios físicos que no informan sobre el tratamiento de datos personales, debiéndose actualizar el código de banco de datos que tiene. - La DFI no señala de forma expresa el hecho infractor. 2° medio: - La DFI brinda el link de una página web deshabilitada, archivándose este extremo.	1° medio: - - - NOS 2° medio: - NOS	Grave	Sí	Mediada correctiva
		C4: La DPDP indica que el cambio de denominación social y nombre no es relevante para inscribir o modificar el banco de datos ante la RNPDP.	E: no es una infracción.	Leve	Sí	-

RD N° 1180-2020-JUS/DGTAIPD-DPDP	Centro Médico Ohi S.A.C	C1: La DFI no sustenta sobre el consentimiento de las imágenes que aparecen en la página web de la administrada.	NOS	Grave	Sí	6 UIT
		C2: El despacho señala que es necesario especificar a detalle cada condición de tratamiento de los datos personales y la administrada cesa la recopilación de esta.	- -	Grave	Sí	1 UIT
		C4: La administrada primero no logra desvirtuar su no inscripción de su banco de datos ante la RNPDP, pero cesa con la recopilación de información, después ratifica esto.	E: rectifica la infracción después de la resolución de imputación de cargos.	Leve	Sí	0,5 UIT
		C5: La administrada cesa el tratamiento de los datos personales después de notificado el PAS.	A: cese del hecho infractor.	Leve		
RD N° 1580-2020-JUS/DGTAIPD-DPDP	Clínica La Luz S.A.C	C2: - La administrada recopilaba información a través de sus historias clínicas, las cuales contienen datos sensibles, lo cual debió informar desde un inicio. - La administrada debió materializar la información. - La administrada no informa el tiempo de conservación de los datos y demás pertinente, lo cual no acredita con medio alguno que se esté implementando. - La DPDP sustenta la omisión de comunicar a los titulares que eran grabados a falta de la directiva en su momento	- -	Grave	Sí	10 UIT
		C4: La administrada omite registrar en la RNPDP su banco de datos de proveedores, lo cual subsana posteriormente.	A: Por acción de enmienda	Leve	Sí	0.5 UIT
		C5: La administrada no informó sobre el uso de flujo transfronterizo.	- -	Leve	Sí	1 UIT

		C6: - La administrada no sustenta la verificación de privilegios. - La administrada no genera el registro de interacción lógica con los bancos de datos. - La administra no presenta el ambiente adecuado para el tratamiento de datos.	- - - - - A: Presentación de documentación que acredita el ambiente idóneo	Leve	Sí	10 UIT
RD N° 3039-2021-JUS/DGTAIPD-DPDP	Genetics S.A.C	C2: La administrada no informa sobre el ejercicio de los derechos ARCO y el tratamiento de datos.	- -	Grave	Sí	9,86 UIT
		C6: - La administrada no acredita que contaba con medidas de seguridad. - La administrada no registra la interacción de los usuarios. - La administrada no cumple con la implementación de medidas de seguridad respecto al manejo de datos de personales. - La administrada no presenta la cerradura y llave del lugar. - La DFI no acredita que la administrada no posee el usuario y la contraseña del banco de datos.	C6: - - Presentación de documentación que acredita el ambiente idóneo - - NOS	Leve		1 UIT
RD N° 2077-2020-JUS/DGTAIPD-DPDP	Hospital de Emergencias José Casimiro Ulloa	C6: - La administrada se encuentra elaborando la documentación de los procedimientos de acceso y gestión; la DPDP no lo consideró como una enmienda. - La administrada admite que faltan controles de acceso para los sistemas “RIS” y “PACS”.	- -	Leve	Sí	Medida correctiva
		C3: La administración fue evidenciada por una filtración de fotografías y tomografías del estado del paciente, lo que demostró que no tenía mecanismos que aseguren la confidencialidad de los datos personales/sensibles; además, no tomó medidas para evitar futuras infracciones.	- -	Grave	Sí	25 UIT

RD N° 515-2019-JUS/DGTAIPD-DPDP	Clínica Médica Cayetano Heredia S.A.	C2: La administrada en su página web no brinda la información consignada en el art 18; sin embargo, presenta un descargo alegando que se corrigieron las observaciones.	A: Por acción de enmienda.	Leve	Sí	2 UIT
		C1: La administrada no presentaba las opciones de aceptar o rechazar los términos y condiciones de su página web.	A: Por colocar las opciones en la página web.	Leve	Sí	1,5 UIT
		C6: - La administrada no define procedimientos de gestión de privilegios y acceso de usuarios al sistema, así como su revisión y verificación. - La administrada no mantiene registros de las cuentas de los usuarios, trazabilidad y acciones significativas.	A: Se presenta la documentación que acredita que sí se cuenta con los medios de seguridad.	Grave	Sí	4,5 UIT
RD N° 1529-2020-JUS/DGTAIPD-DPDP	Clínica Morillas S.A	C1: La administrada realiza uso de imágenes de artistas sin su debido consentimiento; además, en el formulario para el uso de imagen no se estipula la opción de rechazo o aceptación del tratamiento de datos.	A: realización de acciones de subsanación.	Grave	Sí	2UIT
		C2: la administrada, mediante sus formularios físicos y el soporte no automatizado, no brinda la información necesaria para el tratamiento de datos personales.	A: incorporación de consentimiento informado y políticas de privacidad.	Grave	Sí	2UIT
		C5: La administrada alega que presentó su inscripción al RNPDP, pero no pudo realizar la corrección de observaciones; la DPDP alega que la administrada no presentó algo que justifique la negativa de corrección de las subsanaciones.	A: subsanación de observaciones antes de la resolución final.	Leve	Sí	0,5 UIT
		C6: La administrada presenta documentos que acreditan el cumplimiento de los medios de seguridad de los datos personales.	NOS	Grave	No	Infundado
RD N° 1944-2021-	Policlínico Los Naranjos E.I.R.L	C2: La administrada no informa sobre la existencia de banco de datos, la finalidad del tratamiento de datos y el plazo de conservación de datos.	-	Grave	Sí	5,63 UIT

JUS/DGTAIPD -DPDP		C6: La administrada no realiza la inscripción en el RNPDP porque no tiene un proveedor directo.	E: Por no tener proveedores directos.	Leve	No	-
RD N° 418-2021-JUS/DGTAIPD -DPDP	Especialidades Médicas Universales S.A	C2: La administrada no otorga información relevante sobre el tratamiento de datos que se recaba a través de su sitio web.	-	Grave	Sí	12 UIT
RD N° 313-2021-JUS/DGTAIPD -DPDP	Clínica San Judas Tadeo S.A.	C2: - La administrada no presentó evidencia adecuada sobre cómo se realiza y cómo se informa el tratamiento de datos. - La administrada no presenta una correcta política de privacidad; además, no informa sobre la transferencia de datos a nivel internacional y nacional. - La administrada no brindó información sobre los datos recopilados por las cámaras de video vigilancia.	- NOS - - E: La administrativa.	Grave	No	5,01 UIT
		C6: - La administrada no presenta documentos que acrediten la realización de gestión de privilegios y accesos. - La administrada no posee un control de acceso que se genere con la propia interacción de usuario con el sistema, para el almacenamiento de datos.	- - - -	Leve	No	1,5 UIT
RD N° 1981-2020-JUS/DGTAIPD -DPDP	Ópticas GMO Perú S.A.C.	C2: La administrada no brinda información con respecto al tiempo de almacenamiento, y no entrega información en su página web	E: La DPDP determina que la administrada sí entrega información exigida por la LPDP	Leve	No	Infundado

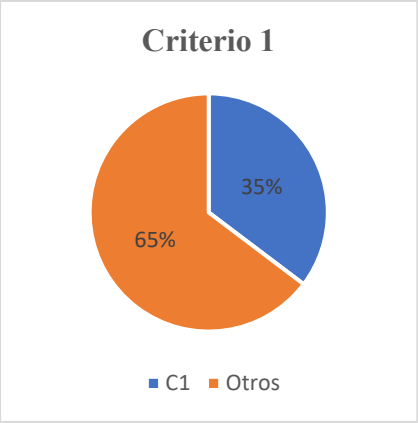
Nota. Elaboración propia.

De la tabla 4, se desprenden los siguientes datos:

En un 35 % (6) de los casos se ha podido advertir una afectación al consentimiento del usuario, siendo una obligación de la administrada solicitarlo, vulnerándose la autonomía de decisión que los usuarios tienen con su información (datos personales).

Figura 9

Criterio 1

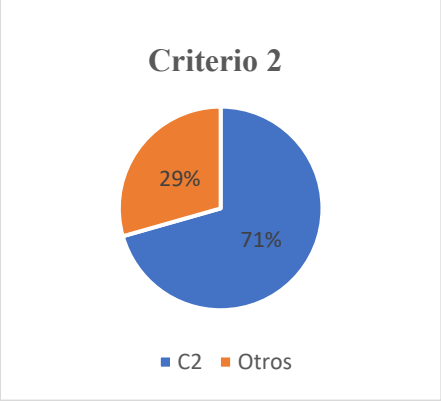


Nota. Elaboración propia.

En el 71 % (12) de los casos se vislumbra que los administrados (entidades) omiten informar al titular de datos personales respecto al tratamiento que brindarán a estos, debiéndose realizar dicho deber antes de que los titulares expongan sus datos personales/sensibles. Además, no informan puntos esenciales previstos por la ley.

Figura 10

Criterio 2

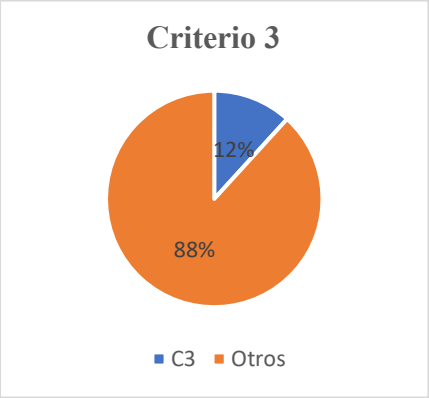


Nota. Elaboración propia.

El 12 % (2) de los casos hace notar que los administrados (entidades) comparten información sensible otorgada por los usuarios sin que estos hayan brindado su consentimiento para dicha exposición, transgrediendo su intimidad y afectándose la relación de confidencialidad entre usuario y entidad.

Figura 11

Criterio 3

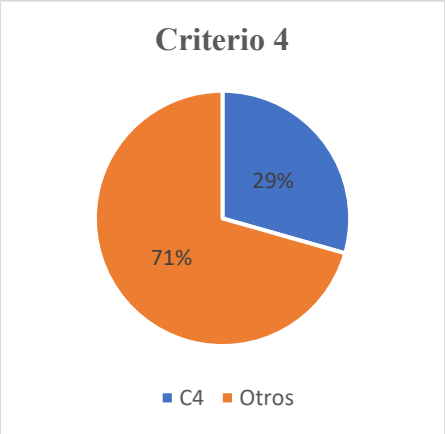


Nota. Elaboración propia.

En ll 29 % (5) de los casos se determina la poca importancia que le brinda la administrada a la inscripción de sus bancos de datos ante la RNPDP, ya que es la encargada de supervisar la administración y actualización. Además, resuelve cualquier tipo de incidencia que postulen los titulares de la información o cuando ejerciten sus derechos ARCO, así como toda atribución correspondiente.

Figura 12

Criterio 4

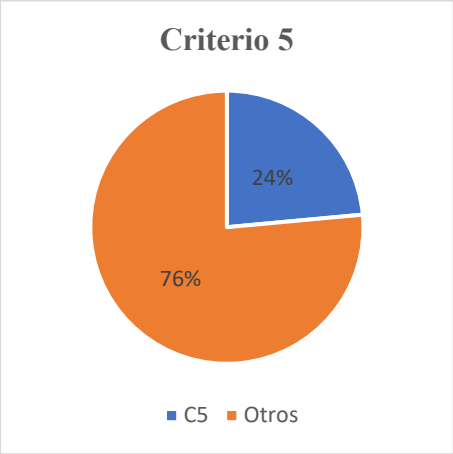


Nota. Elaboración propia.

El 24 % (4) de los casos denota la no comunicación del flujo transfronterizo a la DGTAIPD, siendo de importancia porque la administrada puede solicitar su opinión para ver si realiza o cumple con lo regulado en la LPDP y su RLPDP; asimismo, es obligación de la administrada brindar información con respecto a la transferencia de datos personales y el registro del banco de datos.

Figura 13

Criterio 5

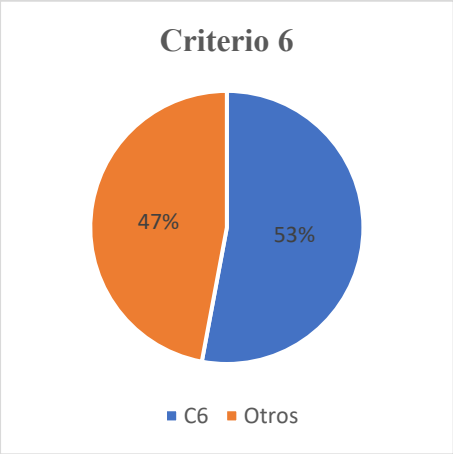


Nota. Elaboración propia.

En el 53 % (9) de los casos se demuestra la importancia de implementar, mantener y resguardar el banco de datos en el cual se almacena información personal y/o sensible de los usuarios que pertenecen a los establecimientos de salud y servicios médicos de apoyo de los administrados.

Figura 14

Criterio 6

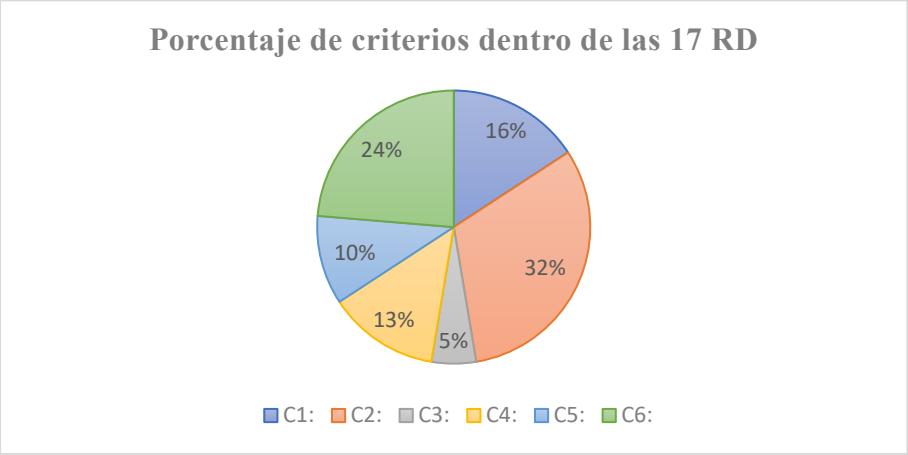


Nota. Elaboración propia.

La DPDP considera criterios claves al emitir las RD. El primer criterio más analizado fue sí las administradas informaban a los titulares de los datos personales respecto al tratamiento que brindarían a estos (C2); en segundo lugar, la omisión por parte de los administrados al implementar medidas de seguridad respecto al tratamiento de datos (C6); en tercer lugar, la no comunicación del uso del flujo transfronterizo ante la DGTAIPD (C5); en cuarto lugar, la negligencia respecto a la inscripción idónea de los bancos de datos de las administradas (C4); en quinto lugar, la omisión de solicitar el consentimiento de los titulares respecto a sus datos personales y sensibles que las administradas expusieron (C1); finalmente, si se respetó la confidencialidad de las entidades con sus usuarios.

Figura 15

Porcentaje de criterios dentro de las 17 RD



Nota. Elaboración propia.

5.1. La Propuesta de Adición

Sobre la base de los datos previamente expuestos y en el desarrollo de este documento, se considera fundamental la realización de una modificación legislativa en la regulación de las funciones de la ANPD. Esta medida se justifica en el principio preventivo, el cual tiene como objetivo la previsión de medidas idóneas para evitar futuras obstaculizaciones. En este sentido, se busca establecer un marco regulatorio respecto a la previa fiscalización de la inscripción del banco de datos vinculados a los servicios de salud, en los cuales se almacenan datos personales y sensibles. El propósito primordial es proteger desde el inicio contra cualquier afectación que pueda surgir debido a la incorrecta inscripción de los bancos de datos y la falta de verificación de los requisitos que deben cumplir los establecimientos de salud y los servicios médicos de apoyo para el almacenamiento de datos personales o sensibles y la recopilación de información de los usuarios.

Tabla 10

Propuesta legislativa de adición de la regulación de una función específica de la ANPD

Texto actual	Texto propuesto
Artículo 33. Funciones de la ANPD 20. Iniciar fiscalizaciones de oficio o por denuncia de parte de presuntos actos contrarios a lo establecido en la presente ley y en su reglamento, y aplicar las sanciones administrativas correspondientes, sin perjuicio de las medidas cautelares o correctivas que establezca el reglamento.	Artículo 33. Funciones de la ANPD 20. Iniciar fiscalizaciones de oficio o por denuncia de parte de presuntos actos contrarios a lo establecido en la presente ley y en su reglamento, y aplicar las sanciones administrativas correspondientes, sin perjuicio de las medidas cautelares o correctivas que establezca el reglamento. 20-A: Fiscalización *ex ante* de los bancos de datos que son utilizados por las entidades de salud y servicios médicos de apoyo, siendo el último paso para emitirse la resolución directoral correspondiente.

Nota. Elaboración propia.

5.2. Exposición de Motivos

El 3 de julio del 2011, el Gobierno público, en el Diario Oficial el Peruano, la LPDP, y el 22 de marzo del 2013 se aprobó mediante Decreto Supremo N.º 003-2013-JUS el Reglamento de la LPDP. De esta manera, esta nueva ley busca garantizar el derecho fundamental de la protección de datos personales, el cual se encuentra previsto en el art. 2, inciso 6 de la Constitución Política del Perú, siempre en el marco de respeto con los demás derechos fundamentales.

El objetivo de este proyecto es adicionar un literal al inciso 20 del artículo 33 de la LPDP sobre la fiscalización, para lo cual la ANPD se enfocará en realizar una fiscalización *ex ante* a las entidades de salud que registren sus bancos de datos ante la RNPDP.

De esta manera, el Estado tiene la obligación de brindar protección a los derechos fundamentales que se puedan ver vulnerados dentro de su territorio, como lo son la intimidad, privacidad y la autonomía informativa, a razón de garantizar un resguardo a los datos

personales/sensibles de los titulares que brindan su información para ser registrada en los bancos de datos que utilicen las entidades de salud.

5.3. Diagnóstico del Inciso 20 del Art. 33 Denominado Funciones de la ANPD de la LPDP

La ANPD basa actualmente sus funciones a razón del art. 33 de la LPDP, designando la facultad de fiscalizar el banco de datos de las entidades que realizan su registro, teniéndose como directriz el principio de veracidad; sin embargo, se puede apreciar falencias que inciden en la vulneración de los datos personales/sensibles de sus titulares, los cuales inician procesos administrativos que terminan imponiendo sanciones administrativas.

En efecto, es de suma importancia solucionar un problema que no ha sido abordado; por ello es trascendental establecer una adición al art. 33, inciso 20 de la LPDP, de conexión con el principio de prevención, a fin de disminuir los procesos donde se vulneren los datos personales por parte de los establecimientos de salud y servicios médicos de apoyo, a razón del indebido cumplimiento de los requisitos que requiere la LPDP en los bancos de datos.

5.4. Principal Falencia Sobre la Protección de Datos Personales en el Ámbito de la Salud

Actualmente, según el inciso 20 del artículo 33 de la LPDP, se otorga facultad a la ANPD para iniciar fiscalizaciones de oficio o en respuesta a denuncias relacionadas con actos contrarios a lo establecido en la LPDP. Un análisis de 17 resoluciones emitidas por la ANPD y publicadas en su portal web oficial, revela que el 29 % de estas resoluciones evidencian inscripciones inadecuadas en el RNPDP, mientras que el 53 % señala la falta de adecuada implementación de medidas de seguridad en los bancos de datos de las entidades de salud durante los años 2020 y 2021. Estas cifras ponen de manifiesto la insuficiente protección estatal en el ámbito de la salud en lo que respecta a datos personales y sensibles.

Es importante destacar que la ANPD realiza fiscalizaciones *ex post*, es decir, después de que se ha vulnerado la protección de datos personales y sensibles, y después de que se han afectado los derechos fundamentales de intimidad, privacidad y autonomía informativa.

5.5. Alternativas

5.5.1. Propuesta de Adición al Inciso 20 del Art. 33 de la LPDP

La fiscalización *ex ante* que se propone es para poder prevenir las posibles vulneraciones a la protección de datos personales y sensibles que se pueden dar a través de los bancos de datos, puesto que el formulario que se solicita para el respectivo registro tiene calidad de declaración jurada y esto se refleja en cada paso para el registro; en consecuencia, se hace más énfasis en el principio de veracidad que tienen los administrados. De esta manera, mediante una fiscalización posterior buscan sancionar, pero para este momento se vulneró la protección y ya se afectó un derecho fundamental: el de la intimidad y privacidad.

En esa línea de análisis, es mejor realizar una fiscalización *ex ante* para poder proteger los datos personales y, de esta manera, evitar la vulneración de un derecho fundamental.

5.5.2 Crear un Manual Señalando los Requisitos que Exige la RNPDP al Momento que el Administrado va a Inscribir el Banco de Datos

Como alternativa adicional, se podría elaborar un manual que explique los requisitos para un debido registro del banco de datos de las entidades que exige la RNPDP destinado a orientar a los administrados en el proceso de inscripción en los bancos de datos de las entidades de servicios de salud. Este manual proporciona el paso a paso, incluyendo pautas para garantizar un entorno adecuado para el resguardo de los datos, así como indicaciones sobre la forma correcta de presentar una inscripción, con el fin de evitar posibles repercusiones. De esta manera, se informará a las entidades de salud previniendo cualquier posible vulneración de la privacidad. Aunque esta medida carecería de carácter legal obligatorio, se puede advertir que su incumplimiento sería una inobservancia por parte de la entidad de estar informado sobre su deber, lo cual podría ser valorado por la DPDP para constituirse como una infracción grave. Sin embargo, esto solo sería relevante tras una fiscalización por parte de la ANPD al administrado, lo que llevaría nuevamente al mismo problema. En este sentido, una vez que se

haya vulnerado el derecho fundamental a la intimidad y privacidad, y luego de una exhaustiva fiscalización por parte de la DFI, se estaría sancionando al propio administrado.

5.6. Análisis Costo-Beneficio

Propuesta de adición: la aplicación de la propuesta que se pretende establecer en el inciso 20 del art. 33 de la LPDP no generará un gasto adicional porque se realizará una fiscalización *ex ante* del registro de los bancos de datos de los establecimientos de salud y servicios médicos de apoyo. El beneficio no será cuantificable, ya que se trata de derechos fundamentales.

La aprobación de esta iniciativa generará una mejor protección de los derechos fundamentales de la intimidad y privacidad, este último unido a la autodeterminación informativa, ya que la vulneración de los datos personales y sensibles disminuirá a razón de la fiscalización *ex ante* que se realizará. En consecuencia, su utilidad se fundamenta en la prevención de la trasgresión que sufren las personas al otorgar sus datos requeridos para su atención médica, los mismos que se almacenan en los bancos de datos que se utilizan en las entidades de salud.

Propuesta de manual: este manual guiaría a los administrados que busquen registrar sus bancos de datos ante la RNPDP para que cumplan lo requerido por ley (requisitos), con ello se busca que los administrados, por voluntad propia, se informen y den cumplimiento a lo desarrollado en este manual, para así prevenir vulneraciones de los datos personales y sensibles.

La implementación del manual conllevaría un aumento en los costos, dado que la ANPD debería destinar un presupuesto para su elaboración y difusión entre todas las instituciones de salud pertinentes. Sin embargo, el beneficio no es cuantificable, ya que se trata de derechos fundamentales. Con respecto al costo de creación, se tomará en cuenta el costo de producción.

5.7. Propuesta de Establecer un Numeral Dentro de las Funciones de la ANPD

Con base en lo expuesto, se considera la necesidad de establecer un nuevo literal al numeral 20 del art. 33 denominado funciones de la ANPD, el cual estará en armonía con los demás cuerpos legales, para no alterar o vulnerar algún derecho, esto en referencia a la fiscalización *ex ante* que se busca que realicen a los bancos de datos que cada entidad de salud busca registrar. Por tanto, el texto a establecer sería:

Art. 33: Funciones de la ANPD:

20: "Iniciar fiscalizaciones de oficio (…) correctivas que establezca el reglamento".

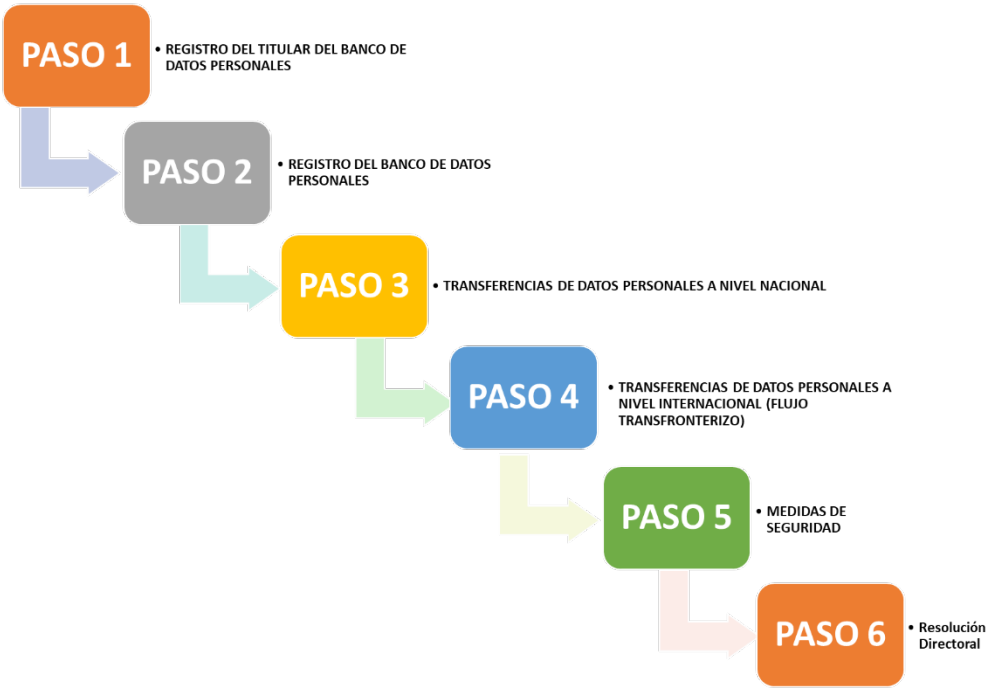
20-A: Fiscalización *ex ante* de los bancos de datos que son utilizados por las entidades de salud y servicios médicos de apoyo, siendo el último paso para emitir la resolución directoral correspondiente.

A continuación, se grafican los pasos que brinda la ANPD para el registro del formulario para los bancos de datos y el paso de fiscalización *ex ante* que nosotros buscamos agregar.

Pasos para la inscripción en el RNPDP

Figura 16

Pasos para la inscripción en el RNPDP

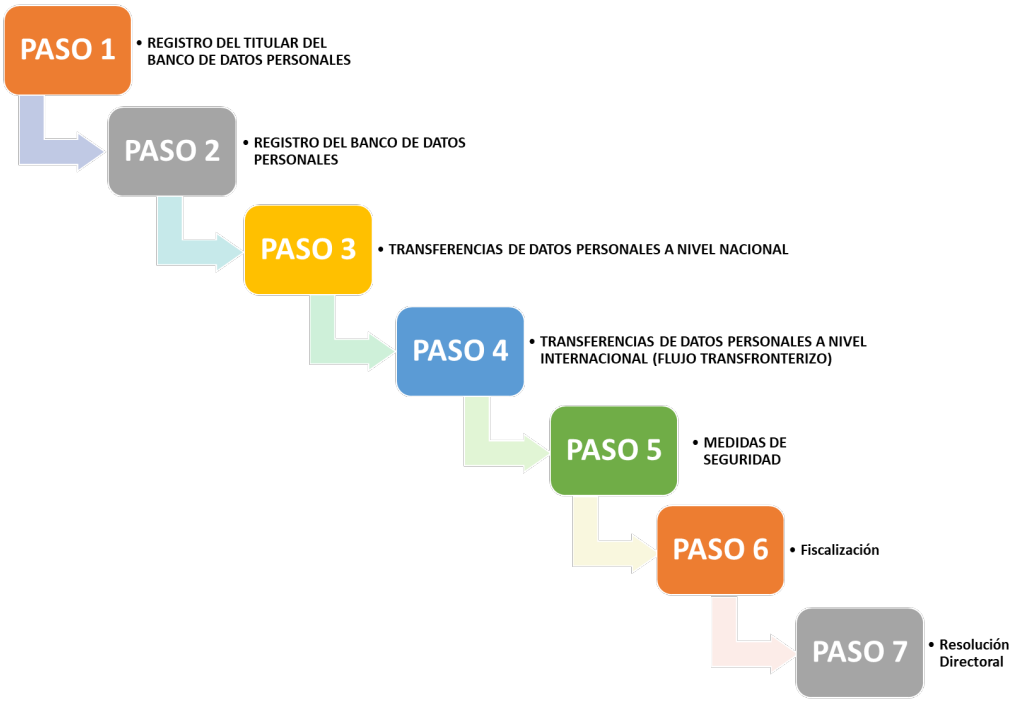


Nota. Elaboración propia.

Propuesta de la fiscalización *ex ante*

Figura 17

Propuesta de la fiscalización ex ante



Nota. Elaboración propia.

Lo que busca establecer la propuesta se enfoca en responder las siguientes preguntas: ¿El registro de banco de datos pertenece a alguna institución que brinde servicio de salud? ¿No registrar el banco de datos adecuadamente cómo afecta a las personas que brindan sus datos? ¿Qué efecto genera la fiscalización *ex ante* en los bancos de datos en los servicios de salud?

En esa línea, las preguntas se generan considerando que la ANPD tiene como objetivo proteger los datos personales y, más aún, los datos sensibles. Desde esta óptica, mediante este mecanismo se podrá regular de mejor manera el adecuado registro de los datos personales y sensibles en las instituciones que brinden servicios de salud. En consecuencia, el objetivo es amortiguar, reducir y, en el mejor de los casos, erradicar la vulneración posterior de los datos personales y sensibles que ocurre en el ámbito del servicio de salud.

Vale precisar que el artículo propuesto se debe establecer en la LPDP para una correcta y objetiva regulación sobre la fiscalización de los bancos de datos en el ámbito de la salud, con el fin de tener un mejor control, puesto que las normas deben buscar brindar y mejorar la protección que se otorga, más aún al tratarse de los datos sensibles que son tratados dentro de este ámbito de la salud.

5.8. Efecto de la Adición en el Inciso 20 del Art. 33 de la LPDP

La aprobación de la presente propuesta supone modificar y, mediante ello, establecer un mecanismo específico que pueda ayudar a mejorar el control y protección de los bancos de datos utilizados por las entidades de salud, para que, de ese modo, se prevenga la vulneración de los datos personales/sensibles ante una fiscalización *ex post* por la ANPD, lo cual termina vulnerando el derecho fundamental a la intimidad, privacidad y autodeterminación informativa, así como los pertinentes que se relacionen a estos derechos.

Esta adición entrará en vigor al día siguiente de su publicación en el Diario Oficial El Peruano, entendiéndose que se está estableciendo un nuevo mecanismo para un caso particular.

5.9. Sobre las Fortalezas y Debilidades del Estudio

5.9.1. Fortalezas

La presente investigación da a conocer con mayor detenimiento que, en el periodo 2020-2021, inmersos en una emergencia sanitaria a razón de la Covid-19, los datos personales brindados a los Establecimiento de Salud y Servicios Médicos de Apoyo han sido pasibles de vulneración, puesto que la ANPD realizó una fiscalización *ex post*.

Se dan a conocer dos procedimientos importantes, que son: el procedimiento trilateral y el PAS, a los cuales los administrados acceden cuando se vulnera su derecho a la privacidad al brindar sus datos a los Establecimientos de Salud y Servicios Médicos de Apoyo; así como las instituciones que se encuentran inmersas en estos procedimientos, como la ANPD, la DPDP, DGTAIPD y la DFI.

5.9.2. Debilidades

La ANPD no está descentralizada, lo cual conlleva a que, en provincia, se tenga mucha desinformación respecto a la protección de datos personales, redundando en el desconocimiento por parte de los administrados sobre el proceso administrativo y la función que realiza la ANPD.

Conclusiones

La DPDP considera varios criterios fundamentales al emitir sus RD. Estos criterios incluyen el consentimiento adecuado para el tratamiento de datos, la provisión de información clara sobre dicho tratamiento, la confidencialidad de los datos proporcionados por los usuarios, la correcta inscripción del banco de datos por parte de la entidad administrada, la comunicación del uso de flujo transfronterizo de datos, y la implementación de medidas de seguridad en el entorno donde se almacenan los datos. El objetivo principal de estos criterios es garantizar una protección más efectiva de la privacidad de los datos personales. La DPDP se basa en la LPDP y RLPDP, y evalúa el impacto de las acciones de los establecimientos de salud para determinar si se ha infringido alguno de estos criterios, lo que puede llevar a la imposición de sanciones.

Los hechos más comunes que vulneran los datos personales suelen estar relacionados con el incumplimiento de los administrados (entidades) de informar a los titulares respecto al tratamiento que se les dará a sus datos personales/sensibles o con la omisión de contar con medidas de seguridad en los lugares donde se resguardan los datos personales/sensibles que almacenan de manera automatiza o no automatizada estos servicios de salud. Estos incidentes se detectan a través de denuncias o reclamos presentados por los usuarios o por fiscalizaciones realizadas de manera interna por la ANPD.

En el proceso con la ANPD, las entidades siguen una estructura común en sus resoluciones. Comienzan con una fase inicial donde se establece la relación entre los informes presentados y la futura RD, asegurando que no se vulneren los derechos de defensa. Luego, se resumen de manera concisa los hechos infractores y se procede al análisis detallado de cada uno de ellos. Durante este análisis se evalúa cualquier explicación o descargo proporcionado por la entidad infractora para subsanar o justificar el incumplimiento. Esto permite determinar si corresponde aplicar una sanción, una medida correctiva o si se exime de la sanción. Las resoluciones administrativas muestran una delimitación de las cuestiones en discusión en

relación con el hecho sujeto de pronunciamiento. Estas resoluciones se caracterizan por su enfoque técnico orientado hacia la parte resolutiva, basando su motivación y desarrollo principalmente en aspectos normativos. Esto implica que la DPDP sustenta su motivación con informes emitidos por la DFI y se basa en la LPDP y RLPDP. Además, se utiliza la doctrina para brindar conceptos para sus explicaciones. Sin embargo, no se observa un análisis referente a jurisprudencia previa en casos similares. Es relevante destacar que la motivación se ve influenciada por aspectos resarcitorios, considerando eximentes y atenuantes en la graduación de la sanción a imponer. Es decir, la DPDP toma en cuenta acciones como la corrección de errores imputados como infracciones antes o después de la emisión del informe. Además, los descargos ofrecidos por la entidad fiscalizada también influyen en la decisión final asumida por la dirección.

Al determinarse las decisiones o fallos de las resoluciones emitidas por la DPDP, se menciona el hecho infractor vulnerado y la multa interpuesta a la entidad. Se mencionan las medidas correctivas interpuestas; asimismo, se menciona que se debe notificar a las partes. La ANPD determina el monto de las multas según el numeral 3 del art. 248 de la LPAG. Las multas son proporcionales a la gravedad de la infracción, considerando: beneficio ilícito, probabilidad de detección, daño al interés público, perjuicio económico, reincidencia, circunstancias de la infracción e intencionalidad. La Resolución Ministerial N.º 0326-2020-JUS aprobó la Metodología para el Cálculo de Multas, estableciendo pautas para calcularlas en casos de infracción a la protección de datos personales.

Nuestra propuesta se centra en reestructurar la legislación de las funciones de la ANPD en el ámbito de la salud, para evitar, en primera instancia, la afectación primordial al derecho a la intimidad. La propuesta de fiscalización "ex ante" busca prevenir este tipo de impacto en el derecho fundamental desde el inicio, sin descartar la posibilidad de realizar una fiscalización posterior. Esta nueva medida se presenta como un mecanismo adicional para un control más

efectivo y un resguardo más robusto de los datos personales y sensibles en los establecimientos de salud.

Recomendaciones

En primer lugar, es esencial que, como administrados, estén al tanto de sus derechos en relación con la protección de datos personales y sensibles. Familiarizarse con la normativa vigente, como la LPDP, les permitirá comprender mejor cómo se manejan sus datos y qué garantías tienen, además de prever el cumplimiento del art. 18 de la LPDP, puesto que la Dirección General de Datos Personales es lo primero que analiza para poder motivar y brindar su decisión final.

En segundo lugar, antes de compartir información con instituciones de salud, es recomendable que revisen detenidamente las políticas de privacidad que estas entidades ofrecen. Esto les proporcionará información clara sobre cómo se utilizarán sus datos, los fines de su tratamiento y el nivel de seguridad implementado para proteger su información.

En tercer lugar, dado que el proceso de fiscalización puede llevar tiempo, es importante que estén conscientes de las posibles vulneraciones a sus datos personales y sensibles durante este periodo. Estar informados les permitirá tomar precauciones adicionales si es necesario. Además, deben asegurarse de otorgar su consentimiento de manera clara y consciente cuando se soliciten sus datos personales y/o sensibles por parte de instituciones médicas. Es recomendable exigir que se les informe adecuadamente sobre cómo y con qué fines se utilizarán sus datos.

En cuarto lugar, es recomendable que la dirección genere precedentes vinculantes para ayudar a resolver de una manera más idónea y ser más eficiente, al objeto de que el proceso no sea muy extenso. Asimismo, se recomienda que en las resoluciones emitidas no solo se utilice la normatividad y las decisiones jurisprudenciales locales, sino los referentes internacionales que pueden coadyuvar a resolver dudas y controversias.

Finalmente, los administrados deben cerciorarse de las políticas de privacidad que cada entidad de salud les brinda, puesto que dentro de estas se informa el cómo, el por qué, el para qué y el fin que va a tener el tratamiento de datos personales.

Bibliografía

Beauchamp, T., & Childress, J. (2011). Bioética y Debat. *Tribuna Abierta del Institut Borja de Bioética*, *6.*

Castro, K. (2008). El derecho fundamental a la protección de datos personales: aportes para su desarrollo en el Perú. *IUS ET VERITAS*, 260-276.

Conde, C. (2005). *La Protección de Datos Personales.* Dykinson S.L.

Constitución Política Del Perú. (1993, noviembre 29). *Constitución Política Del Perú*.

Corral, H. F. (2000). Configuración Jurídica del derecho a la privacidad, I. origen, desarrollo y fundamentos. *Revista de Derecho Pontificia Universidad Católica de Valparaíso*, 1-29. https://dialnet.unirioja.es/servlet/articulo?codigo=2650211

Corte Suprema de Justicia de la República. (2006). Casación N.º 2799-2005. Vista de la Causa. Lima: 25 de setiembre de 2006. https://busquedas.elperuano.pe/cuadernillo/CA/20070105

Cuenya, L., & Ruetti, E. (2010). Controversias epistemológicas y metodológicas entre el paradigma cualitativo y cuantitativo en psicología. *Revista Colombiana de Psicología, 19*(2), 271-277. https://www.redalyc.org/pdf/804/80415435009.pdf

Curioso, W., & Espinoza, E. (2015). Marco conceptual para el fortalecimiento de los Sistemas de Información en Salud en el Perú. *Revista Peruana de Medicina Experimental y Salud Pública,* http://www.scielo.org.pe/scielo.php?pid=S1726-46342015000200019&script=sci_abstract

Defensoría del Pueblo. (2019). Manual de Protección de Datos Peronales. https://www.defensoria.gob.pe/wp-content/uploads/2019/11/Manual-de-Protecci%C3%B3n-de-Datos-Personales.pdf

Derecho de la dignidad humana y el libre desarrollo de la personalidad (Primera Sala del TC Federal Alemán 1983).

El derecho a la protección de datos de carácter personal, 292-2000 (Tribunal Constitucional Noviembre 30, 2000).

Fernández, C. (1997). Daño a la identidad personal. *THEMIS Revista de Derecho*, 245-272.

Franco, D. (2020). La protección de datos personales y el derecho al olvido en el Perú. A propósito de los estándares internacionales del Sistema Interamericano de los Derechos Humanos. *Derecho PUCP*, 271-299.

Gómez, H., Isla, S., & Mejía, G. (2010). Apuntes sobre la Graduación de Sanción por Infracciones a las Normas de Protección al Consumidor. *Derecho & Sociedad, 34*, 134-146.

Hernández, R. (2010). *Metodología de la Investigación.* Mc Graw Hill.

Iñiguez, L. (2008). El debate sobre metodología cualitativa versus cuantitativa. *Centro Universitario de Ciencias Sociales y Humanidades*, 1-5.

La Ley de Transparencia y Acceso a la Información Pública. (2002). Diario Oficial El Peruano.

Ley de Protección de Datos Personales. (2011). *Ley de Protección de Datos Personales.* Editora Perú.

Macutela, N. (2020). *Tratamiento de datos personales sensibles en Perú en el contexto de Covid-19.* Pontificia Universidad Católica del Perú. http://hdl.handle.net/20.500.12404/19125

Ministerio de Justicia y Derechos Humanos. (2013, 22 de marzo). Aprueban Reglamento de la Ley N° 29733, Ley de Protección de Datos Personales. Normas Legales, 491320. Diario Oficial El Peruano. https://cdn.www.gob.pe/uploads/document/file/1913756/DS-3-2013-JUS.REGLAMENTO.LPDP_.pdf.pdf?v=1643315587

Ministerio de Justicia y Derechos Humanos. (2020). Divulgar datos personales de pacientes con coronavirus puede ser multado hasta con 215 mil soles. https://www.gob.pe/institucion/minjus/noticias/108768-divulgar-datos-personales-de-pacientes-con-coronavirus-puede-ser-multado-hasta-con-215-mil-soles

Olvera, A. (2017). *La protección de datos personales por parte de las instituciones públicas de salud.* [Tesis de maestría, Universidad de Guadalajara]. http://148.202.167.116:8080/xmlui/handle/123456789/2158

Piña, J. (2021). Tratamiento y protección de datos personales en el sector público de la salud. El tránsito hacia el expediente clínico electrónico. *Nova Scientia, 13*(26). https://www.scielo.org.mx/scielo.php?script=sci_arttext&pid=S2007-07052021000100122

Praeli, F. (2016). La libertad de información y su relación con los derechos a la intimidad y al honor en el caso peruano. *Ius et Veritas*, *75*.

Praeli, F. (2015). El derecho a la protección de los datos personales. Algunos temas relevantes de su regulación en el Perú. *Themis, 67*, 131-140. https://revistas.pucp.edu.pe/index.php/themis/article/view/14462/15074

Procedimiento Administrativo Sancionador, Resolución Final N° 286-2019/CC3 (Comisión de Protección al Consumidor N° 3 - Sede Central noviembre 20, 2019).

Procedimiento Administrativo Sancionador, Resolución Final N° 288-2019/CC3 (Comisión de Protección al Consumidor N° 3 noviembre 20, 2019).

Procedimiento Administrativo Sancionador, Resolución Final Nº 047-2020/CC3 (Comisión de Protección al Consumidor Nº 3 - Sede Central junio 26, 2020).

Procedimiento Administrativo Sancionador, Resolución Final N.° 033-2020/CC3 (Comisión De Protección Al Consumidor N.° 3 marzo 13, 2020).

Procedimiento Administrativo Sancionador, Resolución Final N° 034-2020/CC3 (Comisión de Protección al Consumidor N° 3 - Sede Central marzo 13, 2020).

Quiroz, R. (2016). El Hábeas Data, protección al derecho a la información y a la autodeterminación informativa. *Letras*, *87*(126). http://www.scielo.org.pe/scielo.php?script=sci_arttext&pid=S2071-50722016000200002

Redacción Gestión. (2020, 7 de marzo). Ley de protección de Datos: sepa cuáles son los sectores con más denuncias por incumplir norma. *Gestión.* https://gestion.pe/peru/ley-de-proteccion-de-datos-sepa-cuales-son-los-sectores-con-mas-denuncias-por-incumplir-la-norma-nndc-noticia/

Rubio, M. (2008). *Para conocer la Constitución de 1993.* Fondo Editorial. Pontifica Universidad Católica del Perú.

Saldaña, M. (2012). "The Right to Privacy". La génesis de la protección de la privacidad en el sistema constitucional norteamericano: el centenario legado de Warren y Brandeis. *Revista de Derecho Político,* (85). https://revistas.uned.es/index.php/derechopolitico/article/view/10723/10242

Tribunal Italiano. (1974, 6 de mayo). Sentencia del Pretor de Roma.

Tribunal Constitucional. (2004). Expediente N.º 0090-2004-AA/TC-Lima. Arequipa: 5 de julio de 2004. https://www.tc.gob.pe/jurisprudencia/2004/00090-2004-AA.html

Tribunal Constitucional. (2011). Expediente N.º 04123-2011-PA/TC-Lima. Lima: 30 de noviembre de 2011. https://www.tc.gob.pe/jurisprudencia/2012/04123-2011-AA.html

Tribunal Constitucional. (2011). Expediente N.º 00744-2011-PA/TC-Ica. Lima: 13 de junio de 2011. https://tc.gob.pe/jurisprudencia/2011/00744-2011-AA.html

Varsi, E. (2018). Creaciones e innovaciones jurídicas de validez universal por Carlos Fernández Sessarego. *ATHINA*, *14.*

https://repositorio.ulima.edu.pe/bitstream/handle/20.500.12724/7372/Varsi_Fernandez_Sesarego.pdf?sequence=1&isAllowed=y

Anexos

Anexo 1: Resol. del Comité Institucional de Ética en Investigación

Universidad Continental

"Año de la unidad, la paz y el desarrollo"

Huancayo, 24 de julio del 2023

OFICIO N°0407-2023-CIEI-UC

Investigadores:

ANA RUTH NATSUMI AMES CARRIÓN
JULIO ADRIAN DELGADO CONISLLA
ANDALUCIA MARIFE MENDOZA TORRES

Presente-

Tengo el agrado de dirigirme a ustedes para saludarles cordialmente y a la vez manifestarles que el estudio de investigación titulado: **LA VULNERACIÓN DE LOS DATOS PERSONALES POR PARTE DE LAS ENTIDADES DE SALUD EN LOS AÑOS 2020 – 2021.**

Ha sido **APROBADO** por el Comité Institucional de Ética en Investigación, bajo las siguientes precisiones:

- El Comité puede en cualquier momento de la ejecución del estudio solicitar información y confirmar el cumplimiento de las normas éticas.
- El Comité puede solicitar el informe final para revisión final.

Aprovechamos la oportunidad para renovar los sentimientos de nuestra consideración y estima personal.

Atentamente

Walter Calderón Gerstein
Presidente del Comité de Ética
Universidad Continental

C.c. Archivo.

Anexo 2: Matriz de consistencia

<table>
<tr><td colspan="4">Título preliminar: La vulneración de los Datos Personales por parte de los Establecimientos de Salud y Servicios Médicos de Apoyo en Lima-Perú 2020-2021</td></tr>
<tr><td colspan="2">Problemas</td><td colspan="2">Objetivos de la investigación</td></tr>
<tr><td colspan="2">General:

¿Cuáles fueron los criterios de la ANPD para resolver casos de vulneración de datos personales en los establecimientos de salud y servicios médicos de apoyo en el año 2020 y 2021?

Específicos:

▪ ¿Cuáles son los hechos más frecuentes que fueron puestos en conocimiento de la ANPD en el año 2020 y 2021?
▪ ¿Cuál es la motivación de la ANPD en las resoluciones de los establecimientos de salud y servicios médicos de apoyo de salud en el año 2020 y 2021?
▪ ¿Cuál es la finalidad e importancia de graduar las sanciones y el cálculo de la multa en los fallos de las resoluciones emitidas por la ANPD en los años 2020 y 2021?
▪ ¿Cómo debería regularse la fiscalización de los bancos de datos en el ámbito de la salud para poder evitar la vulneración del derecho fundamental de la intimidad?</td><td colspan="2">General

Describir los criterios que tomó en cuenta la ANPD en las resoluciones de vulneración de datos personales en establecimientos de salud y servicios médicos de apoyo privadas en el año 2020 y 2021.

Específicos
▪ Identificar los hechos más frecuentes que fueron puestos en conocimiento de la ANPD año 2020 y 2021.
▪ Detallar la motivación de la ANPD en las resoluciones de los establecimientos de salud y servicios médicos de apoyo en el año 2020 y 2021.
▪ Especificar la finalidad e importancia de graduar las sanciones y el cálculo de la multa en los fallos de las resoluciones emitidas por la ANDP en los años 2020 y 2021.
▪ Establecer una propuesta de regulación sobre la fiscalización con respecto al banco de datos en el ámbito de salud para que no se afecte el derecho a la intimidad posteriormente mediante la vulneración de la protección de los datos personales.</td></tr>
<tr><td colspan="4">Diseño metodológico</td></tr>
<tr><td>Tipos de documentos</td><td>Criterios de selección de documentos</td><td>Técnicas de recojo de información</td><td>Instrumentos para recoger información</td></tr>
<tr><td>- Resoluciones
- Leyes o Normas
- Tesis
- Artículos
- Noticias</td><td>- Resoluciones con establecimientos de salud y servicios médicos de apoyo
- Leyes con relación a los datos personales.
- Con referencia al problema del mal uso de los datos personales.
- Con respecto al mal uso de los datos otorgados por los usuarios.
- Con respecto a establecimientos</td><td>- Las resoluciones son recogidas del propio buscador de la ANPD.
- Las leyes son recogidas de SPIJ, del diario oficial el peruano, entidades que tienen relación con su control de los datos personales.
- Los artículos y tesis son recogidos de revistas académicas como Dialnet, Scielo, Redalyc y Renati.
- Las noticias serán recogidas de fuentes confiables como Gestión, La República, El peruano y Comercio.</td><td>- Se elige para los estudios cualitativos, el análisis de datos de las resoluciones establecidas en el ANPD.
- Se recopila información para la recolecció</td></tr>
</table>

	de salud y servicios médicos de apoyo con referentes al mal uso de datos personales.		n, se categoriza y se llega interpretar con la conclusión del análisis.
Objetivos		**Categorías**	
Los artículos y tesis se analizarán con el objetivo de recolectar información con respecto al mal uso de los datos personales en el ámbito de la salud en entes privados. Las noticias se analizarán con el objetivo de recolectar información con respecto al mal uso de los datos personales en el ámbito público como el privado. Las resoluciones y las normas o leyes se analizarán con el objetivo de tener un marco legal donde se pueda entablar las acciones de las entidades con respecto al mal uso de los datos personales.		Mecanismos de control por parte de ANPD frente a estos problemas. Valoración de los hechos por parte de la ANPD. Necesidad de ver si las sanciones aplicadas logran evitar la reincidencia de estas acciones.	
Bibliografía de sustento para la justificación y delimitación del problema		**Bibliografía de sustento usada para el diseño metodológico**	
RD N° 3454-2021-JUS/DGTAIPD-DPDP. [ANPD]. PAS. 30 de noviembre de 2021. RD Nro. 94-2021-JUS/DGTAIPD. [ANPD]. PAS. 17 de diciembre de 2021. RD N° 1045 -2020-JUS/DGTAIPD-DPDP. [ANPD]. PAS. 30 de junio de 2020. RD N° 1436-2021-JUS/DGTAIPD-DPDP. [ANPD]. PAS. 02 de junio de 2021. RD N° 1885-2020-JUS/DGTAIPD-DPDP. [ANPD]. PAS. 02 de junio de 2021.		García Tenorio, Maryori Flor de Jazmín Urquizo Pinto, Jean Pierre Ricardo (2019) PROPUESTA DE UNA METODOLOGÍA PARA LA IMPLEMENTACIÓN DE LA LEY DE PROTECCIÓN DE DATOS PERSONALES APLICADO A UNA EMPRESA DEL SECTOR TEXTIL: MICHELL Y CÍA S.A. [Tesis Título Profesional, Especialidad en Sistemas de Información] Claudia Rios Cataño (2019), Guía para la realización de trabajos de investigación. Universidad Continental SAC.	

Técnicas e instrumentos de recolección de datos

Técnicas de recolección de datos

Para la recolección de datos se empleará la técnica cualitativa de revisión documental.

Instrumento de recolección de datos.

Se utilizará como instrumento de recolección de datos las fichas de revisión documental.

<table>
<tr><td>Resol.: 1885-2020-JUS/DGTAIPD-DPDP</td><td colspan="2">Exp.: 143-128-JUS/DGTAIPD-PAS</td><td>Fecha: 30/10/2020</td></tr>
<tr><td colspan="2">Tipo de Vulneración:
Usar los datos personales de los pacientes para finalidades no vinculadas a la prestación del servicio; sin obtener válidamente el consentimiento.
Realizar tratamiento de datos personales recopilados a través del sistema cliente/servidor denominado "GESTOR CLI", y el aplicativo Microsoft Excel; sin informar a los titulares de los datos lo requerido.</td><td>Entidad:
ONCOLOGIA S.A.C</td><td>Competencia:
Directora de Protección de Datos Personales.</td></tr>
<tr><td colspan="2">Normas Administrativas:
Literal f) del numeral 1 del art. 257 del Texto Único Ordenado de la Ley N° 27444.
Art. 126 del Reglamento de la LPDP.
Numeral 2 del art. 257 de la LPAG.</td><td colspan="2" rowspan="2">Sanción:
La sanción se determinó de acuerdo con estos factores:<table><tr><td>El beneficio ilícito resultante por la comisión de las infracciones</td><td></td></tr><tr><td>La probabilidad de detección de las infracciones</td><td>X</td></tr><tr><td>La gravedad del daño al interés público y/o bien jurídico protegido</td><td>X</td></tr><tr><td>El perjuicio económico causado</td><td></td></tr><tr><td>La reincidencia en la comisión de las infracciones</td><td></td></tr><tr><td>Las circunstancias de la comisión de la infracción</td><td>x</td></tr><tr><td>La existencia o no de intencionalidad en la conducta del infractor.</td><td>x</td></tr></table></td></tr>
<tr><td colspan="2">Puntos controvertidos:
Determinar si la entidad es responsable de contravenir:
Obligación establecida en el inciso 13.5 del art. 13 de la LPDP y el art. 12 del Reglamento de la LPDP. Infracción grave tipificada en el literal b) del inciso 2 del art. 132 del Reglamento de la LPDP.
Art. 18 de la LPDP. Infracción grave tipificada en el literal a) del inciso 2, del art. 132 del Reglamento de la LPDP.</td></tr>
<tr><td colspan="2">Desarrollo:
Que la entidad remitió un formulario denominado "Autorización de uso de datos personales en historia clínica", sin embargo, este no tiene la relevancia necesaria puesto no tiene fecha cierta y así no puede acreditar que esta acción es antes del proceso sancionador, por esos motivos se demuestra que la administrada cometido la infracción.
Que la entidad presento "Documento informativo del tratamiento de datos personales", antes del procedimiento sancionador por tales motivos se le exime de la sanción.</td><td colspan="2">Parte Resolutiva:
Sancionar a ONCOLOGIA S.A.C con la multa ascendente a cinco puntos cero uno Unidades Impositivas Tributarias (5.01 U.I.T.), por usar los datos personales de los pacientes para finalidades no vinculadas a la prestación del servicio, sin obtener válidamente el consentimiento del titular de los datos.
Eximir respecto de la responsabilidad administrativa por la presunta comisión de la infracción grave tipificada en el literal a), numeral 2, del art. 132 del Reglamento de la LPDP.</td></tr>
</table>

<table>
<tr><td>Resol.: 1436-2020-JUS/DGTAIPD-DPDP</td><td colspan="2">Exp.: 110-2019-JUS/DGTAIPD-PAS</td><td>Fecha: 02/06/2020</td></tr>
<tr><td colspan="2">Tipo de Vulneración:
Haber realizado tratamiento de datos personales incumpliendo la obligación de confidencialidad.</td><td>Entidad:
CLÍNICA SAN PABLO S.A.C.</td><td>Competencia:
Directora de Protección de Datos Personales.</td></tr>
<tr><td colspan="2">Normas Administrativas:
Literal f) del numeral 1 del art. 257 del Texto Único Ordenado de la Ley N° 27444.
Art. 126 del Reglamento de la LPDP.
Numeral 2 del art. 257 de la LPAG.</td><td colspan="2" rowspan="2">Sanción:
La sanción se determinó de acuerdo con la formula general, puesto que el beneficio ilícito resulta indeterminable, y es:<table><tr><td colspan="2">Formula general.</td></tr><tr><td rowspan="3">M = Mb x F</td><td>M: Multa preestablecida correspondiente a cada caso.</td></tr><tr><td>MB: Monto base de la multa. Depende de la gravedad del daño</td></tr><tr><td>F: elementos agravantes.</td></tr></table>En el presente caso la entidad reconoció la infracción y también genero un daño, por lo cual la formula seria: 22.50 x 0.80 = 18.</td></tr>
<tr><td colspan="2">Puntos controvertidos:
Determinar si la entidad es responsable de contravenir:
Obligación establecida en el art. 17 de la LPDP, al haber transferido los datos del denunciante sin que éste haya otorgado su consentimiento para dicho tratamiento.</td></tr>
<tr><td colspan="2">Desarrollo:
En el presente caso, según las pruebas aportadas por el denunciante a través del escrito y anexos ingresados con Hoja de Trámite N° 16215-2019MSC, queda acreditado que la administrada proporcionó datos personales del denunciante a su empleador Avianca S.A., situación que es aceptada por la administrada señalando a este incidente como un error al entregar dicha información sin autorización del usuario.
Conforme a los actuados y lo reconocido por la denunciada se tiene por acreditado el incumplimiento normativo.</td><td colspan="2">Parte Resolutiva:
Sancionar a CLÍNICA SAN PABLO S.A.C., con la multa ascendente a dieciocho Unidades Impositivas Tributarias (18,00 UIT) por haber realizado tratamiento de datos personales incumpliendo la obligación de confidencialidad.</td></tr>
</table>

<table>
<tr><td>Resol.: 1045-2020-JUS/DGTAIPD-DPDP</td><td colspan="2">Exp.: 127-2018-JUS/DGTAIPD-PAS</td><td>Fecha: 30/06/2020</td></tr>
<tr><td colspan="3">Tipo de Vulneración:
La administrada estaría difundiendo imágenes de personas en su sitio web www.montefiori.com.pe, sin obtener válidamente el consentimiento.
La administrada estaría realizando tratamiento de datos personales recopilados a través del sitio web www.montefiori.com.pe; mediante el aplicativo Excel sin informar a los titulares.
La administrada no habría cumplido con inscribir en el RNPDP los bancos de datos personales de pacientes, trabajadores, médicos, proveedores, videovigilancia, historias clínicas, usuarios del sitio web, y chequeo ocupacional, detectados en la fiscalización.
La administrada no habría comunicado a la DGTAIPD para su registro en el RNPDP, el flujo transfronterizo que realiza de los datos personales recopilados en el sitio web: www.montefiori.com.pe, debido a que el servidor físico que aloja la información del sitio web se ubica en Estados Unidos de América.
La administrada no habría cumplido con implementar las medidas de seguridad para el tratamiento de datos personales.</td><td>Entidad:
SERVICIOS DE SALUD MONTEFIORI S.A.C</td><td>Competencia:
Directora de Protección de Datos Personales.</td></tr>
<tr><td colspan="2">Normas Administrativas:
Literal f) del numeral 1 del art. 257 del Texto Único Ordenado de la Ley N° 27444.
Art. 126 del Reglamento de la LPDP.
Numeral 2 del art. 257 de la LPAG.
Puntos controvertidos:
Determinar si la entidad es responsable de contravenir:
Obligación establecida en el art. 13, numeral 13.5 de la LPDP y el art. 12 del Reglamento de la LPDP.
Tratamiento de datos sin comunicar a los usuarios de los datos lo requerido por el art. 18 del LPDP.
Obligación establecida en el art. 78 del Reglamento de la LPDP.
Obligación establecida en el art. 26 del Reglamento de la LPDP.
No cumplir con tener medidas de protección para el tratamiento de datos personales.
Obligación establecida en el numeral 1 del art. 39 del Reglamento de la LPDP.
Obligación establecida en el numeral 2 del art. 39 del Reglamento de la LPDP.
Obligación establecida en el primer párrafo del art. 40° del Reglamento de la LPDP.
Obligación establecida en el art. 42 del Reglamento de la LPDP.
Obligación establecida en el art. 43 del Reglamento de la LPDP.</td><td colspan="2">Sanción:
La sanción se determinó de acuerdo con estos factores para los tres hechos infractores:<table><tr><td>El beneficio ilícito resultante por la comisión de las infracciones</td><td></td></tr><tr><td>La probabilidad de detección de las infracciones</td><td>X</td></tr><tr><td>La gravedad del daño al interés público y/o bien jurídico protegido</td><td>X</td></tr><tr><td>El perjuicio económico causado</td><td></td></tr><tr><td>La reincidencia en la comisión de las infracciones</td><td></td></tr><tr><td>Las circunstancias de la comisión de la infracción</td><td>x</td></tr><tr><td>La existencia o no de intencionalidad en la conducta del infractor</td><td>x</td></tr></table></td></tr>
<tr><td colspan="2">Desarrollo:
La dirección considera que sobre el primer punto controvertido no se tiene mucha información con respecto a cómo se obtuvo las imágenes, por ende, no se le podrá sancionar por esta infracción.
La dirección considera que si se vulnero el art. 18 del LPDP. de forma previa al tratamiento de los datos personales que realiza mediante el sistema LOLCLI 9000++ utilizado por los ejecutivos del área de Admisión.
Sobre el tercer punto controvertido la dirección considera lo mismo que en el informe de DFI, lo cual es el archivamiento de la acción.
La dirección encuentra a la administrada infractora del cuarto punto controvertido, puesto que no desvirtuó lo señalado, además que el informe de DFI también corrobora la infracción.
Sobre el último punto controvertido la dirección considera que la administrada cometido infracción, y de esta manera se le sancionará y se pondrá mecanismos de para la seguridad de datos personales.</td><td colspan="2">Parte Resolutiva:
Eximir de responsabilidad SERVICIOS DE SALUD MONTEFIORI S.A.C. por el hecho imputado N° 1, referido al incumplimiento del art. 13, numeral 13.5 de la LPDP y el art. 12 del Reglamento de la LPDP.
Sancionar a SERVICIOS DE SALUD MONTEFIORI S.A.C. con la multa ascendente a siete unidades impositivas tributarias (7 UIT) por la comisión de la infracción grave tipificada en el literal a) del numeral 2 del art. 132 del Reglamento de la LPDP.
Sancionar a SERVICIOS DE SALUD MONTEFIORI S.A.C. con la multa ascendente a uno coma cinco unidades impositivas tributarias (1,5 UIT) por la comisión de la infracción leve tipificada en el literal e), numeral 1, del art. 132° de RLPDP.
Sancionar a SERVICIOS DE SALUD MONTEFIORI S.A.C. con la multa ascendente a seis comas cinco uno unidades impositivas tributarias (6,5 UTT) por la comisión de la infracción grave tipificada en el literal c) del numeral 2 del art. 132 del Reglamento de la LPDP
Imponer como medidas correctivas a SERVICIOS DE SALUD MONTEFIORI S.A.C.</td></tr>
</table>

<table>
<tr><td>Resol.: 94-2021-JUS/DGTAIPD-DPDP</td><td colspan="2">Exp.: 144-1-2018-JUS/DGTAIPD-PAS/ Recurso de Reconsideración</td><td>Fecha: 14/09/2020</td></tr>
<tr><td colspan="2">Tipo de Vulneración:
Usar los datos personales de los pacientes para finalidades no vinculadas a la prestación del servicio; sin obtener válidamente el consentimiento.
Haber realizado el uso de los datos personales a través de la página www.clinicamundosalud.com.pe, así como formularios físicos de uso de consideración de uso de datos personales. Sin informar lo requerido por el art. 18 de la LPDP.
No se inscribió al RNPDP los “Bancos de Sitios Web” y “Accesos”, que han sido detectados por la fiscalización.
No haber comunicado a la DGTAIPD para la respectiva inscripción ante el RNPDP , la realización del Flujo fronterizo de posibles datos que pudieron ser recopilados en el mismo sitio web debido a que este sitio web está ubicado en Inglaterra.</td><td>Entidad:
CLINICA MUNDO SALUD S.A.C.</td><td>Competencia:
Dirección General de Transparencia, Acceso a la Información Pública y Protección de Datos Personales/ Segunda Instancia de Apelación.</td></tr>
<tr><td colspan="2">Normas Administrativas:
Art. 18° de la LPDP.
Infracción grave que se encuentra tipificada en el literal a) del numeral 2 del art. 132 del Reglamento de la LPDP.</td><td colspan="2" rowspan="2">Sanción:
La sanción se determinó de acuerdo con estos factores:<table><tr><td>El beneficio ilícito resultante por la comisión de las infracciones</td><td></td></tr><tr><td>La probabilidad de detección de las infracciones</td><td></td></tr><tr><td>La gravedad del daño al interés público y/o bien jurídico protegido</td><td>X</td></tr><tr><td>El perjuicio económico causado</td><td></td></tr><tr><td>La reincidencia en la comisión de las infracciones</td><td></td></tr><tr><td>Las circunstancias de la comisión de la infracción</td><td>x</td></tr><tr><td>La existencia o no de intencionalidad en la conducta del infractor</td><td>x</td></tr></table></td></tr>
<tr><td colspan="2">Puntos controvertidos:
Determinar si la entidad es responsable de contravenir:
Establecer si la DPDP, evalúa de forma completamente debida sobre el documento “Compromiso de Trabajador”.
Incumplimiento del art. 18 de la Ley LPDP.
Establecer si ha sido considerada subsanadas las observaciones a través de cumplimiento de la medida coercitiva.
Se impuso la sanción administrativa acorde a los pronunciamientos previos emitidos de la DPDP.
Obligación establecida en el art. 248 de la Ley de Procedimientos Administrativos.</td></tr>
<tr><td colspan="2">Desarrollo:
La dirección considera que sobre el primer punto controvertido la sanción es merecida por no haber facilitado la existencia del banco de datos que almacena la información y también por ante una indebida transferencia internacional y nacional de cómo se da tratamiento a los datos; estipula que se vulnero el art. 18 del LPDP, no existe la debida información de derecho de información para cual fue el uso.
Respecto al segundo punto controvertido, cabe señalar que la futura implementación de las medidas coercitivas que tienen naturaleza distinta a la subsanación de las observaciones dentro del Procedimiento Sancionador, de manera que en esta situación ha habido una conducta infractora y no constituye una prueba de reconsideración como el administrado lo veía.
Simplemente para esas fechas aquellas del 2017, si hubo según dispuesto a la normativa actual de esa época sancionar a una situación favorable a la empresa administrada en comparación de la nueva, esto es debida a considerar antes como sanción leve a lo que hoy se puede considerar como grave. Corresponde reiterar sobre la situación del principio de irretroactividad benigna, considera que no se corresponde amparar sobre el extremo de esta apelación en el tercer punto.</td><td colspan="2">Parte Resolutiva:
Se ha declarado infundado el recurso de apelación y confirma la Resol. Directoral suministrada por la Resol. Directoral N° 1459-202-JUS/DGTAIPD-DPDP.</td></tr>
</table>

<table>
<tr><td colspan="2">Resol.: N° 3454-2021-JUS/DGTAIPD-DPDP</td><td>Exp.: 207-2021-PTT</td><td>Fecha: 14/09/2020</td></tr>
<tr><td colspan="2">Tipo de Vulneración:
Solicitar información sobre el estado de reembolso al “Seguro Social de Salud - ESSALUD”, que, ante un silencio administrativo negativo de solicitud de acceso a la información pública, afectando el derecho de autodeterminación bajo la normativa de la DPDP.</td><td>Entidad:
Seguro Social de Salud - ESSALUD</td><td>Competencia:
Dirección General de Transparencia, Acceso a la Información Pública y Protección de Datos Personales/ Segunda Instancia de Apelación.</td></tr>
<tr><td colspan="2">Normas Administrativas:
Art. 18° de la LPDP.
Art. 19° de la LPDP.
Art. 20° de la LPDP.
Art. 21° de la LPDP.
Art. 17° de la Ley de Procedimiento Administrativo General.</td><td colspan="2" rowspan="2">Sanción:
La sanción no repercute ante obtener el resultado favorable a la entidad, por lo siguiente:<table><tr><td>El beneficio ilícito resultante por la comisión de las infracciones</td><td></td></tr><tr><td>La probabilidad de detección de las infracciones</td><td></td></tr><tr><td>La gravedad del bien jurídico protegido o del daño al interés público.</td><td></td></tr><tr><td>Perjuicio económico causado</td><td></td></tr><tr><td>Reincidencia en la comisión de las infracciones</td><td></td></tr><tr><td>Circunstancias de la comisión de la infracción</td><td></td></tr><tr><td>Existencia o no de intencionalidad en la conducta del infractor</td><td></td></tr></table></td></tr>
<tr><td colspan="2">Puntos controvertidos:
Determinar si la entidad es responsable de contravenir:
Establecer si la entidad Administrada que resulte ser titular de bancos personales como el uso de tratamiento u acceso actuó conforme establecida en base al a los artículos 18,19,20 de obtener información sobre ellos mismos, en este caso cuando lo solicito la persona titular.
Sobre el Derecho de Peticiones por parte de la persona natural, a quien se solicita información a la entidad mencionada.</td></tr>
<tr><td colspan="2">Desarrollo:
El derecho de acceso de información al dato personal es necesario en tanto el titular debe obtener el tratamiento de información sobre sí mismo en el banco de datos , cuáles son las razones que fueron motivadas para su recopilación, así también sobre las transferencias realizadas, ahora en base al caso no resulta una condición evidente que su pedido de solicitud no está orientado a conocer sobre este sentido, esto quiere decir que no es necesario que la entidad incurra el aceptar el pedido presentado por el motivo de datos personales, sino ante otros procedimientos administrativos.
Respecto el segundo punto controvertido, cabe señalar atender en el ejercicio de su derecho brindado, puesto que en base la normativa hasta constitucional (Articulo 2, numeral 6) como se señala que si la persona natural es perteneciente sobre este procedimiento el administrado no puede negarse a otorgarle la información correspondiente sobre este.</td><td colspan="2">Parte Resolutiva:
Declarar improcedente la solicitud presentada por el señor contra ESSALUD, por resultar la Dirección de Protección de Datos Personales al resultar de no obtener competencia debido a la materia.</td></tr>
</table>

EXPOSICIÓN DE MOTIVOS	
Fundamentos y problemática	En nuestro ordenamiento jurídico con respecto a la protección de datos, se encuentra inmerso dentro de la Constitución en su art. 6.2, donde se nos menciona que los ciudadanos tiene la disposición de sus datos personales; asimismo, el Tribunal Constitucional desarrolló el derecho a la autodeterminación informativa el cual nos menciona que este derecho protege al titular frente abusos o riesgos que son consecuencia del mal uso de los datos personales; además que, este mismo derecho ofrece que el titular tenga control de su información personal. En nuestro país, la protección de los datos personales se encuentra regulada por la LPDP, y su RLPDP; posteriormente, la ANPD el cual se encarga de hacer cumplir las normas que se encuentran en la ley antes mencionada, puesto que, había diversas maneras de vulnerar estas normas; por ese motivo se debe priorizar la protección de datos personales y sensibles de las personas que son entregadas a las entidades públicas o privadas.
Propuesto	Basándonos en los datos previamente expuestos y en el desarrollo de este documento, consideramos fundamental la realización de una modificación legislativa en la regulación de las funciones de la ANPD. Esta medida se justifica en el principio preventivo, el cual tiene como objetivo la previsión de medidas idóneas para evitar futuras obstaculizaciones. En este sentido, se busca establecer un marco regulatorio respecto a la previa fiscalización de la inscripción del banco de datos vinculados a los servicios de salud, en los cuales se almacenan datos personales y sensibles. El propósito primordial es proteger desde el inicio contra cualquier afectación que pueda surgir debido a la incorrecta inscripción de los bancos de datos y la falta de verificación de los requisitos que deben cumplir los establecimientos de salud y los servicios médicos de apoyo para el almacenamiento de datos personales o sensibles y la recopilación de información de los usuarios. El objetivo de este proyecto es adicionar un literal al inciso 20 del artículo 33 de la LPDP sobre la fiscalización, para lo cual la ANPD se enfocará en realizar una fiscalización ex ante a las entidades de salud que registren sus bancos de datos ante la RNPDP. De esa manera, el Estado tiene la obligación de brindar protección a los derechos fundamentales que se puedan ver vulnerados dentro de su territorio, como lo son la intimidad, privacidad y la autonomía informativa, esto a razón de garantizar un resguardo a los datos personales/sensibles de los titulares que brindan su información a ser registrada en los bancos de datos que utilicen las entidades de salud.
Antecedentes legislativos	De conformidad con lo publicado en la página web del Congreso de la República, no se encuentra iniciativas legislativas en trámite referidas a la propuesta legislativa que se pretende implementar.
Análisis costo Beneficio	La aplicación de la propuesta que se pretende establecer en el inciso 20 del art. 33 de la LPDP no generará un gasto adicional porque se realizará una fiscalización ex ante del registro de los bancos de datos de los establecimientos de salud y servicios médicos de apoyo. El beneficio no será cuantificable ya que se trata de derechos fundamentales. La aprobación de esta iniciativa generará una mejor protección de los derechos fundamentales de la intimidad y privacidad, este último conexo a la autodeterminación informativa porque la vulneración de los datos personales y sensibles disminuirán a razón de la fiscalización ex ante que se realizará. En consecuencia, su utilidad se fundamenta en la prevención de la trasgresión que sufren las personas al otorgar sus datos que se les requieren para a su atención médica las cuales se almacenan en los bancos de datos que se utilizan en las entidades salud.
Impacto en la legislación nacional	La aprobación de la presente propuesta supone modificar y mediante ello establecer un mecanismo específico que pueda ayudar a mejorar el control y protección de los bancos de datos utilizados por las entidades de salud, para que de ese modo se prevenga la vulneración de los datos personales/sensibles ante una fiscalización ex post por la ANPD lo cual termina vulnerando el derecho fundamental a la intimidad, privacidad y autodeterminación informativa, así como los pertinentes que se conexen a estos. Esta adición entrará en vigor al día siguiente de su publicación en el diario Oficial el Peruano, entendiéndose que se está estableciendo un nuevo mecanismo para un caso particular. Además, en relación de la iniciativa con el acuerdo nacional y la agenda legislativa 2024.