



Resolución Directoral N° 2271-2024-JUS/DGTAIPD-DPDP

Expediente N°
122-2023-JUS/DGTAIPD-PAS

Lima, 1 de julio de 2024

VISTOS:

El Informe N° 008-2023-JUS/DGTAIPD-DFI del 23 de enero de 2024¹, emitido por la Dirección de Fiscalización e Instrucción de la Dirección General de Transparencia, Acceso a la Información Pública y Protección de Datos Personales (en adelante, la DFI), y demás documentos que obran en el respectivo expediente, y;

CONSIDERANDO:

I. Antecedentes

1. Mediante el escrito ingresado con la Hoja de Trámite N° 292915-2022MSC del 2 de agosto de 2022², [REDACTED] (en adelante, la denunciante) reportó que el Banco de Crédito del Perú (en adelante, la administrada) estaba realizando el tratamiento de sus datos personales (estado civil, CUI, sexo, fecha de nacimiento, foto, ubigeo, fecha de inscripción, emisión y caducidad), que no son necesarios para cumplir con la finalidad de presentar un reclamo virtual, ya que esta exige la toma fotográfica del DNI y la toma facial de quien presenta reclamación, contrariando lo dispuesto en los artículos 6, 7 y 28 de la Ley N° 29733, Ley de Protección de Datos Personales (en adelante, LPDP).
2. La denunciante detalló que en el intento de obtener una constancia de no adeudo, se tuvo que generar una hoja de reclamación virtual en el sitio web de la administrada (C-08732858), para lo cual se le exigió que consigne su número de cuenta, y en el segundo paso del proceso, una imagen facial para reconocimiento y una imagen de su DNI, los cuales no son exigidos en el Reglamento de Libro de Reclamaciones, aprobado por el Decreto Supremo N° 011-2011-PCM (en adelante, Reglamento del Libro de Reclamaciones), lo cual propiciaría que una persona sin cuentas con la administrada también se vería obligada a aceptar tal tratamiento de datos personales, lo que sería contrario al derecho de reclamo.

¹ Folios 282 al 343

² Folios 2 al 51

Esta es una copia auténtica imprimible de un documento electrónico archivado por el Ministerio de Justicia y Derechos Humanos, aplicando lo dispuesto por el Art. 25 de D.S. 070-2013-PCM y la Tercera Disposición Complementaria Final del D.S. 026-2016-PCM. Su autenticidad e integridad pueden ser contrastadas a través de la siguiente dirección web: https://sgd.minjus.gob.pe/gesdoc_web/login.jsp e ingresando el Tipo de Documento, Número y Rango de Fechas de ser el caso o https://sgd.minjus.gob.pe/gesdoc_web/verifica.jsp e ingresando Tipo de Documento, Número, Remitente y Año, según corresponda.

Resolución Directoral N° 2271-2023-JUS/DGTAIPD-DPDP

3. La denunciante menciona también que a modo de prueba se ingresó un segundo reclamo a su nombre, verificando que la administrada continuaba exigiendo información y/o documentación innecesaria.
4. Mediante la Carta N° 599-2022-JUS/DGTAIPD-DFI del 7 de diciembre de 2022³, se solicitó a la administrada lo siguiente:
 - Señalar, acreditar y justificar el procedimiento que ha implementado para la interposición de reclamos de sus clientes y no clientes, respecto al tratamiento de los datos personales.
 - Precisar cuál es la relevancia de los datos personales requeridos para ingresar reclamos.
5. Por medio del escrito ingresado con la Hoja de Trámite N° 511686-2022MSC del 29 de diciembre de 2022⁴, la administrada dio respuesta al requerimiento de la DFI, señalando lo siguiente:
 - Es necesario encausar esta y la anterior denuncia presentada en un mismo expediente, por tratar de lo mismo.
 - Para atender un reclamo a través de su sitio web, se solicita al usuario que valide su identidad, contando para ello con dos opciones: Validación a través del reconocimiento facial y del DNI o, validación a través del número y clave de una tarjeta de su propiedad; todo ello con la finalidad de brindar seguridad, evitando los riesgos de suplantación al momento del enrolamiento.
 - Dichos datos personales son recolectados con la finalidad de poder verificar y validar a través del registro del Reniec la identidad del usuario que presenta el reclamo a través de un medio digital; a su vez, son almacenados con la finalidad de sustentar que se ha realizado la correcta verificación de la identidad para poder registrar un reclamo.
 - A fin de brindarle información antes de la toma de las imágenes, se tiene por obligatoria la lectura de un informativo sobre el tratamiento de datos personales que manejan, lo cual omitió referir la denunciante.
 - Estas medidas obedecen a las exigencias de la Superintendencia de Banca, Seguros y AFP (en adelante, SBS), contenidas en la Resolución N° 504-2021, mediante el cual se aprobó el Reglamento para la Gestión de Seguridad de la Información y Ciberseguridad (en adelante, Reglamento de la SBS), cuyos artículos 2 y 18 establecen que cuando se realice cualquier enrolamiento de un usuario en un canal digital, se requiere por lo menos verificar la identidad del usuario y las medidas para reducir la posibilidad de suplantación de identidad.
 - Por eso, cuando no se tiene datos de algún cliente en su base de datos, se efectúa su enrolamiento con las imágenes de su DNI, del mismo cliente, para luego recurrir al servicio de consulta de datos de sistema del Reniec para obtener los datos del DNI del cliente y compararlos con lo obtenido, más precisamente, entre los patrones biométricos de cada imagen, cuya coincidencia implica la correcta validación de la identidad.
 - Cuando cuentan previamente con los datos del solicitante, comparan el patrón de la imagen del cliente con aquella que ya tienen, buscando su coincidencia.

³ Folios 52 al 56

⁴ Folios 63 al 77

Resolución Directoral N° 2271-2023-JUS/DGTAIPD-DPDP

- Los datos personales recopilados son esenciales para verificar y validar a través del registro de la Reniec la identidad del usuario que presenta el reclamo a través de un medio digital, cumpliendo sus obligaciones regulatorias.
6. Mediante el proveído del 17 de febrero de 2023⁵, la DFI dispuso la acumulación de los expedientes de fiscalización de las denuncias presentadas por la denunciante (expedientes N° 186 y 291-2022).
7. Por medio del Informe de Fiscalización N° 068-2023-JUS/DGTAIPD-DFI-EMZA⁶, el 7 de marzo de 2023, el Analista Legal de Fiscalización de la DFI concluye que se han determinado con carácter preliminar las circunstancias que justifican la instauración de un procedimiento administrativo sancionador, al haberse hallado indicios de una inobservancia del principio de Proporcionalidad del artículo 7 de la LPDP, que configuraría la infracción grave tipificada en el literal d) del numeral 2 del artículo 132 del Reglamento de la LPDP, aprobado por el Decreto Supremo N° 003-2013-JUS (en adelante, Reglamento de la LPDP).
8. Dicho informe fue notificado con la Cédula de Notificación N° 216-2023-JUS/DGTAIPD-DFI, el 8 de marzo de 2023⁷.
9. El 21 de agosto de 2023, personal de la DFI ingresó al sitio web de la administrada, a fin de verificar la forma en que se valida la identidad de los reclamantes⁸.
10. Mediante la Orden de Visita N° 106-2023-JUS/DGTAIPD-DFI del 26 de septiembre de 2023⁹, la administrada dispuso efectuar una visita de fiscalización al establecimiento de la administrada, a fin de verificar el procedimiento utilizado para la validación facial (verificación biométrica) implementado en su entidad para la atención de sus clientes y usuarios de sus servicios en general que incluye el Libro de Reclamaciones virtual.
11. La primera visita de fiscalización a la administrada se realizó en la misma fecha¹⁰, anotándose en el acta de fiscalización la solicitud de reprogramación de la visita, debido a que el personal responsable del tratamiento de la base de datos "Biometría" estaba trabajando de manera remota.
12. El 27 de septiembre de 2023 se realizó la segunda visita de fiscalización a la administrada, consignándose en el acto de fiscalización respectiva¹¹, lo siguiente:
- La administrada señaló que emplea la biometría para validar la identidad de personas que presentan reclamos virtuales, empleando dicho servicio para otras aplicaciones: Yape, seguros, Dinero al instante, Cocos y Lucas, Banca Móvil, tarjetas.

⁵ Folios 79 al 87

⁶ Folios 162 al 177

⁷ Folios 178 al 191

⁸ Folios 192 al 198

⁹ Folios 199 al 202

¹⁰ Folios 203 al 205

¹¹ Folios 206 al 216

Resolución Directoral N° 2271-2023-JUS/DGTAIPD-DPDP

- La validación biométrica es realizada con un componente tecnológico (motor biométrico) provisto por Facephi Biometría S.A. (en adelante, Facephi).
 - Al hacer pruebas de funcionalidad de dicho motor, se constató lo siguiente:
 - Luego del registro del número del DNI del reclamante, el "Gateway biométrico" valida si el dato biométrico (la imagen facial) ya se encuentra en su base de datos "BIOM", donde se almacenan imágenes del DNI y/o de los rostros, encriptadas.
 - Solo en caso de que sea el primer uso del reclamante, se procede a su enrolamiento usando el servicio de consulta provisto por el Reniec, donde extrae la imagen a cotejar con el dispositivo biométrico provisto por Facephi, que puede determinar su grado de similitud y si se está empleando una imagen en tiempo real del reclamante (al momento de presentación de la reclamación) y no de otra imagen.
 - Su libro de reclamaciones tiene dos mecanismos de validación: Número y clave de tarjeta, conjuntamente con la validación biométrica.
 - Genera copias de respaldo completas e incrementales de la base "BIOM".
 - La validación biométrica facial se realiza por la necesidad de evitar revelar información bancaria a terceros, siguiendo la normativa sectorial.
 - Por ello, para validar la identidad del reclamante, que accederá a tal información, tiene como única herramienta para ello la modalidad biométrica.
13. En el Informe Técnico N° 107-2023-DFI-ORQR del 2 de octubre de 2023, el Analista de Fiscalización en Seguridad de la Información emitió las siguientes conclusiones sobre la visita de fiscalización efectuada:
- Se verificó que para el caso de personas que van a registrar un reclamo por primera vez y no han sido sometidas a una verificación biométrica facial previamente, se les enrola valiéndose del servicio de consulta del Reniec, de donde se obtiene la ficha que incluye la fotografía que luego será empleada para el análisis biométrico.
 - Cuando una persona previamente enrolada realiza una operación o reclamo que requiera una validación biométrica facial, en las consultas ya no se emplea el servicio del Reniec, sino su base de datos "BIOM".
14. Por medio de la Resolución Directoral N° 232-2023-JUS/DGTAIPD-DFI del 13 de octubre de 2023¹², la DFI resolvió iniciar procedimiento administrativo sancionador a la administrada, por las siguientes presuntas infracciones:
- **Hecho imputado N° 1:** Haber realizado el tratamiento desproporcionado de los datos personales de quienes generan un reclamo a través del libro de reclamaciones virtual publicado en su sitio web, al recopilar imágenes del DNI y de la imagen facial para tratarla con medios técnicos específicos para identificación a través de la validación biométrica (dato sensible), los cuales no son adecuados, necesarios ni pertinentes para la finalidad de identificar plenamente al reclamante, incumpliendo lo dispuesto en los artículos 7 y numeral 3 del artículo 28 de la LPDP, lo que configuraría la infracción grave

¹² Folios 223 al 255

Esta es una copia auténtica imprimible de un documento electrónico archivado por el Ministerio de Justicia y Derechos Humanos, aplicando lo dispuesto por el Art. 25 de D.S. 070-2013-PCM y la Tercera Disposición Complementaria Final del D.S. 026-2016-PCM. Su autenticidad e integridad pueden ser contrastadas a través de la siguiente dirección web: https://sgd.minjus.gob.pe/gesdoc_web/login.jsp e ingresando el Tipo de Documento, Número y Rango de Fechas de ser el caso o https://sgd.minjus.gob.pe/gesdoc_web/verifica.jsp e ingresando Tipo de Documento, Número, Remitente y Año, según corresponda.

Resolución Directoral N° 2271-2023-JUS/DGTAIPD-DPDP

tipificada en el literal d) del numeral 2 del artículo 132 del reglamento de dicha ley.

- **Hecho imputado N° 2:** Haber realizado el tratamiento de los datos personales de quienes generan un reclamo, al almacenar el dato biométrico de la imagen facial en una base de datos propia, sin obtener válidamente el consentimiento de sus titulares, incumpliendo con la obligación establecida en los artículos 5 y 13 de la LPDP, así como de los artículos 7 y 12 de su reglamento, lo que configuraría la infracción grave tipificada en el literal b) del numeral 2 del artículo 132 de tal reglamento.
15. A través de la Cédula de Notificación N° 928-2023-JUS/DGTAIPD-DFI se notificó a la administrada dicha resolución directoral, el 17 de octubre de 2023¹³.
16. Mediante el escrito ingresado con la Hoja de Trámite N° 521071-2023MC del 8 de noviembre de 2023¹⁴, la administrada presentó sus descargos, señalando lo siguiente:
- Para presentar un reclamo a través de su sitio web, se tienen dos opciones: Para los no clientes, se realiza a través de la biometría facial, empleando la imagen en tiempo real al contrastar con la imagen del DNI; y en el caso de los clientes, utilizando la tarjeta de débito y su clave.
 - Tales procedimientos tienen como fin evitar cualquier riesgo de suplantación de identidad de los clientes y el acceso no autorizado a información sensible, como es la financiera.
 - Obedeciendo a tal finalidad, así como a la observancia de las normas sectoriales pertinentes (Reglamento de la SBS), el tratamiento de los datos biométricos señalados resulta proporcional, considerando que solo se requiere tal información en el medio virtual.
 - El artículo 5 del Reglamento del Libro de Reclamaciones no establece la información que una empresa puede pedir ni excluye otros requisitos o medidas de seguridad para identificar al reclamante, pues solo establece mínimos; norma que sí sería aplicable al caso, considerando que es parte de los servicios del crédito hipotecario solicitado por la denunciante y no un reclamo como se está entendiendo.
 - Debe tomarse en cuenta que el retiro de estas medidas de seguridad llevaría inevitablemente a una desprotección de la información y recursos financieros de los clientes y usuarios.
 - El tratamiento de los datos personales de biometría facial de los usuarios se realiza con la finalidad de velar por la seguridad de su información y sus productos financieros, sin apartar de lo que el cumplimiento de lo que la normativa sectorial requiere; lo que configura las excepciones de obligatoriedad del consentimiento de los numerales 5, 9 y 13 del artículo 14 de la LPDP.
 - Dicha situación se concatena con el hecho de que tales datos personales no son usados para otras finalidades, como aquellas de índole publicitario, pues obedece estrictamente a los intereses de sus usuarios.
 - Con el tratamiento de los datos biométricos efectuado se cumple también el principio de Calidad de la LPDP, pues se contribuye con mantener la actualidad

¹³ Folios 256 al 263

¹⁴ Folios 265 al 281

Resolución Directoral N° 2271-2023-JUS/DGTAIPD-DPDP

de los datos previamente obtenidos, con lo que se preserva la fidelidad de la información empleada.

- También se debe apreciar que el servicio del Reniec suele presentar disfunciones que afectan el sistema de validación de identidad, lo que puede impedir contar con un servicio ágil, fiable y disponible en todo momento, haciendo necesario tener otra fuente en su base de datos.
 - Cada mes realizan entre 3.5 y 4 millones validaciones de identidad, por lo que la caída breve de tal sistema puede representar una cantidad significativa de clientes no atendidos.
 - Sancionarlos por ambas imputaciones implicaría la vulneración del principio de *Non bis in idem* del artículo 248 del Texto Único Ordenado de la Ley del Procedimiento Administrativo General, aprobado por Decreto Supremo N° 004-2019-JUS (en adelante, LPAG), toda vez que concluir que se efectuó el tratamiento desproporcionado de datos, implicaría que también se considere que hubo un tratamiento sin consentimiento de los mismos datos.
 - Las infracciones que se han imputado se sustentan en el hecho de que la autoridad considera que la medida implementada para la validación de identidad a través de biometría facial no sería adecuada ni justificada por las obligaciones sectoriales, vale decir, carecería de legitimidad; tal circunstancia no puede permitir que en razón de dicho tratamiento ilícito de los datos biométricos, se impongan dos sanciones.
 - Las imputaciones son nulas, toda vez que se formularon en vulneración de los principios de Legalidad y Tipicidad que rigen la potestad sancionadora, del artículo 248 de la LPAG, de acuerdo con la interpretación del Tribunal Constitucional y de la Corte Suprema de Justicia de la República.
17. Mediante el Informe N° 008-2023-JUS/DGTAIPD-DFI, la DFI remitió a la Dirección de Protección de Datos Personales de la Dirección General de Transparencia, Acceso a la Información Pública y Protección de Datos Personales (en adelante, la DPDP) los actuados para que resuelva en primera instancia el procedimiento administrativo sancionador iniciado, recomendando lo siguiente:
- Imponer la multa de veintisiete unidades impositivas tributarias (27 UIT) por la comisión de la infracción grave tipificada en el literal d) del numeral 2, del artículo 132 del Reglamento de la LPDP
 - Imponer la multa de cuarenta y cinco unidades impositivas tributarias (45 UIT) por la comisión de la infracción grave tipificada en el literal b) del numeral 2, del artículo 132 del Reglamento de la LPDP.
18. Con la Resolución Directoral N° 018-2024-JUS/DGTAIPD-DFI del 23 de enero de 2024¹⁵, la DFI dio por concluidas las actuaciones instructivas correspondientes al procedimiento sancionador.
19. Dichos documentos fueron notificados a la administrada a través de la Cédula de Notificación N° 069-2024-JUS/DGTAIPD-DFI el 24 de enero de 2024¹⁶.

¹⁵ Folios 344 al 348

¹⁶ Folios 349 al 352

Resolución Directoral N° 2271-2023-JUS/DGTAIPD-DPDP

20. Mediante el escrito ingresado con la Hoja de Trámite N° 55458-2024MSC del 1 de febrero de 2024¹⁷, la administrada presentó sus alegatos respecto al informe de instrucción, especificando lo siguiente:
- Las conclusiones de la DFI concernientes a que la recopilación es excesiva en el caso de los reclamantes que no son sus clientes y a que el Reglamento de la SBS establece medidas menos “intrusivas” que podrían haberse implementado en vez de la biometría facial, son incorrectas, toda vez que efectúan el tratamiento ajustado al balance de las finalidades y la protección de los datos personales de las personas, aparte de responder a las necesidades de seguridad que un negocio financiero requiere, así como a una exigencia regulatoria del sistema bancario.
 - Ante la circunstancia de atender el reclamo a distancia, se hace necesaria la verificación facial en tiempo real para la comprobación de la identidad de los reclamantes, teniendo en cuenta los riesgos que se corren en las actividades de su giro.
 - Solo el 11% de las comunicaciones vía su sitio web, constituyen quejas, vale decir, comunicaciones de personas que no tienen ninguno de sus productos financieros; mientras que el porcentaje restante corresponde a consultas y reclamos sobre operaciones financieras.
 - La propia DFI ha admitido la funcionalidad de la validación biométrica de la identidad para la contratación de sus productos, lo cual también es entendible para los casos en los que se hace una reclamación.
 - En atención a la sensibilidad de la información tratada, se han implementado todas las medidas de seguridad recomendadas en la Opinión Consultiva N° 32-2017-JUS/DGTAIPD, asumiendo los altos costos de su implementación.
 - Corresponde diferenciar entre los usuarios “clientes intermitentes” y los usuarios “clientes”, que son los dos tipos de usuario que tiene su sistema de reclamos y reciben sus servicios, por lo que en ambos casos, la verificación biométrica es necesaria.
 - No es posible establecer distintos mecanismos para la presentación de reclamos en su libro de reclamaciones virtual en función del tipo de reclamo, pues es inviable implementar una diversidad de procesos para atender los tipos de reclamos, que recién con el ingreso del reclamo y su posterior evaluación por un asesor (horas o días después) se podría saber sobre qué servicio es y qué tipo de validación se requerirá, demorando el proceso requerido por el consumidor e incurriendo en incumplimiento.
 - La DFI ha observado que esta medida de todos modos sería desproporcional dado que el Reglamento de la SBS requiere la utilización de dos factores de autenticación entre los que enumera, sin que la biometría sea obligatoria, cuando en realidad, dicha norma le permite usar dos medios, lo cual resulta más intrusivo que utilizar uno solo en lugar de dos factores independientes, en lugar de la biometría, que puede operarse solo con el número DNI (algo que solo él tiene) y algo que es, su biometría facial.
 - Se cuestiona la implementación del factor de biometría pero la autoridad instructora no ha propuesto algún ejemplo de alternativa que sería “más proporcional” o “menos intrusiva” y que cumpla con igual eficacia y seguridad;

¹⁷ Folios 354 al 388

Resolución Directoral N° 2271-2023-JUS/DGTAIPD-DPDP

lo cual no pudo hacer, incluso porque en los fundamentos de la segunda imputación, la DFI admitió que para algunos casos, la biometría es un medio adecuado.

- El Reglamento del Libro de Reclamaciones no establece en su artículo 5 una lista cerrada de información a tratar, no existiendo un límite para establecer un mecanismo de validación biométrico.
 - No requieren del consentimiento de las personas que presentan reclamaciones, puesto que dicha actividad se encuadra en las excepciones del artículo 14 de la LPDP, al tratarse de datos necesarios para la ejecución contractual y que solo se utilizan para la validación de la identidad del reclamante.
 - En tal sentido, si el usuario de los productos financieros requiere efectuar algún trámite con validación de identidad, no será necesario volver a pedir la información biométrica ni recurrir al servicio de Reniec, bastando solo el contraste con lo previamente almacenado.
 - La DFI ha propuesto el monto de la sanción partiendo de un monto base erróneo, cuando el monto base para las infracciones graves es de cinco unidades impositivas tributarias.
 - Al no verificarse perjuicio económico causado, ni reincidencia por esta infracción, debió evaluarse la propuesta de atenuación de la multa, en lugar de concluir tautológicamente que el presunto hechizo infractor de por sí, generaba daños a más de dos personas, constituyéndose una motivación aparente que invalidaría el pronunciamiento de la autoridad.
 - Sancionar por las dos infracciones imputadas constituiría una vulneración del principio del *Non bis in Idem*, pues si se determina que el empleo de datos biométricos es proporcional para el fin señalado, entonces no se hubiera requerido el consentimiento de su titular, ya que se hubiera configurado un supuesto de excepción del artículo 14 de la LPDP; lo que demuestra que son hechos indesligables.
 - Se pretende aplicar sanciones tipificadas con normas infralegales, contrariando los principios de Legalidad y Tipicidad.
21. El 27 de febrero de 2024, se efectuó el informe oral solicitado por la administrada, que presentó los siguientes argumentos:
- En su informe final de instrucción, la DFI no ha tomado en cuenta las particularidades del mercado financiero ni de la específica actividad en la que se enmarca el caso.
 - La verificación biométrica se explica por la necesidad de autenticación de la identidad en los canales virtuales de reclamaciones, que representa el 89% de comunicaciones, frente al 11% que constituyen quejas, mientras que el 0.3% de estas comunicaciones son de "clientes intermitentes" cuyas transacciones sí implican el empleo de información sensible.
 - A través de la Opinión Consultiva N° 32-2021-JUS/DGTAIPD, la autoridad reconoció que es proporcional el uso de la información biométrica para la identificación de contratantes de créditos, lo que hace que su caso sea válido, toda vez que el libro de reclamaciones es parte de sus servicios.
 - Así también, con tal opinión consultiva, se establecieron directrices de seguridad para el empleo de sistemas de identificación biométrica, las cuales en el presente caso, son acatadas.

Esta es una copia auténtica imprimible de un documento electrónico archivado por el Ministerio de Justicia y Derechos Humanos, aplicando lo dispuesto por el Art. 25 de D.S. 070-2013-PCM y la Tercera Disposición Complementaria Final del D.S. 026-2016-PCM. Su autenticidad e integridad pueden ser contrastadas a través de la siguiente dirección web: https://sgd.minjus.gob.pe/gesdoc_web/login.jsp e ingresando el Tipo de Documento, Número y Rango de Fechas de ser el caso o https://sgd.minjus.gob.pe/gesdoc_web/verifica.jsp e ingresando Tipo de Documento, Número, Remitente y Año, según corresponda.

Resolución Directoral N° 2271-2023-JUS/DGTAIPD-DPDP

- En observancia de la normativa sectorial (Reglamento de la SBS) cuyo artículo 18 establece la necesidad de verificar la identidad, requiere de dos factores de categorías diferentes e independientes (algo que solo el usuario posee, el DNI, y un factor biométrico), siendo esta la menos intrusiva.
 - La regulación del libro de reclamaciones no establece una lista cerrada de información que se puede requerir, sino un mínimo.
22. Por medio de la Carta N° 310-2024-JUS/DGTAIPD-DPDP del 28 de febrero de 2024¹⁸, se solicitó a la administrada remitir los documentos (contratos, convenios y/o adendas) suscritos con el Reniec, por los cuales este último brinda los servicios de consulta de datos y provee las fichas que contienen las imágenes de rostros de los reclamantes.
23. Mediante el escrito ingresado con la Hoja de Trámite N° 113250-2024MSC del 13 de marzo de 2024, la administrada remitió la documentación requerida, señalando lo siguiente:
- En la segunda cláusula del "Convenio de consulta en línea utilizando línea digital" suscrito con el Reniec, este pone a disposición la base de datos del Registro Único de Identificación de las Personas Naturales – RUIPN, el cual contiene la fotografía de cada persona, a fin de utilizarlo como medio de consulta en las actividades del usuario.
 - Esta información es empleada para validar la identidad de los usuarios que interponen reclamos o solicitudes en línea, quienes se toman una fotografía en tiempo real que es contrastada con la imagen que posee Reniec y una vez tal validación se efectúa, el empleo de la información cesa.
 - No descarga, capta ni almacena la información puesta a su disposición por Reniec, dicha información solo es utilizada para el proceso de validación de identidad, en estricto cumplimiento de lo regulado en el mencionado convenio.
 - Debe reiterarse la necesidad de conocer a profundidad las particularidades del mercado, entre ellas las exigencias de las normas sectoriales y las que surgen del contexto actual de inseguridad, que impone cargas relevantes sobre las empresas del sector bancario, a fin de evitar perjuicios a sus clientes y usuarios.
 - En tal sentido, el uso de esta información resulta razonable para tener la certeza de que el usuario es quien dice ser antes de proveerle información vinculada con información financiera.

II. Competencia

24. De conformidad con el artículo 74 del Reglamento de Organización y Funciones del Ministerio de Justicia y Derechos Humanos, aprobado por Decreto Supremo N° 013-2017-JUS, la DPDP es la unidad orgánica competente para resolver en primera instancia, los procedimientos administrativos sancionadores iniciados por la DFI.
25. En tal sentido, la autoridad que debe conocer el presente procedimiento sancionador, a fin de emitir resolución en primera instancia, es la Directora de Protección de Datos Personales.

¹⁸ Folios 410 al 428

Esta es una copia auténtica imprimible de un documento electrónico archivado por el Ministerio de Justicia y Derechos Humanos, aplicando lo dispuesto por el Art. 25 de D.S. 070-2013-PCM y la Tercera Disposición Complementaria Final del D.S. 026-2016-PCM. Su autenticidad e integridad pueden ser contrastadas a través de la siguiente dirección web: https://sgd.minjus.gob.pe/gesdoc_web/login.jsp e ingresando el Tipo de Documento, Número y Rango de Fechas de ser el caso o https://sgd.minjus.gob.pe/gesdoc_web/verifica.jsp e ingresando Tipo de Documento, Número, Remitente y Año, según corresponda.

Resolución Directoral N° 2271-2023-JUS/DGTAIPD-DPDP

III. Normas concernientes a la responsabilidad de la administrada

26. Para la determinación de la responsabilidad de la administrada respecto de una infracción, se deberá tomar en cuenta lo establecido en el artículo 257 del Texto Único Ordenado de la Ley N° 27444, Ley del Procedimiento Administrativo General, aprobado por Decreto Supremo N° 004-2019-JUS (en adelante, la LPAG), en su calidad de norma común para los procedimientos administrativos, conjuntamente con lo establecido en el Reglamento de la LPDP.
27. En tal sentido, se atiende al hecho de que el literal f) del numeral 1 de dicho artículo de la LPAG, establece como una causal eximente de la responsabilidad por infracciones, la subsanación voluntaria del hecho imputado como infractor, si es realizada de forma previa a la notificación de imputación de cargos¹⁹ y siempre que el carácter del hecho infractor en cada caso, permitan dicha subsanación, entendida esta como la reposición de la situaciones a una situación anterior al mismo, estudiando también el ajuste de la conducta del responsable a lo dispuesto en la normativa, atendiendo a circunstancias tales como el carácter instantáneo, continuado o permanente de las infracciones y la disminución o grado de reversión de las consecuencias dañinas del hecho infractor consumado.
28. En lo que atañe a las atenuantes de la responsabilidad administrativa, se debe prestar atención a lo dispuesto en el numeral 2 del mismo artículo de la LPAG²⁰, en virtud del cual la aplicación de aquellas dependerá del reconocimiento expreso de la infracción, conjuntamente con los factores establecidos en la norma especial, el artículo 126 del Reglamento de la LPDP: El reconocimiento espontáneo, acompañado de acciones para su enmienda y colaboración con las acciones de la autoridad, factores que, de acuerdo con lo oportuno del reconocimiento y la efectividad de la enmienda (esto último de acuerdo a las situaciones mencionadas en el considerando anterior), pueden conllevar la reducción de la sanción hasta por debajo del rango previsto en la LPDP²¹.
29. Por supuesto, la efectividad de los actos de enmienda mencionados, de acuerdo con el objetivo de las normas de protección de datos personales y del procedimiento administrativo, dependerá de su capacidad de diluir la

¹⁹ **Artículo 257.- Eximentes y atenuantes de responsabilidad por infracciones**

1.- Constituyen condiciones eximentes de la responsabilidad por infracciones las siguientes:

(...)

f) La subsanación voluntaria por parte del posible sancionado del acto u omisión 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 255.

²⁰ **Artículo 257.- Eximentes y atenuantes de responsabilidad por infracciones**

(...)

2.- Constituyen condiciones atenuantes de la responsabilidad por infracciones las siguientes:

a) Si iniciado un procedimiento administrativo sancionador 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.

b) Otros que se establezcan por norma especial.

²¹ **Artículo 126.- Atenuantes.**

La colaboración con las acciones de la autoridad y el reconocimiento espontáneo de las infracciones acompañado de acciones de enmienda se considerarán atenuantes. Atendiendo a la oportunidad del reconocimiento y a las fórmulas de enmienda, la atenuación permitirá incluso la reducción motivada de la sanción por debajo del rango previsto en la Ley.

Resolución Directoral N° 2271-2023-JUS/DGTAIPD-DPDP

trascendencia y los efectos antijurídicos de la conducta infractora, reparando la situación al punto de acercarla lo más posible al estado anterior al hecho infractor.

- IV. **Primera cuestión previa: Sobre la vinculación entre el Informe de Instrucción y el pronunciamiento de esta dirección**
30. El artículo 254 de la LPAG establece como carácter fundamental del procedimiento administrativo sancionador, la separación entre la autoridad instructora y la autoridad sancionadora o resolutora:

“Artículo 254.- Carácteres del procedimiento sancionador

254.1 Para el ejercicio de la potestad sancionadora se requiere obligatoriamente haber seguido el procedimiento legal o reglamentariamente establecido caracterizado por:

1. Diferenciar en su estructura entre la autoridad que conduce la fase instructora y la que decide la aplicación de la sanción.
(...)"

31. Por su parte, el artículo 255 de dicha ley establece lo siguiente:

“Artículo 255.- Procedimiento sancionador

Las entidades en el ejercicio de su potestad sancionadora se ciñen a las siguientes disposiciones:

(...)

5. Concluida, de ser el caso, la recolección de pruebas, la autoridad instructora del procedimiento concluye determinando la existencia de una infracción y, por ende, la imposición de una sanción; o la no existencia de infracción. La autoridad instructora formula un informe final de instrucción en el que se determina, de manera motivada, las conductas que se consideren probadas constitutivas de infracción, la norma que prevé la imposición de sanción; y, la sanción propuesta o la declaración de no existencia de infracción, según corresponda.

Recibido el informe final, el órgano competente para decidir la aplicación de la sanción puede disponer la realización de actuaciones complementarias, siempre que las considere indispensables para resolver el procedimiento. El informe final de instrucción debe ser notificado al administrado para que formule sus descargos en un plazo no menor de cinco (5) días hábiles.”

32. De los artículos transcritos, se desprende que la separación de las dos autoridades, así como la previsión de ejercicio de actuaciones por parte de la autoridad sancionadora o resolutora, situaciones que implican la autonomía de criterio de cada una de ellas.
33. En tal sentido, la autoridad sancionadora o resolutora puede hacer suyos todos los argumentos, conclusiones y recomendaciones expuestos por la autoridad instructora, así como puede efectuar una distinta evaluación de los hechos comprobados o inclusive, cuestionar estos hechos o evaluar situaciones que, si bien fueron tomadas en cuenta al momento de efectuar la imputación, no se evaluaron de la misma manera al finalizar la instrucción.

Esta es una copia auténtica imprimible de un documento electrónico archivado por el Ministerio de Justicia y Derechos Humanos, aplicando lo dispuesto por el Art. 25 de D.S. 070-2013-PCM y la Tercera Disposición Complementaria Final del D.S. 026-2016-PCM. Su autenticidad e integridad pueden ser contrastadas a través de la siguiente dirección web: https://sgd.minjus.gob.pe/gesdoc_web/login.jsp e ingresando el Tipo de Documento, Número y Rango de Fechas de ser el caso o https://sgd.minjus.gob.pe/gesdoc_web/verifica.jsp e ingresando Tipo de Documento, Número, Remitente y Año, según corresponda.

Resolución Directoral N° 2271-2023-JUS/DGTAIPD-DPDP

34. Por tal motivo, la resolución que emita una autoridad sancionadora o resolutora, puede apartarse de las recomendaciones del informe final de instrucción o incluso cuestionar los hechos expuestos y su valoración, haciendo una evaluación diferente, teniendo en cuenta la su naturaleza no vinculante de dicho informe, sin que ello conlleve una vulneración de la predictibilidad o de la expectativa legítima del administrado, esta última que no encuentra asidero en la normativa referida al procedimiento administrativo.
35. Por supuesto, la divergencia de criterios mencionada, no puede implicar vulneraciones al debido procedimiento, como el impedir el derecho de defensa de los administrados, ni ampliar o variar los hechos imputados y su valoración como presuntas infracciones.

V. Segunda cuestión previa: Sobre los datos biométricos

36. El presente caso aborda situaciones relacionadas con el tratamiento de datos biométricos, incluidos estos en la definición de datos sensibles del numeral 5 del artículo 2 de la LPDP, por lo cual reciben una protección más fuerte y su tratamiento inadecuado puede constituir una infracción grave.
37. Para entender el motivo de esta protección reforzada, es preciso entender la particularidad de los datos biométricos, para lo cual se puede acudir a la definición del numeral 14 del artículo 4 del Reglamento del Parlamento Europeo y del Consejo, del 27 de abril de 2016 relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (en adelante, RGPD): *“datos personales obtenidos a partir de un tratamiento técnico específico, relativos a las características físicas, fisiológicas o conductuales de una persona física que permitan o confirmen la identificación única de dicha persona, como imágenes faciales o datos dactiloscópicos”*.
38. Al respecto, es importante tener en cuenta la distinción que el RGPD hace en su considerando 51, entre el dato biométrico en sí mismo y su soporte: *“El tratamiento de fotografías no debe considerarse sistemáticamente tratamiento de categorías especiales de datos personales, pues únicamente se encuentran comprendidas en la definición de datos biométricos cuando el hecho de ser tratadas con medios técnicos específicos permita la identificación o la autenticación unívocas de una persona física.”*
39. De lo anterior, se desprende que el concepto del dato biométrico se compone de dos características esenciales:
 - Son relativos a características físicas, fisiológicas (características y funcionamiento del cuerpo humano) o conductuales (acciones, movimientos o rasgos exteriorizados físicamente).
 - Son obtenidos por medio de un medio técnico específico
 - Permiten o confirman la identificación única de la persona
40. En tal sentido, el soporte de ciertos datos biométricos, como en el caso de las imágenes para el reconocimiento facial, son los denominados “patrones

Esta es una copia auténtica imprimible de un documento electrónico archivado por el Ministerio de Justicia y Derechos Humanos, aplicando lo dispuesto por el Art. 25 de D.S. 070-2013-PCM y la Tercera Disposición Complementaria Final del D.S. 026-2016-PCM. Su autenticidad e integridad pueden ser contrastadas a través de la siguiente dirección web: https://sgd.minjus.gob.pe/gesdoc_web/login.jsp e ingresando el Tipo de Documento, Número y Rango de Fechas de ser el caso o https://sgd.minjus.gob.pe/gesdoc_web/verifica.jsp e ingresando Tipo de Documento, Número, Remitente y Año, según corresponda.

Resolución Directoral N° 2271-2023-JUS/DGTAIPD-DPDP

biométricos", los cuales son obtenidos sometiendo al procedimiento técnico pertinente la imagen previamente extraída, a fin de tener un elemento que identifique indubitablemente a la persona; lo que implica que sobre el dato biométrico, la primera acción recopilatoria se efectúa desde la imagen previamente tomada.

41. De lo expuesto, se deducen razones por las cuales un dato biométrico debe considerarse sensible, pues más allá de que el uso de medios técnicos especiales, de alcance no ordinario para toda aquella persona que realice tratamiento de datos personales, este tipo de datos contiene información sobre elementos tangibles, escrutables, vinculadas al ámbito más íntimo de la persona, como es la composición física y más involucrado, el funcionamiento de su cuerpo (fisiología), que puede abarcar cuestiones bioquímicas, neurológicas, relativas a la locomoción y a la determinación de la personalidad, cuyo manejo abarca riesgos variados, desde los concernientes a la suplantación de identidad hasta la predeterminación (en atención a la unicidad del dato biométrico, correspondiente solo a una persona perpetuamente) y posibilidad de interferencia en los procesos biológicos de su titular.

VI. Tercera cuestión previa: Sobre la supuesta contravención a los principios de legalidad y tipicidad de la potestad sancionadora de la administración

42. En su comunicación de descargo de junio, la administrada señala que en este procedimiento sancionador se vulneran principios de la potestad sancionadora de la administración, previsto en el 248 de la LPAG (Legalidad y Tipicidad), inobservado al emprender un procedimiento sancionador sobre una tipificación establecida reglamentariamente y no por una norma de rango de ley.
43. El análisis de este argumento requiere que esta Dirección haga referencia tanto al principio de Legalidad como al de Tipicidad, ambos aplicables a la potestad sancionadora, contenidos en el artículo 248 de la LPAG.
44. Del mencionado principio de Legalidad derivan dos requisitos: La de atribuir potestad sancionadora a las entidades solamente por medio de normas con rango de ley; y que por normas de este rango, se prevean las consecuencias administrativas que a título de sanción se aplicarían a un infractor, vale decir, las medidas represivas, de gravamen, cancelación de derechos, inhabilitaciones, así como los márgenes de estos (sanciones mínimas y máximas, o plazos de inhabilitación mínimos y máximos), como señala Morón²²; lo cual implica que a través de la ley se establezca, de forma genérica, lo que sucede en caso de que las disposiciones normativas no sean acatadas por los administrados.
45. Por su parte, el principio de Tipicidad establece como regla o situación ordinaria, que la tipificación de las infracciones, esto es, la predeterminación de las conductas específicas que afectan a cada uno de los bienes jurídicos protegidos por una norma y que por ello, son sancionables.

²² MORÓN URBINA, Juan Carlos: "Comentarios a la Ley del Procedimiento Administrativo General". Décimo quinta edición. Lima, Gaceta Jurídica, 2020, tomo II, p. 400 a 401.

Resolución Directoral N° 2271-2023-JUS/DGTAIPD-DPDP

46. A su vez, este principio establece que la tipificación se realiza por norma con rango de ley, salvo que a través de una norma de este rango se permita expresamente la tipificación por vía reglamentaria.
47. Al respecto, expone la administrada en sus argumentos, que el requerimiento de tipicidad con rango de ley es desarrollado en la sentencia del Tribunal Constitucional del 24 de abril de 2019, recaída en el expediente N° 20-2015-AI, en lo que concierne a la inconstitucionalidad del artículo 46 de la Ley N°27785, Ley Orgánica del Sistema Nacional de Control y de la Contraloría General de la República, modificada por la Ley N° 29622 (en adelante, LOCGR), que dispone lo siguiente:

“46. Por tanto, al desarrollar normas con rango de ley, los reglamentos no pueden desnaturalizarlos creando infracciones sin una debida base legal. Admitir lo contrario implicaría aceptar una desviación de la potestad reglamentaria y vaciar de contenido los principios de legalidad y tipicidad que guardan una estrecha relación con el derecho fundamental al debido proceso.”
48. Para determinar el grado de generalidad de tal interpretación, vale decir, lo extensible que puede ser a otras normas que ostenten caracteres sancionadores, es necesario entender el alcance de lo dispuesto por el Tribunal Constitucional en dicho caso, para lo cual se requiere conocer la norma cuya constitucionalidad que se cuestionó y su marco normativo.
49. Como se señala en el considerando 47 de la misma sentencia, el primer párrafo del artículo 40 de la Constitución Política del Perú²³ delimita el ámbito de la reserva de ley en lo que concierne a la función pública y al sistema nacional de control, las responsabilidades del servidor público que lleva aparejada y por consiguiente, la determinación de las infracciones.
50. Entonces, siguiendo lo mencionado en el considerando 48 de la sentencia analizada²⁴, la disposición de la reserva de ley derivada de la norma constitucional requiere que la norma legal de aquella materia (función pública y sistema nacional de control) defina en sí misma, con total certeza, tales cuestiones, incluyendo la tipificación de las infracciones.

²³ **Artículo 40.- Carrera Administrativa**

La ley regula el ingreso a la carrera administrativa, y los derechos, deberes y responsabilidades de los servidores públicos. No están comprendidos en dicha carrera los funcionarios que desempeñan cargos políticos o de confianza. Ningún funcionario o servidor público puede desempeñar más de un empleo o cargo público remunerado, con excepción de uno más por función docente.

No están comprendidos en la función pública los trabajadores de las empresas del Estado o de sociedades de economía mixta.

Es obligatoria la publicación periódica en el diario oficial de los ingresos que, por todo concepto, perciben los altos funcionarios, y otros servidores públicos que señala la ley, en razón de sus cargos.

²⁴ **Sentencia del Tribunal Constitucional recaída en el expediente N° 0020-2015-AI**

“48. Dicha disposición establece una reserva de ley para que, en principio, sea el legislador quien se encargue de regular el ingreso a la carrera administrativa así como los deberes y responsabilidades de los servidores públicos. En consecuencia, si bien las normas legales que desarrollan esos temas pueden ser precisadas o complementadas por reglamentos, no es constitucionalmente admisible que éstos desborden dichas normas legales refiriéndose a asuntos que no han sido regulados en ellas con un grado mínimo de claridad o precisión.”

Resolución Directoral N° 2271-2023-JUS/DGTAIPD-DPDP

51. Por tal motivo, el Tribunal Constitucional efectúa el análisis de los considerandos 49 al 54 de la misma sentencia, revisando el contenido de cada párrafo del artículo 46 de la LOCGR, a fin de constatar si dicho artículo, en sí mismo, tipifica certeramente las infracciones.
52. Una situación distinta es la de la LPDP, que no se encuentra sujeta a una disposición similar a la del artículo 40 de la Constitución Política del Perú, basando su objeto es el de garantizar el derecho fundamental a la protección de los datos personales contenido en el numeral 6 del artículo 2 de dicha norma suprema.
53. Para alcanzar tal finalidad, dicha ley contiene una lista enumerativa de principios rectores, los cuales constituyen pautas que los responsables del tratamiento de datos personales deben seguir para llevarlo a cabo y para el ejercicio de los derechos que dicha ley premune a las personas naturales, como titulares de los datos personales.
54. A fin de garantizar la observancia de tales principios y derechos, se establece en la normativa de protección de datos personales, obligaciones específicas que deben ser cumplidas por los responsables del tratamiento, siendo que en caso de su incumplimiento, se incurre en infracción.
55. Entonces, a diferencia de las normas del sistema nacional de control (la LOCGR), la normativa de protección de datos personales no cuenta con una norma de nivel constitucional que ciña su estructura ni su contenido; solo obedece al objetivo de garantizar una el derecho fundamental a la protección de datos personales, teniendo la libertad de desarrollar a través de la LPDP y su reglamento, las obligaciones y las infracciones que derivan de su incumplimiento.
56. De otro lado, el Pleno del Tribunal Constitucional, en su sentencia para los expedientes N° 0014-2014-PI/TC, N° 0016- 2014-PI/TC, N° 0019-2014-P1/TC y N° 0007-2015-PI/TC, referidas a la Ley Universitaria, indicó respecto de tales principios, lo siguiente: *“En esta materia aplica entonces aquella reserva de ley relativa. Por ende, no resulta inconstitucional que se derive al reglamento la tipificación de las infracciones, en tanto se ha fijado en la ley las conductas sancionables y la escala y los tipos de sanción. (...) cabe añadir que si se regula una actividad con miras a garantizar la calidad del servicio público, resulta necesario dotar al organismo supervisor de las herramientas necesarias para corregir las infracciones que se adviertan en su ámbito específico”*.
57. Circunstancias similares a las analizadas por el máximo intérprete de la Constitución Política del Perú, habilitaron a que la normativa especial de protección de datos personales, en razón de la especialización de su materia, permita que la LPDP acude a la colaboración reglamentaria por habitación legal, siendo posible que las disposiciones reglamentarias contemplen los supuestos típicos, o infracciones, con sus correspondientes sanciones; siempre que se respeten las previsiones de lo contemplado en la ley, que deberá contener los elementos básicos cuyo desarrollo se hará a través de la remisión al reglamento
58. Respecto de la especialización de la materia, es necesario resaltar también que la LPDP, así como su normativa complementaria (el Reglamento de la LPDP) tiene

Esta es una copia auténtica imprimible de un documento electrónico archivado por el Ministerio de Justicia y Derechos Humanos, aplicando lo dispuesto por el Art. 25 de D.S. 070-2013-PCM y la Tercera Disposición Complementaria Final del D.S. 026-2016-PCM. Su autenticidad e integridad pueden ser contrastadas a través de la siguiente dirección web: https://sgd.minjus.gob.pe/gesdoc_web/login.jsp e ingresando el Tipo de Documento, Número y Rango de Fechas de ser el caso o https://sgd.minjus.gob.pe/gesdoc_web/verifica.jsp e ingresando Tipo de Documento, Número, Remitente y Año, según corresponda.

Resolución Directoral N° 2271-2023-JUS/DGTAIPD-DPDP

como objeto es el de garantizar un derecho fundamental, que es el de la protección de los datos personales, contenido en el numeral 6 del artículo 2 de la Constitución Política del Perú.

59. Para alcanzar tal finalidad, la LPDP contiene una lista enumerativa de principios rectores, los cuales constituyen pautas que los responsables del tratamiento de datos personales deben seguir para llevarlo a cabo y para garantizar el ejercicio de los derechos que dicha ley premune a las personas naturales, como titulares de los datos personales.
60. A fin de garantizar la observancia de tales principios y derechos, se establece en la normativa de protección de datos personales, obligaciones específicas que deben ser cumplidas por los responsables del tratamiento, siendo que en caso de su incumplimiento, se incurre en alguna de las infracciones, las que son conductas específicas contenidas en el artículo 132 del Reglamento de la LPDP.
61. Ahora bien, la sentencia de la Sala Civil Permanente recaída en la Apelación N° 5440-2019, señalada por la administrada, establece que deben entenderse complementariamente los mencionados principios, en mérito de lo cual se acoge una reserva de ley para determinar las conductas sancionables administrativamente, que deberán estar tipificadas de manera clara, específica, precisa e inequívoca.
62. El considerando séptimo de dicha sentencia, hace referencia a la excepción de la reserva de ley, por la cual “se permite el desarrollo mediante reglamento además de la habilitación legal para la tipificación; en el primer supuesto de excepción se aplica el principio de cobertura legal, en el cual la norma legal constituye o define la conducta sancionable, y el reglamento desarrolla la ley con la finalidad de identificar las conductas y sanciones que originalmente han sido establecidos por ella, por lo que la ley constituye el límite del reglamento, que no puede ir más allá de lo establecido legalmente, ni constituir conductas sancionables no previstas en la ley; en el segundo supuesto de excepción, la norma legal autoriza la tipificación de conductas sancionables mediante reglamento”.
63. Entonces, la sentencia reseñada admite a la excepción de la reserva de ley que en su momento, el Tribunal Constitucional acogió, permitiendo que mediante reglamento se desarrolle las conductas sancionables, sin crear nuevos supuestos infractores ni extralimitarse de lo que las normas legales impongan.
64. Se aprecia en el caso de la LPDP, que cumple con el requisito de reserva de ley para atribuir el ejercicio de potestad sancionadora (y sus funciones, como la fiscalización, instrucción e imposición de sanciones) y de imponer sanciones ante el incumplimiento de sus disposiciones, a la Autoridad Nacional de Protección de Datos Personales, en observancia del principio de legalidad, al aplicarse lo establecido en sus artículos 32, 33 y 39:

“Artículo 32. Órgano competente y régimen jurídico

(...)

Corresponde a la Autoridad Nacional de Protección de Datos Personales realizar todas las acciones necesarias para el cumplimiento del objeto y

Esta es una copia auténtica imprimible de un documento electrónico archivado por el Ministerio de Justicia y Derechos Humanos, aplicando lo dispuesto por el Art. 25 de D.S. 070-2013-PCM y la Tercera Disposición Complementaria Final del D.S. 026-2016-PCM. Su autenticidad e integridad pueden ser contrastadas a través de la siguiente dirección web: https://sgd.minjus.gob.pe/gesdoc_web/login.jsp e ingresando el Tipo de Documento, Número y Rango de Fechas de ser el caso o https://sgd.minjus.gob.pe/gesdoc_web/verifica.jsp e ingresando Tipo de Documento, Número, Remitente y Año, según corresponda.

Resolución Directoral N° 2271-2023-JUS/DGTAIPD-DPDP

demás disposiciones de la presente Ley y de su reglamento. Para tal efecto, goza de potestad sancionadora, de conformidad con la Ley 27444, Ley del Procedimiento Administrativo General, o la que haga sus veces, así como de potestad coactiva, de conformidad con la Ley 26979, Ley de Procedimiento de Ejecución Coactiva, o la que haga sus veces.

(...)

Artículo 33. Funciones de la Autoridad Nacional de Protección de Datos Personales

La Autoridad Nacional de Protección de Datos Personales ejerce las funciones administrativas, orientadoras, normativas, resolutivas, fiscalizadoras y sancionadoras siguientes:

(...)

20. Iniciar fiscalizaciones de oficio o por denuncia de parte por 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.

(...)"

65. En lo concerniente al establecimiento de un supuesto de ilicitud (contrarios a la normativa) y a la tipificación de conductas específicas que encarnen tal ilicitud (infracciones), se debe analizar las normas del Título VII de dicha ley:

“TÍTULO VII

INFRACCIONES Y SANCIONES ADMINISTRATIVAS

Artículo 37. Procedimiento sancionador

El procedimiento sancionador se inicia de oficio, por la Autoridad Nacional de Protección de Datos Personales o por denuncia de parte, ante la presunta comisión de actos contrarios a lo dispuesto en la presente Ley o en su reglamento, sin perjuicio del procedimiento seguido en el marco de lo dispuesto en el artículo 24.

Artículo 38. Tipificación de infracciones

Las infracciones se clasifican en leves, graves y muy graves, las cuales son tipificadas vía reglamentaria, de acuerdo a lo establecido en el numeral 4) del artículo 230 de la Ley N° 27444, Ley del Procedimiento Administrativo General, mediante Decreto Supremo con el voto aprobatorio del Consejo de Ministros.

(...)"

66. De lo transscrito, se aprecia que la LPDP, en su artículo 37 establece una situación sancionable general: La comisión de actos contrarios a la LPDP y su reglamento; dejando la tipificación exhaustiva y específica al reglamento, como dispone el artículo 38 de dicha ley, que clasifica a las infracciones según su gravedad.
67. En tales artículos, la LPDP equipara el bien jurídico a proteger (preservar el derecho fundamental del numeral 6 del artículo 2 de la Constitución Política del Perú) con el cumplimiento del íntegro de sus disposiciones, siendo las situaciones contrarias a dicha ley y su reglamento, una conducta infractora sancionable, cuyos caracteres se especifican en su reglamento, al identificar tales conductas de forma exhaustiva, sin “crear” supuestos jurídicos que carezcan de base en la LPDP.

Esta es una copia auténtica imprimible de un documento electrónico archivado por el Ministerio de Justicia y Derechos Humanos, aplicando lo dispuesto por el Art. 25 de D.S. 070-2013-PCM y la Tercera Disposición Complementaria Final del D.S. 026-2016-PCM. Su autenticidad e integridad pueden ser contrastadas a través de la siguiente dirección web: https://sgd.minjus.gob.pe/gesdoc_web/login.jsp e ingresando el Tipo de Documento, Número y Rango de Fechas de ser el caso o https://sgd.minjus.gob.pe/gesdoc_web/verifica.jsp e ingresando Tipo de Documento, Número, Remitente y Año, según corresponda.

Resolución Directoral N° 2271-2023-JUS/DGTAIPD-DPDP

68. Dicha tipificación, que especifica los hechos que configuran la conducta general de incumplimiento, se desarrolla en el artículo 132 del Reglamento de la LPDP, sirviéndose de lo establecido en el artículo 38 de dicha ley.
69. Con ello, se configura la observancia de los principios de legalidad y tipicidad de la potestad sancionadora administrativa del artículo 248 de la LPAG, al ceñirse la normativa de protección de datos personales a la excepción establecida, así como estableciendo claramente las competencias para el ejercicio de dicha potestad.
70. Se debe remarcar que la tipificación reglamentaria no constituye una reiteración o añadidura al sentido del artículo 37 de la LPDP, como puede suceder, por ejemplo, si se incluyen algún supuesto que consista exclusivamente en el incumplimiento de normas relativas a otros derechos fundamentales que no desarrolla esta ley; tampoco desnaturalizan el objeto de dicho artículo, que es preservar el cumplimiento de las disposiciones de dicha ley y su reglamento.
71. En consecuencia, esta Dirección aprecia que la tipificación del artículo 132 del Reglamento de la LPDP se está aplicando con la especificidad suficiente para otorgar certeza sobre cada hecho ilícito, en observancia los principios mencionados del artículo 248 de la LPAG, por lo que cualquier acto administrativo que se emita respecto de ella estará premunido de validez.

VII. Cuarta cuestión previa: Sobre el principio de *Non bis in ídem* y el concurso de infracciones

72. En su escrito de descargos del 8 de noviembre de 2023, la administrada solicitó la aplicación del principio de *Non bis in ídem* puesto que concluir que se efectuó el tratamiento desproporcionado de datos, implicaría que también se considere que hubo un tratamiento sin consentimiento de los mismos datos.
73. En primer término, es importante resaltar que el numeral 11 del artículo 248 de la LPAG, comprende el principio de *Non bis in ídem*, el cual prohíbe el sucesivo o simultáneo sometimiento al reproche administrativo por hechos infractores, respecto de los cuales exista identidad del sujeto, hecho y fundamento.
74. Es pertinente reseñar las dos vertientes de dicho principio, de acuerdo con lo desarrollado por el Tribunal Constitucional, en el criterio desarrollado en las sentencias de los expedientes N° 2050-2002-AA/TC y N° 2868-2004/TC:
 - Versión sustantiva o material: Prohibición de sancionar dos veces por un mismo hecho, llevado a cabo por el mismo sujeto, tipificado como infracción por el mismo fundamento jurídico (la misma norma).
 - Versión procesal: Prohibición de establecer dos procedimientos distintos por el mismo hecho, llevado a cabo por el mismo sujeto, tipificado como infracción por el mismo fundamento jurídico (la misma norma), a fin de evitar la duplicidad.
75. Sin perjuicio de lo alegado por la administrada, esta Dirección considera pertinente evaluar también la posibilidad de un concurso de infracciones, de acuerdo con el numeral 6 del artículo 248 de la LPAG:

Esta es una copia auténtica imprimible de un documento electrónico archivado por el Ministerio de Justicia y Derechos Humanos, aplicando lo dispuesto por el Art. 25 de D.S. 070-2013-PCM y la Tercera Disposición Complementaria Final del D.S. 026-2016-PCM. Su autenticidad e integridad pueden ser contrastadas a través de la siguiente dirección web: https://sgd.minjus.gob.pe/gesdoc_web/login.jsp e ingresando el Tipo de Documento, Número y Rango de Fechas de ser el caso o https://sgd.minjus.gob.pe/gesdoc_web/verifica.jsp e ingresando Tipo de Documento, Número, Remitente y Año, según corresponda.

Resolución Directoral N° 2271-2023-JUS/DGTAIPD-DPDP

“Artículo 248.- Principios de la potestad sancionadora administrativa
La potestad sancionadora de todas las entidades está regida adicionalmente por los siguientes principios especiales:

(...)

6. Concurso de Infracciones. - Cuando una misma conducta califique como más de una infracción se aplicará la sanción prevista para la infracción de mayor gravedad, sin perjuicio que puedan exigirse las demás responsabilidades que establezcan las leyes.”

76. Según lo transcrita, la administración tiene la obligación, en casos de concurso de infracciones, de aplicar la sanción por la infracción que considere más grave, sin que ello necesariamente deba determinarse solo por lo gravoso de la sanción, como bien señala Morón²⁵, sino por diversas cuestiones como la trascendencia de la norma infringida, de las obligaciones incumplidas o su influencia en los derechos de terceros.
77. En el presente caso, ambas imputaciones tienen en común la discusión de la legitimidad de la recopilación, empleo y almacenamiento permanente de los patrones biométricos faciales obtenidos desde una imagen facial tomada para el uso del libro de reclamaciones virtual.
78. La discusión de la primera imputación reside en la necesidad y utilidad de los mencionados datos biométricos respecto de la finalidad reconocida para su recopilación (debida autenticación de la identidad de los usuarios), vale decir que se calificará su legitimidad según sea necesario y suficiente su tratamiento para ello, siendo ilegítimo este en caso de resultar excesivo.
79. En cambio, la segunda imputación está relacionada a la solicitud de consentimiento para un tratamiento distinto, que es el almacenamiento de los datos biométricos recopilados para una futura posible identificación, lo que implica evaluar una base de legitimidad distinta.
80. Ahora bien, en el caso bajo análisis, el mero almacenamiento de los patrones biométricos faciales, más allá de que se empleen efectivamente para la verificación de identidad, requiere de la obtención del consentimiento válido, de acuerdo con lo dispuesto en el artículo 13 de la LPDP y artículo 12 del Reglamento de dicha ley.
81. Al desplegarse en este caso un proceso de tratamiento de datos biométricos que implican los presuntos incumplimientos de dos de los principios de la LPDP, será necesario determinar, de acuerdo con los hechos si se configura un concurso de infracciones y de ser el caso, aplicar la multa de mayor cuantía entre las dos infracciones graves según lo tipificado en el artículo 132 del Reglamento de la LPDP, recurriendo también a la Metodología para el Cálculo de Multas en materia de Protección de Datos Personales, aprobado mediante la Resolución Ministerial N° 0326-2020-JUS (en adelante, Metodología para el Cálculo de Multas)²⁶.

²⁵ MORÓN URBINA, Juan Carlos: “Comentarios a la Ley del Procedimiento Administrativo General”. Décimo quinta edición. Lima, Gaceta Jurídica, 2020, tomo II, p. 430.

²⁶ Documento disponible en: <https://bni.minjus.gob.pe/bni/>.

Resolución Directoral N° 2271-2023-JUS/DGTAIPD-DPDP

VIII. Cuestiones en discusión

82. Para emitir pronunciamiento en el presente caso, se debe determinar lo siguiente:

82.1 Si la administrada es responsable por:

- Haber realizado el tratamiento desproporcionado de los datos personales de quienes generan un reclamo a través del libro de reclamaciones virtual publicado en su sitio web, al recopilar imágenes del DNI y de la imagen facial para tratarla con medios técnicos específicos para identificación a través de la validación biométrica, los cuales no son adecuados, necesarios ni pertinentes para la finalidad de identificar plenamente al reclamante, incumpliendo lo dispuesto en los artículos 7 y numeral 3 del artículo 28 de la LPDP.
- Haber realizado el tratamiento de los datos personales de quienes generan un reclamo, al almacenar el dato biométrico de la imagen facial en una base de datos propia, sin obtener válidamente el consentimiento de sus titulares, incumpliendo con la obligación establecida en los artículos 5 y 13 de la LPDP, así como de los artículos 7 y 12 de su reglamento.

82.2 En el supuesto de resultar responsable, si debe aplicarse la exención de responsabilidad por la subsanación de la infracción, según lo previsto en el numeral 1 del artículo 257 de la LPAG, o las atenuantes, de acuerdo con lo dispuesto en el artículo 126 del Reglamento de la LPDP, en consonancia con el numeral 2 del artículo 257 de la LPAG.

82.3 Determinar la multa que corresponde imponer, tomando en consideración los criterios de graduación del numeral 3) del artículo 248 de la LPAG.

IX. Análisis de las cuestiones en discusión

Sobre el presunto tratamiento de datos personales biométricos (imagen facial) sin haber cumplido con el principio de proporcionalidad

83. La Constitución Política del Perú, establece en el artículo 2, numeral 6, que toda persona tiene derecho "a que los servicios informáticos, computarizados o no, públicos o privados, no suministren informaciones que afecten la intimidad personal y familiar", es decir toda persona tiene derecho a la autodeterminación informativa y, por lo tanto, a la protección de sus datos personales.

84. El Tribunal Constitucional, máximo intérprete de la Constitución Política del Perú, ha definido el derecho a la autodeterminación informativa (contenido en el numeral mencionado en el considerando precedente) en la sentencia del expediente N° 4739-2007-PHD/TC de la siguiente forma:

"el derecho a la autodeterminación informativa consiste en la serie de facultades que tiene toda persona para ejercer control sobre la información personal que le concierne, contenida en registros ya sean públicos, privados

Esta es una copia auténtica imprimible de un documento electrónico archivado por el Ministerio de Justicia y Derechos Humanos, aplicando lo dispuesto por el Art. 25 de D.S. 070-2013-PCM y la Tercera Disposición Complementaria Final del D.S. 026-2016-PCM. Su autenticidad e integridad pueden ser contrastadas a través de la siguiente dirección web: https://sgd.minjus.gob.pe/gesdoc_web/login.jsp e ingresando el Tipo de Documento, Número y Rango de Fechas de ser el caso o https://sgd.minjus.gob.pe/gesdoc_web/verifica.jsp e ingresando Tipo de Documento, Número, Remitente y Año, según corresponda.

Resolución Directoral N° 2271-2023-JUS/DGTAIPD-DPDP

o informáticos, a fin de enfrentar las posibles extralimitaciones de los mismos. Se encuentra estrechamente ligado a un control sobre la información, como una autodeterminación de la vida íntima, de la esfera personal. Mediante la autodeterminación informativa se busca proteger a la persona en sí misma, no únicamente en los derechos que conciernen a su esfera personalísima, sino a la persona en la totalidad de ámbitos; por tanto, no puede identificarse con el derecho a la intimidad, personal o familiar, ya que mientras éste protege el derecho a la vida privada, el derecho a la autodeterminación informativa busca garantizar la facultad de todo individuo de poder preservarla ejerciendo un control en el registro, uso y revelación de los datos que le conciernen (...). En este orden de ideas, el derecho a la autodeterminación informativa protege al titular del mismo frente a posibles abusos o riesgos derivados de la utilización de los datos, brindando al titular afectado la posibilidad de lograr la exclusión de los datos que considera 'sensibles' y que no deben ser objeto de difusión ni de registro; así como le otorga la facultad de poder oponerse a la transmisión y difusión de los mismos"

85. En esa línea, el ejercicio del derecho fundamental se fundamenta en la limitación sobre la cantidad de datos personales objeto de tratamiento y de las actividades de tratamiento a realizar, limitándose a lo necesario y útil para alcanzar una finalidad, la cual debe ser determinada, explícita para el titular de los datos personales y lícita.
86. Estando predeterminada y siendo reconocible la finalidad del tratamiento para el titular de los datos personales, este deberá abarcar solo lo adecuado, relevante y no excesivo para alcanzar tal finalidad, no debiendo recopilarse más datos personales de los necesarios, ni realizar actividades de tratamiento que no contribuyan ni se relacionen con tal objetivo, mucho menos mantener estas últimas actividades por períodos en los que ya no sea necesario efectuar el tratamiento, por haberse cumplido con la finalidad, limitándose el tiempo de su conservación a este cumplimiento.
87. Tales requisitos de licitud del tratamiento se traducen en los principios de Finalidad y Proporcionalidad de los artículos 6 y 7 de la LPDP, transcritos a continuación:

"Artículo 6. Principio de finalidad

Los datos personales deben ser recopilados para una finalidad determinada, explícita y lícita. El tratamiento de los datos personales no debe extenderse a otra finalidad que no haya sido la establecida de manera inequívoca como tal al momento de su recopilación, excluyendo los casos de actividades de valor histórico, estadístico o científico cuando se utilice un procedimiento de disociación o anonimización.

Artículo 7. Principio de proporcionalidad

Todo tratamiento de datos personales debe ser adecuado, relevante y no excesivo a la finalidad para la que estos hubiesen sido recopilados."

Esta es una copia auténtica imprimible de un documento electrónico archivado por el Ministerio de Justicia y Derechos Humanos, aplicando lo dispuesto por el Art. 25 de D.S. 070-2013-PCM y la Tercera Disposición Complementaria Final del D.S. 026-2016-PCM. Su autenticidad e integridad pueden ser contrastadas a través de la siguiente dirección web: https://sgd.minjus.gob.pe/gesdoc_web/login.jsp e ingresando el Tipo de Documento, Número y Rango de Fechas de ser el caso o https://sgd.minjus.gob.pe/gesdoc_web/verifica.jsp e ingresando Tipo de Documento, Número, Remitente y Año, según corresponda.

Resolución Directoral N° 2271-2023-JUS/DGTAIPD-DPDP

88. En virtud de dichos principios, la LPDP establece la siguiente obligación:

“Artículo 28. Obligaciones

El titular y el encargado de tratamiento de datos personales, según sea el caso, tienen las siguientes obligaciones:

(...)

3. Recopilar datos personales que sean actualizados, necesarios, pertinentes y adecuados, con relación a finalidades determinadas, explícitas y lícitas para las que se hayan obtenido.”

89. Dichas obligaciones, entonces, determinan dos mandatos:

- Por un lado, limitar la recopilación y conservación de datos personales y las actividades de tratamiento, solo a lo necesario para cumplir con la finalidad determinada y reconocible por el titular de los datos personales.
- Una vez cumplida tal finalidad o extintas las condiciones que hacían necesario el tratamiento, adoptar medidas que eviten la continuidad del mismo, como la supresión de los datos personales o el bloqueo, en los casos en que exista una obligación normativa de conservarlos.

90. Establecido ello, corresponde resaltar la trascendencia de estos principios en el tratamiento de datos personales sensibles, en la medida que la minimización de la cantidad de datos personales y de acciones de tratamiento contribuyen a evitar situaciones riesgosas que, con esta clase de datos, conllevan un riesgo mayor para sus titulares.

91. A su vez, este riesgo mayor que entraña el tratamiento de datos sensibles, en el presente caso, conlleva una mayor responsabilidad, por desarrollarse bajo la responsabilidad de una entidad que emplea un procedimiento especial para su obtención y la singularidad del dato obtenido, cuyo tratamiento inadecuado o no autorizado entraña riesgos que superan la sola confidencialidad de la información.

92. En la denuncia presentada, se detalló que para presentar un reclamo virtual, la administrada requiere a través de su sistema, imágenes de su DNI y su rostro, que no serían exigidos por el artículo 5 del Reglamento del Libro de Reclamaciones, situación que propiciaría que incluso, personas sin productos financieros se vean obligada a aceptar el tratamiento de sus imágenes; a su vez, la denunciante detalló que para la interposición de un segundo reclamo, se le solicitó la misma información.

93. La administrada, por su parte, informa que el objeto de solicitar la imagen facial es la validación de la identidad de las personas, la cual se hace contrastando la que se toma al momento (tiempo real), a través de sus patrones biométricos con la que se obtiene del RUIPN del Reniec, al cual tiene acceso en virtud de un acuerdo interinstitucional; siendo este procedimiento obligatorio, en observancia de lo dispuesto en el articulado del Reglamento de la SBS, obligando a adoptar medidas que reduzcan la posibilidad de suplantar la identidad.

Resolución Directoral N° 2271-2023-JUS/DGTAIPD-DPDP

94. Comunica la administrada también que cuenta con una base de datos denominada "BIOM" en el que almacena las imágenes, para efectuar contrastes posteriores, cada vez que el cliente efectúe alguna reclamación digital.
95. Deja claro la administrada que la finalidad de la recopilación de las imágenes de los rostros de los usuarios de su libro de reclamaciones virtual es la correcta validación de identidad, siguiendo los estándares que la normativa sectorial establece en el Reglamento de la SBS, que se transcribe a continuación:

"Artículo 2. Definiciones

Para efectos de la aplicación del presente Reglamento deben considerarse las siguientes definiciones

(...)

j) Factores de autenticación de usuario: Aquellos factores empleados para verificar la identidad de un usuario, que pueden corresponder a las siguientes categorías:

- Algo que solo el usuario conoce.*
- Algo que solo el usuario posee.*
- Algo que el usuario es, que incluye las características biométricas.*

(...)

Artículo 18. Enrolamiento del usuario en servicios provistos por canal digital

18.1 El enrolamiento de un usuario en un canal digital requiere por lo menos:

a) Verificar la identidad del usuario y tomar las medidas necesarias para reducir la posibilidad de suplantación de identidad, lo que incluye el uso de dos factores independientes de categorías diferentes, según el literal j) del artículo 2 de este Reglamento.

b) Generar las credenciales y asignarlas al usuario.

(...)

Artículo 19. Autenticación reforzada para operaciones por canal digital

Se requiere de autenticación reforzada para aquellas acciones que puedan originar operaciones fraudulentas u otro abuso del servicio en perjuicio del cliente, como las operaciones a través de un canal digital que impliquen pagos o transferencia de fondos a terceros, registro de un beneficiario de confianza, modificación en los productos de seguro ahorro/inversión contratados, la contratación de un producto o servicio, modificación de límites y condiciones, para lo cual se requiere:

- a) Utilizar una combinación de factores de autenticación, según el literal j) del artículo 2 del presente Reglamento que, por lo menos, correspondan a dos categorías distintas y que sean independientes uno del otro.*
- b) Generar un código de autenticación mediante métodos criptográficos, a partir de los datos específicos de cada operación, el cual debe utilizarse por única vez.*
- c) Cuando la operación sea exitosa, notificar los datos de la operación al usuario."*

96. La administrada a su vez, hace referencia al artículo 5 del Reglamento del Libro de Reclamaciones, que contiene los siguientes términos:

Esta es una copia auténtica imprimible de un documento electrónico archivado por el Ministerio de Justicia y Derechos Humanos, aplicando lo dispuesto por el Art. 25 de D.S. 070-2013-PCM y la Tercera Disposición Complementaria Final del D.S. 026-2016-PCM. Su autenticidad e integridad pueden ser contrastadas a través de la siguiente dirección web: https://sgd.minjus.gob.pe/gesdoc_web/login.jsp e ingresando el Tipo de Documento, Número y Rango de Fechas de ser el caso o https://sgd.minjus.gob.pe/gesdoc_web/verifica.jsp e ingresando Tipo de Documento, Número, Remitente y Año, según corresponda.

Resolución Directoral N° 2271-2023-JUS/DGTAIPD-DPDP

“Artículo 5.- Características de la Hoja de Reclamación

Cada Hoja de Reclamación de naturaleza física deberá contar con tres (03) hojas desglosables, una (01) original y dos (02) autocopiativas; la original será obligatoriamente entregada al consumidor al momento de dejar constancia de su queja o reclamo, la primera copia quedará en posesión del proveedor y la segunda copia será remitida o entregada al INDECOPI cuando sea solicitada por éste.

Las Hojas de Reclamaciones, tanto de los Libros de Reclamaciones de naturaleza física como virtual, deberán contener como mínimo la información consignada en el formato del Anexo I del presente Reglamento. Dicha información incluye:

- Denominación que permita identificar claramente a la Hoja de Reclamación como tal, incluyendo la razón social del proveedor, número de Registro Único de Contribuyentes y dirección del establecimiento comercial, los cuales estarán impresos o deberán aparecer por defecto, según corresponda.*
- Numeración correlativa impresa o que deberá aparecer por defecto*
- Código de identificación impreso, o que deberá aparecer por defecto, de conformidad con lo establecido en el Artículo 8, según corresponda.*
- Fecha del reclamo o queja.*
- Nombre, domicilio, número de documento de identidad, teléfono y correo electrónico del consumidor.*
- Nombre, domicilio, teléfono y correo electrónico de uno de los padres o representantes del consumidor, en caso se trate de un menor de edad.*
- Identificación del producto o servicio contratado.*
- Monto del producto o servicio contratado objeto del reclamo.*
- Detalle de la reclamación o queja.*
- Pedido concreto del consumidor respecto al hecho que motiva el reclamo o queja.*
- Espacio físico para que el proveedor anote las observaciones y acciones adoptadas con respecto a la queja o reclamo.*
- Firma del Consumidor en el caso del Libro de Reclamaciones físico.*
- Nombre del destinatario de la hoja de reclamaciones impreso (consumidor, proveedor, INDECOPI)*

En caso que el consumidor no consigne como mínimo su nombre, DNI, domicilio o correo electrónico, fecha del reclamo o queja y el detalle de los mismos, estos se considerarán como no presentados.”

97. De la normativa sectorial emitida por la SBS, se deduce que para la autenticación de la identidad de los usuarios de servicios digitales, se tienen tres tipos de factores para su verificación, de los cuales pueden ser utilizados dos combinados en los casos de enrolamiento del usuario, cuando no se opte por la asignación de credenciales, o en los casos que requieran autenticación reforzada, previstos en el artículo 18 del Reglamento de la SBS.
98. Por su parte, el Reglamento del Libro de Reclamaciones, en su artículo 5, establece un conjunto de requisitos informativos mínimos para la presentación de reclamaciones, sin importar el formato del libro de reclamaciones en cada caso.
99. Durante la etapa de fiscalización, se verificó que la administrada solicita la toma en tiempo real de la imagen facial de los usuarios de su libro de reclamaciones

Esta es una copia auténtica imprimible de un documento electrónico archivado por el Ministerio de Justicia y Derechos Humanos, aplicando lo dispuesto por el Art. 25 de D.S. 070-2013-PCM y la Tercera Disposición Complementaria Final del D.S. 026-2016-PCM. Su autenticidad e integridad pueden ser contrastadas a través de la siguiente dirección web: https://sgd.minjus.gob.pe/gesdoc_web/login.jsp e ingresando el Tipo de Documento, Número y Rango de Fechas de ser el caso o https://sgd.minjus.gob.pe/gesdoc_web/verifica.jsp e ingresando Tipo de Documento, Número, Remitente y Año, según corresponda.

Resolución Directoral N° 2271-2023-JUS/DGTAIPD-DPDP

virtual, a fin de enrolarla en su base de datos “BIOM” (que almacena imágenes de los DNI y los rostros de los usuarios), luego de hacer el contraste con el servicio de consulta provisto por el Reniec, empleando el motor biométrico provisto por Facephi para obtener los patrones biométricos.

100. Así también, se aprecia que el libro de reclamaciones virtual con el que cuenta, tiene dos mecanismos de validación, el primero con el número y clave con la tarjeta de cada usuario; y aquel en el que se emplea validación biométrica, la cual era empleada primordialmente para evitar la suplantación de identidad, verificando indubitablemente a quién se le iba a proveer la información financiera relativa a los reclamos.
101. En tal sentido, se aprecia en primer lugar que existe una modalidad de autenticación que se circunscribiría a todas aquellas personas que cuenten con un producto financiero, a las que se le asigna una tarjeta, cuya verificación de identidad podrá completarse con una contraseña; a su vez, que se emplea el patrón biométrico obtenido en tiempo real, al momento de la verificación de la imagen, la administrada cuenta con el acceso al registro del Reniec para efectuar el contraste con la imagen facial de cada rostro, y a la vez, en el caso de las personas que hayan hecho uso del servicio virtual anteriormente, los patrones almacenados en el banco de datos “BIOM”.
102. En la Resolución Directoral N° 232-2023-JUS/DGTAIPD-DFI, se analizó los hechos, concluyendo lo siguiente para fundamentar la imputación:

“gg. De lo expuesto en el presente caso, las actuaciones de fiscalización comprobaron que la administrada condiciona injustificadamente a los usuarios y clientes que pretenden ingresar un reclamo virtual en su sitio web <https://libroreclamos.viabcp.com/> el registrar obligatoriamente, datos personales contenidos en el documento nacional de identidad (mediante el escaneo o fotografía), así como permitir la recopilación y almacenamiento de sus datos biométricos, al tener que entregar su imagen para ser tratada con medios técnicos específicos que permita su identificación o la autenticación inequívoca (datos biométricos). Todo esto con la finalidad de realizar un procedimiento de autenticación de la identidad de los clientes y usuarios, justificada, según la administrada, en los estándares establecidos por la [REDACTED] sin embargo, de la normatividad sectorial analizada, se advierte que la presentación de un reclamo no se encuentra dentro de las operaciones que necesitan realizar una validación biométrica para su trámite, mucho menos permitirle a la administrada recopilar y almacenar datos biométricos en una base propia para tratamientos posteriores de autenticación o verificación.

hh. Por consiguiente, el tratamiento descrito, incumple el principio de proporcionalidad en la medida que la recopilación de los datos personales contenidos en el documento nacional de identidad, así como los datos sensibles requeridos y almacenados, resultan siendo innecesarios y excesivos para la finalidad, que viene a ser el de validar la identidad de quien formula un reclamo a través de una verificación biométrica y/o autenticación de la identidad, recopilación de datos que es intrusiva para la privacidad que puede exponer al titular de los datos personales a distintos riesgos, como

Resolución Directoral N° 2271-2023-JUS/DGTAIPD-DPDP

podría ser en el caso de una filtración ya sea que provenga de los medios técnicos utilizados o del factor humano.

ii. La administrada debe tener en cuenta que, el requerimiento de datos personales, de acuerdo a la finalidad para la cual se requieran, deben ser únicamente los que resulten adecuados, pertinentes y limitados al mínimo necesario para las finalidades específicas de su recopilación y tratamiento posterior; es decir, deberían seguir un criterio de limitación o minimización, de acuerdo con el cual deberían hacer un esfuerzo razonable para cerciorarse de que los datos personales que manejen correspondan al mínimo requerido para la finalidad expresa, lo cual evidentemente no ocurre en el presente caso, dado que la administrada requiere información inclusive referida al reconocimiento facial para poder interponer un reclamo, hecho que afecta el derecho fundamental a la protección de datos personales.”

103. Esta Dirección considera que si bien existe una disposición sectorial que tiene previsto el uso de la autenticación biométrica con lo almacenado en su base de datos “BIOM” como mecanismo de validación de identidad, este no es el único ni excluyente medio para tal fin, toda vez que se cuenta con la comprobación de factores como aquello que solo el usuario tiene y un elemento que solo el usuario conoce, pudiendo emplearse estos conjuntamente, en observancia del principio de proporcionalidad.
104. En efecto, la DFI pudo comprobar, al revisar el procedimiento de presentación de reclamaciones virtuales, que estas incluyen tanto la validación empleando el número de tarjeta asignado al usuario y la contraseña creada por este, que constituyen el factor que solo este “posee” y que solo este “conoce”, en concordancia con el literal j) del artículo 2 del Reglamento de la SBS, y lo requerido en el artículo 18 de dicha norma.
105. Debe tenerse claro que el proceso anterior es aplicable a los portadores de las tarjetas señaladas, de quienes también se tiene otros datos personales preexistentes, recopilados al momento de haber adquirido algún producto financiero, que contribuyen a la verificación de la identidad, así como a la remisión de la información financiera a la persona titular de un número telefónico o correo electrónico inscrito como dato de contacto de este usuario, con lo cual es tangible la existencia de más elementos a emplear para la verificación de la identidad y para sostener una comunicación con el verdadero cliente, con la que este pueda estar al tanto de cualquier movimiento o proceso de reclamación.
106. Por otra parte, para otro tipo de usuarios de dicho libro de reclamaciones (denominados “clientes intermitentes” por la administrada), se emplea la imagen del DNI, así como la fotografía facial, en tiempo real, de la cual se obtienen los datos biométricos materia de tratamiento; acciones con las cuales, a entender de la administrada, se asegura la correcta verificación de la identidad, cumpliendo con el principio de Calidad de la LPDP.
107. Para el caso del empleo de datos biométricos, se aprecia que la administrada cuenta con dos fuentes de las cuales puede obtener imágenes y patrones biométricos: Uno, el registro del Reniec, que contiene imágenes de las personas

Esta es una copia auténtica imprimible de un documento electrónico archivado por el Ministerio de Justicia y Derechos Humanos, aplicando lo dispuesto por el Art. 25 de D.S. 070-2013-PCM y la Tercera Disposición Complementaria Final del D.S. 026-2016-PCM. Su autenticidad e integridad pueden ser contrastadas a través de la siguiente dirección web: https://sgd.minjus.gob.pe/gesdoc_web/login.jsp e ingresando el Tipo de Documento, Número y Rango de Fechas de ser el caso o https://sgd.minjus.gob.pe/gesdoc_web/verifica.jsp e ingresando Tipo de Documento, Número, Remitente y Año, según corresponda.

Resolución Directoral N° 2271-2023-JUS/DGTAIPD-DPDP

en cada uno de los registros; y la base de datos “BIOM” creada por ella misma con los datos biométricos que se recopilan a partir de las imágenes faciales.

108. En su comunicación del 29 de diciembre de 2022, la administrada señaló al respecto que, con la finalidad de verificar y validar la identidad de los usuarios que presentan reclamos por medios virtuales, emplean el Registro del Reniec al cual tienen acceso empleando la imagen del DNI y del rostro, siendo estas últimas recopiladas en formato biométrico y almacenadas, guardando tal información para sustentar que se ha realizado la correcta verificación de la identidad; todo ello, en cumplimiento de las disposiciones del Reglamento de la SBS.
109. Tal argumentación se reiteró en el escrito de descargos del 8 de noviembre de 2023, sosteniendo además que el empleo de los datos biométricos mencionados, desde su base de datos “BIOM”, aparte de obedecer a una disposición sectorial, es necesaria para el cumplimiento de las relaciones contractuales y de prestación de servicios, así como para la protección del interés individual de cada usuario.
110. Al respecto, en sus alegatos de febrero de 2024, la administrada complementa su argumentación señalando que el tratamiento de los datos biométricos se ajusta a las necesidades de seguridad de su giro, relativas a la correcta identificación de los usuarios del libro de reclamaciones virtual, y que para ello se ha implementado las medidas de seguridad acordes al grado de sensibilidad de tal información, siguiendo lo indicado en la Opinión Consultiva.
111. En esta comunicación, añade que no se puede establecer distintos mecanismos para la presentación de reclamos en su libro de reclamaciones virtual en función del tipo de reclamo, pues es inviable implementar una diversidad de procesos para los tipos de reclamos, pues recién con el ingreso del reclamo y su posterior evaluación por un asesor (horas o días después) se podría saber sobre qué servicio es y qué tipo de validación es necesaria; y además, que el uso de los otros dos factores independientes aparte de la biometría (algo que solo él tiene y algo que solo él posee) resultaría más intrusivo.
112. Esta Dirección concuerda con la necesidad de una correcta verificación de la identidad de los usuarios en transacciones y reclamaciones financieras efectuadas en vía virtual, siendo una finalidad válida para cuyo alcance es necesario analizar opciones que sean menos intrusivas y perjudiciales para la privacidad de la información personal del usuario, como concreción de su derecho fundamental a la protección de datos personales; por lo que resulta necesario efectuar sobre este un *test* de proporcionalidad sobre su tratamiento, vale decir, la determinación de su idoneidad, necesidad y ponderación o proporcionalidad en sentido estricto, de acuerdo con lo establecido en la sentencia del Tribunal Constitucional recaída en el expediente N° 0045-2004-PI/TC, pudiendo determinar con ello si la obtención y empleo de los patrones biométricos faciales es necesaria o si existe una modalidad menos invasiva y riesgosa para la privacidad de los usuarios.
113. En cuanto a la idoneidad, entendida como la causalidad entre un determinado medio y su finalidad, justificando su adopción, se ve que en el presente caso, la administrada requiere alcanzar la válida finalidad de verificación de identidad de los reclamantes vía libro de reclamaciones virtual, para lo cual cuenta con una

Esta es una copia auténtica imprimible de un documento electrónico archivado por el Ministerio de Justicia y Derechos Humanos, aplicando lo dispuesto por el Art. 25 de D.S. 070-2013-PCM y la Tercera Disposición Complementaria Final del D.S. 026-2016-PCM. Su autenticidad e integridad pueden ser contrastadas a través de la siguiente dirección web: https://sgd.minjus.gob.pe/gesdoc_web/login.jsp e ingresando el Tipo de Documento, Número y Rango de Fechas de ser el caso o https://sgd.minjus.gob.pe/gesdoc_web/verifica.jsp e ingresando Tipo de Documento, Número, Remitente y Año, según corresponda.

Resolución Directoral N° 2271-2023-JUS/DGTAIPD-DPDP

pluralidad de opciones: Uso del número de tarjeta y contraseña, y en casos en los que el usuario no posea tarjetas ni productos financieros, la imagen del DNI en conjunto con el dato biométrico obtenido, a ser contrastadas con las imágenes del Registro del Reniec y la base de datos "BIOM" de patrones biométricos.

114. Esta Dirección aprecia que para el caso de titulares de tarjetas y productos financieros de la administrada, se aprecia la importancia de una mayor seguridad en la autenticación de la identidad, por lo que la administrada se sirve de la biometría facial, contrastando el patrón biométrico de una imagen tomada en tiempo real, con las de las imágenes del Reniec a las que tiene acceso y con los patrones biométricos almacenados en la base de datos "BIOM".
115. En concordancia con lo explicado en el considerando 105 de esta resolución directoral, no es necesaria la recopilación ni uso de datos biométricos (patrón facial biométrico), existiendo claramente otros medios para la verificación de la identidad de los usuarios del libro de reclamaciones virtual que sean clientes y tengan algún producto financiero, así como para el posterior seguimiento de las comunicaciones y sus respuestas.
116. Por su parte, para el específico caso de usuarios que no cuenten con tarjetas de la administrada, los denominados "clientes intermitentes", y/o quienes interpongan quejas, primordialmente comunicaciones en las que no es necesaria la información financiera, el movimiento de dinero u otra acción que implique un riesgo significativo para información patrimonial, la verificación de la identidad es necesaria, pero puede satisfacerse con la consignación del número de DNI en el formulario correspondientes.
117. Ahora bien, dentro de este tipo de comunicaciones de los "clientes intermitentes", en supuestos menos comunes en los que podría comprometerse algún tipo de información patrimonial y/o pueda vulnerar la privacidad del usuario o algún cliente, podría ser necesaria una última verificación de identidad más rigurosa, dependiendo esto de algún dato que se consigne o se marque en el formulario correspondiente, como la existencia de dinero comprometido.
118. Entonces, el empleo del patrón biométrico facial solo sería necesario para estos últimos casos, en los que usuarios sin productos financieros de la administrada comuniquen alguna discrepancia relacionada con algún movimiento de dinero, factor por el cual podría activarse tal modalidad de identidad, conjuntamente con la mención del número de DNI del usuario.
119. Respecto de los recursos biométricos debe examinarse, por otro lado, la proporcionalidad o ponderación de su obtención y empleo para estos fines, que obliga a que el grado de afectación de los usuarios corresponda a la importancia o trascendencia del derecho o finalidad que se le contrapone.
120. Este factor obliga a ponderar la principal finalidad de la administrada, que es la correcta autenticación de identidad de los usuarios para evitar suplantaciones de identidad u otras situaciones perjudiciales en su libro de reclamaciones virtuales; observando el medio empleado para ello, que en el caso analizado, se sirve del

Esta es una copia auténtica imprimible de un documento electrónico archivado por el Ministerio de Justicia y Derechos Humanos, aplicando lo dispuesto por el Art. 25 de D.S. 070-2013-PCM y la Tercera Disposición Complementaria Final del D.S. 026-2016-PCM. Su autenticidad e integridad pueden ser contrastadas a través de la siguiente dirección web: https://sgd.minjus.gob.pe/gesdoc_web/login.jsp e ingresando el Tipo de Documento, Número y Rango de Fechas de ser el caso o https://sgd.minjus.gob.pe/gesdoc_web/verifica.jsp e ingresando Tipo de Documento, Número, Remitente y Año, según corresponda.

Resolución Directoral N° 2271-2023-JUS/DGTAIPD-DPDP

uso de los patrones biométricos faciales recopilados y luego conservados en la base de datos "BIOM".

121. Debe reiterarse que la administrada emplea dos medios de autenticación, uno de ellos el que utiliza los patrones biométricos faciales, siguiendo lo que permite el articulado del Reglamento de la SBS; para lo cual dos fuentes de patrones para contrastar con la imagen tomada en tiempo real: La base de datos "BIOM", alimentada con los datos biométricos recopilados de los usuarios, y la imagen almacenada en el RUIPN del Reniec, al cual se le provee acceso.
122. Sobre esto último, es importante mencionar que la administrada cuenta ordinariamente con dicho recurso del Reniec, para el cual no se establece limitaciones cuantitativas, sino que de acuerdo con los términos del convenio que los vincula, la contraprestación depende de las consultas efectuadas por día; y que ofrece una imagen cotejable con la del DNI que se toma en tiempo real y también puede ser contrastable con la facial, no solo para el primer enrolamiento del usuario del libro de reclamaciones virtual.
123. Conociendo ello, es posible evaluar si existen o no medios alternativos a la recopilación y almacenamiento de los patrones biométricos faciales de los usuarios, que resulten menos invasivos o riesgosos para los usuarios, debiendo optar por minimizar acciones de tratamiento, sobretodo de los datos biométricos.
124. En atención a lo desarrollado a los considerandos anteriores de esta resolución directoral (117), la verificación de identidad con datos biométricos tomados en tiempo real, debe restringirse solo para casos de usuarios que no tienen productos financieros y cuyas comunicaciones a través del libro de reclamaciones virtual impliquen cuestiones patrimoniales o dinerarias, es necesaria a falta de otro medio de autenticación, efectuada conjuntamente con los datos del DNI.
125. Esta Dirección aprecia que en este caso especial de usuarios, la verificación empleando patrones faciales solo requiere una fuente de estos para el contraste en tiempo real, que es la extraída del registro del Reniec, sin que sea necesario recopilar ni almacenar posteriormente los patrones biométricos faciales en una base de datos permanente, como en el caso del "BIOM".
126. En sus descargos, la administrada señaló que el sistema del Reniec con el cual se ofrece el servicio aludido, suele presentar averías o problemas, lo que puede impedir que el servicio se brinde de forma ágil y fiable durante lapsos considerables.
127. Sobre este argumento, es necesario volver a tomar en cuenta las otras modalidades para las comunicaciones a través del libro de reclamaciones virtual, como las señaladas anteriormente, circunscribiendo el empleo del patrón biométrico facial a la situación excepcional descrita (solo comunicaciones de parte de usuarios sin productos financieros cuya disconformidad implique una cuestión patrimonial o dineraria), siendo suficiente en otros casos la consignación de tarjetas y contraseñas, del número de DNI y otros datos que a la vez, faciliten la comunicación posterior.

Esta es una copia auténtica imprimible de un documento electrónico archivado por el Ministerio de Justicia y Derechos Humanos, aplicando lo dispuesto por el Art. 25 de D.S. 070-2013-PCM y la Tercera Disposición Complementaria Final del D.S. 026-2016-PCM. Su autenticidad e integridad pueden ser contrastadas a través de la siguiente dirección web: https://sgd.minjus.gob.pe/gesdoc_web/login.jsp e ingresando el Tipo de Documento, Número y Rango de Fechas de ser el caso o https://sgd.minjus.gob.pe/gesdoc_web/verifica.jsp e ingresando Tipo de Documento, Número, Remitente y Año, según corresponda.

Resolución Directoral N° 2271-2023-JUS/DGTAIPD-DPDP

128. De otro lado, respecto de la alegada dificultad de distinguir los tipos de comunicaciones que pueden registrarse en el libro de reclamación virtual, que la misma puede realizarse expresamente en la interfaz correspondiente del sitio web, detallando las diferencias entre cada tipo de comunicación y empleando formas de acceso y formularios distintos, pudiendo evitarse para el caso de las meras quejas el tratamiento de datos biométricos, requiriendo solo datos identificativos no sensibles.
129. Así, debe reafirmarse que en el caso de las reclamaciones, relativas a cuestiones que tengan que ver con el efectivo servicio o provisión de productos por parte de la administrada, la verificación de identidad puede realizarse con el uso de la tarjeta y contraseña asignada a esta por el propio usuario, empleando algo que solo él posee y solo él conoce, así como los datos de contacto previamente registrados y empleados en otras operaciones.
130. A su vez, en caso de requerirse una verificación biométrica de aquellos que no poseen tarjetas ni productos financieros, puede circunscribirse el contraste de los datos biométricos tomados en tiempo real con la información que posee Reniec en el sistema al que tiene acceso, sin necesidad de recopilar o almacenar imágenes faciales ni datos biométricos de los usuarios.
131. En lo concerniente a las normas sectoriales invocadas (Reglamento de la SBS y el Reglamento del Libro de Reclamaciones), esta Dirección percibe que en el caso del primer Reglamento, se establecen más opciones aparte del empleo de datos biométricos para la verificación de los reclamantes, lo cual ofrece más posibilidades por las que se puede prescindir de la toma y almacenamiento de los patrones biométricos faciales; mientras que el Reglamento del Libro de Reclamaciones, en efecto, establece un mínimo de características que debe poseer un libro de reclamaciones físico o virtual, sin que ello lleve a pensar en una cantidad ilimitada de tipos de datos personales que deben componerlo, debiendo restringirse estos según la necesidad que haya de recopilarlos.
132. En consecuencia, la administrada se encuentra en posición de optar por emplear otros datos personales aparte de los conformados por los patrones biométricos faciales, para la atención de reclamaciones y quejas por parte de usuarios de su libro de reclamaciones virtual; siendo así que la actual recopilación de dichos patrones biométricos constituye una acción de tratamiento excesiva y no necesaria, contraria a la necesidad de minimización de los datos personales y de acciones de tratamiento que deriva del principio de Proporcionalidad del artículo 7 de la LPDP.
133. Por consiguiente, se deduce que la administrada, con el empleo de patrones biométricos faciales (datos sensibles) para la validación de identidad de usuarios de sus libros de reclamaciones virtuales, ha inobservado el mencionado principio, incurriendo en la infracción grave tipificada en el literal d) del numeral 2 del artículo 132 del Reglamento de la LPDP; situación que aparte de ameritar una multa a modo de sanción, requiere la imposición de una medida correctiva.

Esta es una copia auténtica imprimible de un documento electrónico archivado por el Ministerio de Justicia y Derechos Humanos, aplicando lo dispuesto por el Art. 25 de D.S. 070-2013-PCM y la Tercera Disposición Complementaria Final del D.S. 026-2016-PCM. Su autenticidad e integridad pueden ser contrastadas a través de la siguiente dirección web: https://sgd.minjus.gob.pe/gesdoc_web/login.jsp e ingresando el Tipo de Documento, Número y Rango de Fechas de ser el caso o https://sgd.minjus.gob.pe/gesdoc_web/verifica.jsp e ingresando Tipo de Documento, Número, Remitente y Año, según corresponda.

Resolución Directoral N° 2271-2023-JUS/DGTAIPD-DPDP

Sobre el presunto tratamiento de datos sensibles (patrones biométricos faciales) sin el consentimiento de sus titulares

134. Teniendo en cuenta que el ejercicio del derecho fundamental consiste en la posibilidad de autorizar o impedir el tratamiento de sus datos personales, vale decir, de manifestar su voluntad al respecto, expresada afirmativamente a través del consentimiento, corresponde que la conducta de quien realiza el tratamiento de sus datos personales se adecúe a los conscientemente autorizado.
135. En virtud de ello, no se puede ejercer un control efectivo de la información personal a través de un consentimiento basado en el desconocimiento respecto de cómo se van a utilizar los datos recopilados, qué tratamiento se les va a dar, con quiénes se va a compartir y otros pormenores del tratamiento, así como tampoco se puede obtener este consentimiento a través de engaño, inducción a error, ni de formas ambiguas, que dejen dudas respecto del acto que permite la disposición de los datos personales.
136. La LPDP, que desarrolla el mencionado derecho fundamental, establece que el tratamiento de datos personales requiere el consentimiento del titular de los datos personales. Así, el principio de consentimiento se tiene previsto en su artículo 5 lo siguiente:

“Artículo 5. Principio de consentimiento

Para el tratamiento de los datos personales debe mediarse el consentimiento de su titular.”

137. Asimismo, según lo dispone el inciso 13.5 del artículo 13 de la LPDP, el consentimiento del titular de los datos personales deberá ser otorgado de manera previa, informada, expresa e inequívoca:

“Artículo 13. Alcances sobre el tratamiento de datos personales

(...)

13.5 Los datos personales solo pueden ser objeto de tratamiento con consentimiento de su titular, salvo ley autoritativa al respecto. El consentimiento debe ser previo, informado, expreso e inequívoco.

13.6 En el caso de datos sensibles, el consentimiento para efectos de su tratamiento, además, debe efectuarse por escrito. Aun cuando no mediare el consentimiento del titular, el tratamiento de datos sensibles puede efectuarse cuando la ley lo autorice, siempre que ello atienda a motivos importantes de interés público.”

138. Por su parte, el artículo 12 del Reglamento de la LPDP establece los presupuestos bajo los cuales se otorga válidamente el consentimiento para el tratamiento de los datos personales: 1. Libre; 2. Previo; 3. Expreso e Inequívoco; y, 4. Informado²⁷.

²⁷ **Artículo 12.- Características del consentimiento.**

Además de lo dispuesto en el artículo 18 de la Ley y en el artículo precedente del presente reglamento, la obtención del consentimiento debe ser:

1. Libre: Sin que medie error, mala fe, violencia o dolo que puedan afectar la manifestación de voluntad del titular de los datos personales. La entrega de obsequios o el otorgamiento de beneficios al titular de los datos personales con ocasión de su consentimiento no afectan la condición de libertad que tiene para otorgarlo, salvo en el caso de menores de edad,

Esta es una copia auténtica imprimible de un documento electrónico archivado por el Ministerio de Justicia y Derechos Humanos, aplicando lo dispuesto por el Art. 25 de D.S. 070-2013-PCM y la Tercera Disposición Complementaria Final del D.S. 026-2016-PCM. Su autenticidad e integridad pueden ser contrastadas a través de la siguiente dirección web: https://sgd.minjus.gob.pe/gesdoc_web/login.jsp e ingresando el Tipo de Documento, Número y Rango de Fechas de ser el caso o https://sgd.minjus.gob.pe/gesdoc_web/verifica.jsp e ingresando Tipo de Documento, Número, Remitente y Año, según corresponda.

Resolución Directoral N° 2271-2023-JUS/DGTAIPD-DPDP

139. De otro lado, es preciso tener en cuenta que la obligación de obtener el consentimiento tiene excepciones, las cuales se encuentran previstas en el artículo 14 de la LPDP²⁸.

en los supuestos en que se admite su consentimiento, en que no se considerará libre el consentimiento otorgado mediando obsequios o beneficios. El condicionamiento de la prestación de un servicio, o la advertencia o amenaza de denegar el acceso a beneficios o servicios que normalmente son de acceso no restringido, sí afecta la libertad de quien otorga consentimiento para el tratamiento de sus datos personales, si los datos solicitados no son indispensables para la prestación de los beneficios o servicios.

2. Previo: Con anterioridad a la recopilación de los datos o en su caso, anterior al tratamiento distinto a aquel por el cual ya se recopilaron.

3. Expreso e inequívoco: Con anterioridad a la recopilación de los datos o en su caso, anterior al tratamiento distinto a aquel por el cual ya se recopilaron queda o pueda ser impreso en una superficie de papel o similar. La condición de expreso no se limita a la manifestación verbal o escrita. En sentido restrictivo y siempre de acuerdo con lo dispuesto por el artículo 7 del presente reglamento, se considerará consentimiento expreso a aquel que se manifieste mediante la conducta del titular que evidencie que ha consentido inequívocamente, dado que de lo contrario su conducta, necesariamente, hubiera sido otra.

Tratándose del entorno digital, también se considera expresa la manifestación consistente en "hacer clic", "cliquear" o "pinchar", "dar un toque", "touch" o "pad" u otros similares. En este contexto el consentimiento escrito podrá otorgarse mediante firma electrónica, mediante escritura que quede grabada, de forma tal que pueda ser leída e impresa, o que por cualquier otro mecanismo o procedimiento establecido permita identificar al titular y recabar su consentimiento, a través de texto escrito. También podrá otorgarse mediante texto preestablecido, fácilmente visible, legible y en lenguaje sencillo, que el titular pueda hacer suyo, o no, mediante una respuesta escrita, gráfica o mediante clic o pinchado. La sola conducta de expresar voluntad en cualquiera de las formas reguladas en el presente numeral no elimina, ni da por cumplidos, los otros requisitos del consentimiento referidos a la libertad, oportunidad e información.

4. Informado: Cuando al titular de los datos personales se le comunique clara, expresa e indubitablemente, con lenguaje sencillo, cuando menos de lo siguiente a. La identidad y domicilio o dirección del titular del banco de datos personales o del responsable del tratamiento al que puede dirigirse para revocar el consentimiento o ejercer sus derechos. b. La finalidad o finalidades del tratamiento a las que sus datos serán sometidos. c. La identidad de los que son o pueden ser sus destinatarios, de ser el caso. d. La existencia del banco de datos personales en que se almacenarán, cuando corresponda. e. El carácter obligatorio o facultativo de sus respuestas al cuestionario que se le proponga, cuando sea el caso. f. Las consecuencias de proporcionar sus datos personales y de su negativa a hacerlo. g. En su caso, la transferencia nacional e internacional de datos que se efectúen.

28 Artículo 14. Limitaciones al consentimiento para el tratamiento de datos personales

No se requiere el consentimiento del titular de datos personales, para los efectos de su tratamiento, en los siguientes casos:

1. Cuando los datos personales se recopilen o transfieran para el ejercicio de las funciones de las entidades públicas en el ámbito de sus competencias.
2. Cuando se trate de datos personales contenidos o destinados a ser contenidos en fuentes accesibles para el público.
3. Cuando se trate de datos personales relativos a la solvencia patrimonial y de crédito, conforme a ley.
4. Cuando medie norma para la promoción de la competencia en los mercados regulados emitida en ejercicio de la función normativa por los organismos reguladores a que se refiere la Ley 27332, Ley Marco de los Organismos Reguladores de la Inversión Privada en los Servicios Públicos, o la que haga sus veces, siempre que la información brindada no sea utilizada en perjuicio de la privacidad del usuario.
5. Cuando los datos personales sean necesarios para la preparación, celebración y ejecución de una relación contractual en la que el titular de datos personales sea parte, o cuando se trate de datos personales que deriven de una relación científica o profesional del titular y sean necesarios para su desarrollo o cumplimiento.
6. Cuando se trate de datos personales relativos a la salud y sea necesario, en circunstancia de riesgo, para la prevención, diagnóstico y tratamiento médico o quirúrgico del titular, siempre que dicho tratamiento sea realizado en establecimientos de salud o por profesionales en ciencias de la salud, observando el secreto profesional; o cuando medien razones de interés público previstas por ley o cuando deban tratarse por razones de salud pública, ambas razones deben ser calificadas como tales por el Ministerio de Salud; o para la realización de estudios epidemiológicos o análogos, en tanto se apliquen procedimientos de disociación adecuados.
7. Cuando el tratamiento sea efectuado por organismos sin fines de lucro cuya finalidad sea política, religiosa o sindical y se refiera a los datos personales recopilados de sus respectivos miembros, los que deben guardar relación con el propósito a que se circunscriben sus actividades, no pudiendo ser transferidos sin consentimiento de aquellos.
8. Cuando se hubiera aplicado un procedimiento de anonimización o disociación.
9. Cuando el tratamiento de los datos personales sea necesario para salvaguardar intereses legítimos del titular de datos personales por parte del titular de datos personales o por el encargado de tratamiento de datos personales.
10. Cuando el tratamiento sea para fines vinculados al sistema de prevención de lavado de activos y financiamiento del terrorismo u otros que respondan a un mandato legal.
11. En el caso de grupos económicos conformados por empresas que son consideradas sujetos obligados a informar, conforme a las normas que regulan a la Unidad de Inteligencia Financiera, que éstas puedan compartir información entre sí de sus respectivos clientes para fines de prevención de lavado de activos y financiamiento del terrorismo, así como

Esta es una copia auténtica imprimible de un documento electrónico archivado por el Ministerio de Justicia y Derechos Humanos, aplicando lo dispuesto por el Art. 25 de D.S. 070-2013-PCM y la Tercera Disposición Complementaria Final del D.S. 026-2016-PCM. Su autenticidad e integridad pueden ser contrastadas a través de la siguiente dirección web: https://sgd.minjus.gob.pe/gesdoc_web/login.jsp e ingresando el Tipo de Documento, Número y Rango de Fechas de ser el caso o https://sgd.minjus.gob.pe/gesdoc_web/verifica.jsp e ingresando Tipo de Documento, Número, Remitente y Año, según corresponda.

Resolución Directoral N° 2271-2023-JUS/DGTAIPD-DPDP

140. Respecto de la prueba de la obtención válida del consentimiento para el tratamiento de los datos personales, debe señalarse que esta corre a cargo del responsable del tratamiento, quien debe ser siempre capaz de sustentar tal obtención, de acuerdo con el artículo 15 del Reglamento de la LPDP:

“Artículo 15.- Consentimiento y carga de la prueba.

Para efectos de demostrar la obtención del consentimiento en los términos establecidos en la Ley y en el presente reglamento, la carga de la prueba recaerá en todos los casos en el titular del banco de datos personales o quien resulte el responsable del tratamiento.”

141. De lo expuesto, se desprende la necesidad de obtener el consentimiento válido (libre, expreso e inequívoco, previo e informado) y a la vez de forma escrita, para el tratamiento de datos personales, a fin de mantener el sustento tangible de tal obtención, que el responsable del tratamiento siempre debe estar en capacidad de comprobar.
142. En el presente caso, es necesario distinguir las dos acciones de tratamiento de los datos biométricos (patrones biométricos faciales) efectuadas a través del libro de reclamaciones virtual:
- Recopilación en tiempo real para la validación de identidad del usuario del libro de reclamaciones virtual
 - Recopilación y almacenamiento para la validación de identidad a futuro, en la base de datos “BIOM”
143. En el subtítulo anterior se analizó la proporcionalidad de la recopilación de datos para la identificación del usuario, y solo para ese momento, deduciéndose el carácter excesivo de la recopilación de los datos biométricos para la validación en tiempo real, ante la existencia de medios menos útiles e igualmente funcionales, según cada tipo de usuario y comunicación.
144. Esclarecida la anterior ilicitud, en el presente subtítulo se analiza si la recopilación y almacenamiento de tales datos sensibles en la mencionada base de datos, para posteriores validaciones, se sostiene en la obtención del consentimiento válido de parte de sus titulares, esto último como factor que legitimaría tal tratamiento.
145. Sobre ello, la cuestión previa de la Resolución Directoral N° 232-2023-JUS/DGTAIPD-DFI desarrolló lo siguiente:

“18. Asimismo, informaron que, los datos son recabados únicamente con la finalidad de verificar la identidad, y para las comunicaciones necesarias a fin de atender el reclamo, validación que se realiza conforme la exigencia dada por la Superintendencia de Banca, Seguros y AFP (SBS) a través de la Resolución n.º 504-2021 del 19 de febrero de 2021, con la cual se aprobó el

otros de cumplimiento regulatorio, estableciendo las salvaguardas adecuadas sobre la confidencialidad y uso de la información intercambiada.

12. Cuando el tratamiento se realiza en ejercicio constitucionalmente válido del derecho fundamental a la libertad de información.

13. Otros que deriven del ejercicio de competencias expresamente establecidas por Ley.

Esta es una copia auténtica imprimible de un documento electrónico archivado por el Ministerio de Justicia y Derechos Humanos, aplicando lo dispuesto por el Art. 25 de D.S. 070-2013-PCM y la Tercera Disposición Complementaria Final del D.S. 026-2016-PCM. Su autenticidad e integridad pueden ser contrastadas a través de la siguiente dirección web: https://sgd.minjus.gob.pe/gesdoc_web/login.jsp e ingresando el Tipo de Documento, Número y Rango de Fechas de ser el caso o https://sgd.minjus.gob.pe/gesdoc_web/verifica.jsp e ingresando Tipo de Documento, Número, Remitente y Año, según corresponda.

Resolución Directoral N° 2271-2023-JUS/DGTAIPD-DPDP

Reglamento para la Gestión de Seguridad de la Información y Ciberseguridad. Por lo que, los datos biométricos recabados durante el proceso de presentación de un reclamo a través de un canal digital son almacenados en el Banco de Datos Personales denominado 'Base Biométrica', el cual cuenta con código RNPDP-PJP N° 15280.

19. *De lo manifestado por la administrada, esta Dirección, advierte que, estaría realizando tratamiento de datos personales sensibles (datos biométricos) de sus clientes y usuarios, al recopilarlos y almacenarlos en una base de datos propia; tratamiento que para legitimarse debe contar con el consentimiento escrito de su titular cumpliendo lo regulado en el artículo 12° del Reglamento de la LPDP, salvo que exista una ley autoritativa al respecto. De conformidad a lo dispuesto en el artículo 13 de la LPDP.*

20. *El 27 de setiembre de 2023, se realizó una visita de inspección con la finalidad de investigar de manera plena los hechos, así, mediante Acta n.º 002-2023-DFI27, se constató que la administrada hace uso del servicio de biometría facial en el libro de reclamaciones virtual, Yape, Seguros, Dinero al Instante, Coco y Lucas, Banca Móvil, Tarjetas, Homebanking (VíaBcp). Asimismo, se constató que no solicita el consentimiento del titular de los datos para la recopilación de los datos sensibles y su almacenamiento en el banco de datos personales 'Base Biométrica', para el tratamiento posterior en los servicios y trámites mencionados.*

21. *Por lo que, corresponde imputar, el presunto incumplimiento de la obligación establecida en el artículo 13.5° de la LPDP, así como lo previsto en el artículo 12° del Reglamento de la LPDP, referido a dar tratamiento de datos personales sensibles sin el consentimiento libre, expreso, inequívoco, previo e informado del titular de los datos personales, de acuerdo a los argumentos que se desarrollarán en el hecho imputado n.º 02.”*

146. Por su parte, en el desarrollo de esta imputación del acápite III de dicha resolución directoral de la DFI, se anotó lo siguiente:

“z. Cabe indicar que, la LPDP dispone que los datos personales solo pueden ser objeto de tratamiento con consentimiento de su titular, salvo ley autoritativa al respecto. El consentimiento debe ser previo, informado, expreso e inequívoco. Y para el caso de los datos sensibles el consentimiento para efectos de su tratamiento, además, debe efectuarse por escrito. Precisa la LPDP que, cuando no mediara el consentimiento del titular, el tratamiento de datos sensibles puede efectuarse cuando la ley lo autorice, siempre que ello atienda a motivos importantes de interés público. Lo que en el presente caso no ocurre, tal como se ha verificado en las actuaciones realizadas por esta Dirección, en las que se ha verificado que la administrada no cuenta con el consentimiento para el tratamiento de datos biométricos ni hay una ley que sustente dicho tratamiento.

aa. De la documentación que obra en el expediente, se ofrecen evidencias de que la administrada, habría vulnerado el principio de consentimiento señalado en el artículo 5° de la LPDP y artículo 7° del Reglamento de la LPDP, en la medida que no cumple con recabar el consentimiento conforme lo regulado en el artículo 12° del Reglamento de la LPDP, para recopilar y almacenar en una base de datos propia datos sensibles como son los datos biométricos.

Esta es una copia auténtica imprimible de un documento electrónico archivado por el Ministerio de Justicia y Derechos Humanos, aplicando lo dispuesto por el Art. 25 de D.S. 070-2013-PCM y la Tercera Disposición Complementaria Final del D.S. 026-2016-PCM. Su autenticidad e integridad pueden ser contrastadas a través de la siguiente dirección web: https://sgd.minjus.gob.pe/gesdoc_web/login.jsp e ingresando el Tipo de Documento, Número y Rango de Fechas de ser el caso o https://sgd.minjus.gob.pe/gesdoc_web/verifica.jsp e ingresando Tipo de Documento, Número, Remitente y Año, según corresponda.

Resolución Directoral N° 2271-2023-JUS/DGTAIPD-DPDP

bb. Así, analizada la información relacionada al tratamiento de datos personales que la administrada proporciona durante el procedimiento de verificación biométrica, se observa que se indica lo siguiente: 'Usted autoriza al BCP a recopilar y almacenar la información consignada en su documento de identidad, incluyendo su imagen, con la única finalidad de verificar su identidad en este proceso. La información que el BCP recopila en este proceso será utilizada únicamente para efectos de comunicarse con usted en relación al proceso iniciado por este medio. En ningún caso, el BCP en mérito de esta cláusula le ofrecerá productos o servicios del BCP. (...)'

cc. Como puede verse, la administrada en la información que traslada al usuario o cliente, señala que almacenará la información que consta en el DNI así como la imagen del reclamante, sin que haya establecido un mecanismo adecuado a través del cual la persona pueda otorgar válidamente su consentimiento para que la administrada almacene el dato biométrico referido a la imagen facial, por lo cual se infiere que almacena este dato personal sin la obtención del consentimiento del titular de los datos.

dd. Por lo tanto, el tratamiento del dato personal referido a la imagen biométrica, no se legitima con la sola información al titular de los datos personales acerca de su tratamiento, sino que es necesario que se recabe el consentimiento, y que este además cumpla con los requisitos ya mencionados anteriormente, de otra manera, la conducta de la administrada configura una infracción.

ee. Por consiguiente, tal como se ha indicado, no existiendo norma legal que legitime a la administrada a recopilar y almacenar datos biométricos, dicho tratamiento únicamente podría basarse en el consentimiento del titular de los datos personales que deberá cumplir, en todo caso, con los requisitos contenidos en el artículo 13° de la LPDP y artículo 12° de su reglamento.”

147. Lo señalado en lo transcurrido toma en cuenta también la verificación del sitio web efectuada el 21 de agosto de 2023, constatándose que para el paso “Tómate una foto y sube las imágenes de tu DNI desde tu computadora. Por tu seguridad lo validaremos”, utilizada toma de la imagen facial se había habilitado el enlace “He leído y acepto el Tratamiento de Datos Personales”, acompañado de una casilla cuyo marcado condiciona la continuidad y abre una ventana emergente con el siguiente texto:

“Usted autoriza al BCP a recopilar y almacenar la información consignada en su documento de identidad, incluyendo su imagen, con la única finalidad de verificar su identidad en este proceso. La información que el BCP puede recopilar en este proceso será utilizada únicamente para efectos de comunicarse con usted en relación al proceso iniciado por este medio. En ningún caso el BCP en mérito de esta cláusula le ofrecerá producto o servicios del BCP.

Mantendremos su información hasta diez años después de que finalice su relación contractual con el BCP y no transferiremos su información a terceros no autorizados. En caso usted quiera ejercer sus derechos de acceso, rectificación, cancelación y oposición y revocación, deberá dirigirse al BCP en cualquiera de sus oficinas a nivel nacional, a través de Banca por Internet o vía Banca por Teléfono.”

Esta es una copia auténtica imprimible de un documento electrónico archivado por el Ministerio de Justicia y Derechos Humanos, aplicando lo dispuesto por el Art. 25 de D.S. 070-2013-PCM y la Tercera Disposición Complementaria Final del D.S. 026-2016-PCM. Su autenticidad e integridad pueden ser contrastadas a través de la siguiente dirección web: https://sgd.minjus.gob.pe/gesdoc_web/login.jsp e ingresando el Tipo de Documento, Número y Rango de Fechas de ser el caso o https://sgd.minjus.gob.pe/gesdoc_web/verifica.jsp e ingresando Tipo de Documento, Número, Remitente y Año, según corresponda.

Resolución Directoral N° 2271-2023-JUS/DGTAIPD-DPDP

148. En efecto, es tangible lo mencionado por la DFI en su imputación: La continuidad del proceso depende del marcado del sitio web cuando se efectúa la validación con la imagen facial, de la cual se obtiene un patrón biométrico a contrastar; el mismo que informa sobre la finalidad, plazo de conservación, no transferencia de tales datos biométricos, pero no brinda alguna posibilidad de denegar expresamente tal consentimiento, a la vez que se hace mención al contraste con la información que almacena Reniec, sin señalar su base de datos “BIOM”.
149. Lo anterior resume una conducta que concretaría la obtención del consentimiento sin cumplir completamente con el requisito de información, ni mucho menos los del consentimiento libre y expreso; lo cual es necesario para legitimar el tratamiento de los patrones biométricos faciales para la validación de identidad, toda vez que las normas sectoriales, como ya se vio, no obligan a la administrada a emplear la verificación de ese tipo.
150. En sus descargos de noviembre de 2023, la administrada señaló que el tratamiento de datos biométricos cuestionados, al tener por finalidad velar por la seguridad de los usuarios y el cumplimiento de la normativa sectorial que se le aplica, configuran las excepciones a la obligatoriedad del consentimiento, previstas en los numerales 5, 9 y 13 del artículo 14 de la LPDP y que tales datos no son empleados para otras finalidades.
151. Respecto de las excepciones contempladas en los numerales 5 y 9 de dicho artículo de la LPDP, relativos a los intereses individuales de los usuarios, es preciso tener en cuenta lo ya dilucidado en esta resolución: Para la verificación de la identidad de los usuarios del libro de reclamaciones virtual, el empleo de los patrones biométricos faciales resulta excesivo, por lo que excede del ámbito necesario para esta actividad complementaria de sus servicios (las reclamaciones y quejas), no configurando los supuestos previstos en tales numerales.
152. Sobre lo concerniente al numeral 13 del mismo artículo, debe reiterarse que las normas sectoriales no disponen que el empleo de datos biométricos como única forma de verificación de identidades ni la requerida en algún caso especial, así como el hecho de que no existe alguna norma de rango legal que autorice o requiera tal tratamiento de datos, aparte de las disposiciones sectoriales que se refirieron líneas arriba.
153. Acerca del acatamiento del principio de Calidad alegado por la administrada, es pertinente señalar que el mismo busca preservar la utilidad y actualización de los datos personales a fin de contribuir al cumplimiento de las finalidades, estando como presupuesto para su exigibilidad que se aplique sobre datos personales necesarios para la finalidad preestablecida y reconocida que constituiría, por tanto, de tratamiento legítimo.
154. En lo concerniente a la imposibilidad de imponer una segunda sanción por los hechos analizados en este expediente, a fin de evitar la configuración del *Non bis in ídem*, es necesario indicar que la primera infracción se comienza a configurar con recopilación de los datos biométricos, siendo posterior el almacenamiento de estos en la base de datos “BIOM”, lo cual genera una segunda obligación, que es la de obtener el consentimiento válido para tales acciones.

Esta es una copia auténtica imprimible de un documento electrónico archivado por el Ministerio de Justicia y Derechos Humanos, aplicando lo dispuesto por el Art. 25 de D.S. 070-2013-PCM y la Tercera Disposición Complementaria Final del D.S. 026-2016-PCM. Su autenticidad e integridad pueden ser contrastadas a través de la siguiente dirección web: https://sgd.minjus.gob.pe/gesdoc_web/login.jsp e ingresando el Tipo de Documento, Número y Rango de Fechas de ser el caso o https://sgd.minjus.gob.pe/gesdoc_web/verifica.jsp e ingresando Tipo de Documento, Número, Remitente y Año, según corresponda.

Resolución Directoral N° 2271-2023-JUS/DGTAIPD-DPDP

155. De acuerdo con lo obrante en el expediente, la administrada emplea el texto informativo transrito en el considerando 147 de esta resolución, alcanzando información sobre ciertos pormenores del tratamiento (finalidad y plazo del tratamiento, así como modalidades de ejercicio de los derechos ARCO), sin permitir manifestar expresamente al usuario su voluntad para consentir o denegar el consentimiento respectivo.
156. Entonces, la administrada carece de un mecanismo que permita obtener este consentimiento válidamente, incumpliendo los requisitos de información de emitirse de forma expresa e indubitable, el mismo que en el caso de los datos sensibles debe constar en un soporte escrito o similar donde figure la manifestación del titular de los datos personales; al tiempo que tampoco es libre, toda vez que se condiciona la continuidad del proceso de interposición de reclamación o queja a la aprobación del aviso informativo.
157. Por consiguiente, la administrada configura la conducta infractora tipificada en el literal b) del numeral 2 del artículo 132 del Reglamento de la LPDP.

X. Sobre la determinación de las sanciones a aplicar

158. La Tercera Disposición Complementaria Modificatoria del Reglamento del Decreto Legislativo N° 1353, modificó el artículo 38 de la LPDP que tipificaba las infracciones a la LPDP y su reglamento, incorporando el artículo 132 al Título VI sobre Infracciones y Sanciones de dicho reglamento, que en adelante tipifica las infracciones.
159. Por su parte, el artículo 39 de la LPDP establece las sanciones administrativas calificándolas como leves, graves o muy graves y su imposición va desde una multa de cero coma cinco (0,5) unidades impositivas tributarias hasta una multa de cien (100) unidades impositivas tributarias²⁹, sin perjuicio de las medidas correctivas que puedan determinarse de acuerdo con el artículo 118 del Reglamento de la LPDP³⁰.
160. En el presente caso, se ha establecido la responsabilidad por lo siguiente:
 - Haber realizado el tratamiento desproporcionado de los datos personales de quienes generan un reclamo a través del libro de reclamaciones virtual

²⁹ **Artículo 39. Sanciones administrativas**

En caso de violación de las normas de esta Ley o de su reglamento, la Autoridad Nacional de Protección de Datos Personales puede aplicar las siguientes multas:

1. Las infracciones leves son sancionadas con una multa mínima desde cero coma cinco de una unidad impositiva tributaria (UIT) hasta cinco unidades impositivas tributarias (UIT).
2. Las infracciones graves son sancionadas con multa desde más de cinco unidades impositivas tributarias (UIT) hasta cincuenta unidades impositivas tributarias (UIT).
3. Las infracciones muy graves son sancionadas con multa desde más de cincuenta unidades impositivas tributarias (UIT) hasta cien unidades impositivas tributarias (UIT).

(...)

³⁰ **Artículo 118.- Medidas cautelares y correctivas.**

Una vez iniciado el procedimiento sancionador, la Dirección de Sanciones podrá disponer, mediante acto motivado, la adopción de medidas de carácter provisional que aseguren la eficacia de la resolución final que pudiera recaer en el referido procedimiento, con observancia de las normas aplicables de la Ley N° 27444, Ley del Procedimiento Administrativo General.

Asimismo, sin perjuicio de la sanción administrativa que corresponda por una infracción a las disposiciones contenidas en la Ley y el presente reglamento, se podrán dictar, cuando sea posible, medidas correctivas destinadas a eliminar, evitar o detener los efectos de las infracciones.

Esta es una copia auténtica imprimible de un documento electrónico archivado por el Ministerio de Justicia y Derechos Humanos, aplicando lo dispuesto por el Art. 25 de D.S. 070-2013-PCM y la Tercera Disposición Complementaria Final del D.S. 026-2016-PCM. Su autenticidad e integridad pueden ser contrastadas a través de la siguiente dirección web: https://sgd.minjus.gob.pe/gesdoc_web/login.jsp e ingresando el Tipo de Documento, Número y Rango de Fechas de ser el caso o https://sgd.minjus.gob.pe/gesdoc_web/verifica.jsp e ingresando Tipo de Documento, Número, Remitente y Año, según corresponda.

Resolución Directoral N° 2271-2023-JUS/DGTAIPD-DPDP

publicado en su sitio web, al recopilar imágenes del DNI y de la imagen facial para tratarla con medios técnicos específicos para identificación a través de la validación biométrica (patrón biométrico facial, dato sensible), que no es adecuado, necesario ni pertinente para la finalidad de identificar plenamente al reclamante, incumpliendo lo dispuesto en los artículos 7 y numeral 3 del artículo 28 de la LPDP.

- Haber realizado el tratamiento de los datos personales de quienes generan un reclamo, al almacenar el dato biométrico de la imagen facial en una base de datos propia, sin obtener válidamente el consentimiento de sus titulares, incumpliendo con la obligación establecida en los artículos 5 y 13 de la LPDP, así como de los artículos 7 y 12 de su reglamento.
161. Con el objeto de establecer las pautas y criterios para realizar el cálculo del monto de las multas por infracciones a la normativa de protección de datos personales en el ejercicio de la potestad sancionadora de la Autoridad Nacional de Protección de Datos Personales, se aprobó la Metodología para el Cálculo de Multas³¹.
162. Sobre la base de tal documento, se determinará el monto de la sanción a imponer en cada caso.

Haber efectuado el tratamiento de datos personales sensibles (datos biométricos), siendo estos excesivos, no necesarios ni adecuados para su finalidad

Se ha determinado la comisión de la infracción grave tipificada en el literal d) del numeral 2 del artículo 132 del Reglamento de la LPDP, a la cual, de acuerdo con lo establecido en el numeral 2 del artículo 39 de la LPDP, corresponde una multa desde más de cinco (5) UIT hasta cincuenta (50) UIT.

El beneficio ilícito no se ha podido determinar, pues en el trámite del procedimiento administrativo sancionador se ha verificado que la administrada no retuvo ningún ingreso como consecuencia de la infracción; así como tampoco se tiene información sobre el monto que ahorró, ahorraría o pensaba ahorrar cometiendo la infracción (costos evitados).

En la medida que el beneficio ilícito es indeterminable, para determinar el monto de la multa corresponde aplicar la “multa pre establecida”, cuya fórmula general es:

$$M = Mb \times F, \text{ donde:}$$

M	Multa pre establecida que corresponderá aplicar en cada caso.
Mb	Monto base de la multa. Depende de la gravedad del daño del bien jurídico protegido: variable absoluta y relativa.
F	Criterios o elementos agravantes o atenuantes.

Bajo la fórmula de la multa pre establecida, el monto de la misma es producto del Monto Base (variable absoluta y la variable relativa) por los factores atenuantes o agravantes que se hayan presentado, conforme al inciso 3 del artículo 248 de la LPAG, así como los artículos 125 y 126 del Reglamento de la LPDP.

³¹ Documento disponible en: <https://bni.minjus.gob.pe/bni/>

Resolución Directoral N° 2271-2023-JUS/DGTAIPD-DPDP

La variable absoluta da cuenta del rango en el que se encontraría la multa aplicable, dependiendo de si es una infracción muy grave, grave o leve. Por su parte, la variable relativa determina valores específicos dependiendo de la existencia de condiciones referidas al daño al bien jurídico protegido, como se aprecia en el siguiente gráfico:

Cuadro 2
Montos base de multas pre establecidas (Mb),
según variable absoluta y relativa de la infracción

Gravedad de la infracción	Multa UIT					Variable relativa y monto base (Mb)	
	Min	Máx	1	2	3	4	5
Leve	0.5	5	1.08	2.17	3.25		
Grave	5	50	7.50	15.00	22.50	30.00	37.50
Muy grave	50	100			55.00	73.33	91.67

Siendo que en el presente caso se ha acreditado la responsabilidad administrativa de la administrada conforme a la tipificación establecida en el literal d) del numeral 2 del artículo 132 del Reglamento de la LPDP, corresponde el grado relativo "3" lo cual significa que la multa tendrá como Mb (Monto base) 22,50 UIT, conforme al siguiente gráfico:

N°	Infracciones graves	Grado relativo
2.d	Recopilar datos personales sensibles que no sean necesarios, pertinentes ni adecuados con relación a las finalidades determinadas, explícitas y lícitas para las que requieren ser obtenidos.	3

Ahora, conforme a lo expuesto, el Mb debe multiplicarse por F, el valor atribuido a cada uno de los factores agravantes y atenuantes previstos en la normativa.

Cuadro 3 Valores de factores agravantes y atenuantes		
f_n	Factores agravantes o atenuantes	Valor
$f_{1,1}$	(d) Perjuicio económico causado	
$f_{1,2}$	- 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 interés público.	0.30
$f_{3,4}$	- Cuando la infracción es de carácter instantáneo y genera riesgo de afectación de otros derechos.	0.15
$f_{3,5}$	- Cuando la duración de la infracción es mayor a 24 meses.	0.25
$f_{3,6}$	- Entorpecimiento en la investigación y/o durante el procedimiento.	0.15
$f_{3,7}$	- 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

Esta es una copia auténtica imprimible de un documento electrónico archivado por el Ministerio de Justicia y Derechos Humanos, aplicando lo dispuesto por el Art. 25 de D.S. 070-2013-PCM y la Tercera Disposición Complementaria Final del D.S. 026-2016-PCM. Su autenticidad e integridad pueden ser contrastadas a través de la siguiente dirección web: https://sgd.minjus.gob.pe/gesdoc_web/login.jsp e ingresando el Tipo de Documento, Número y Rango de Fechas de ser el caso o https://sgd.minjus.gob.pe/gesdoc_web/verifica.jsp e ingresando Tipo de Documento, Número, Remitente y Año, según corresponda.

Resolución Directoral N° 2271-2023-JUS/DGTAIPD-DPDP

En el presente caso, no se tiene sustento de que se haya provocado un perjuicio económico con la conducta infractora.

Por su parte, de acuerdo con los hechos que subyacen del expediente y de lo comunicado por la administrada, efectúan la recopilación de los datos personales biométricos de un numero considerable de personas entre clientes, "clientes intermitentes" y meros usuarios, no siendo necesario, a través de su libro de reclamaciones, por lo que corresponde aplicar la agravante por el tratamiento ilícito efectuado a datos personales de más de dos personas (factor f3.2, +20%).

En cuanto a las circunstancias de la infracción, el incumplimiento del numeral 3 del artículo 28 de la LPDP implica la vulneración del principio de Proporcionalidad, mediante el cual se busca evitar el tratamiento indiscriminado de datos personales, por no ser necesarios ni pertinentes a una finalidad lícita y reconocida; limitación que opera sobre la conducta de quienes realizan el tratamiento, creando obligaciones con las que se garantiza la minimización del tratamiento de datos personales y con ello, menguando el riesgo de vulneraciones a los derechos de sus titulares y preservando el dominio sobre su información personal, riesgos que pueden conllevar afectaciones más graves a los derechos de las personas, cuando se trata de datos sensibles (datos biométricos), como en este caso.

Por su parte, en el presente caso, la administrada no reconoció responsabilidad alguna ni presentó medios sustentarios de acciones de enmienda.

De otro lado, entendiendo la intencionalidad en personas jurídicas desde la perspectiva de la inobservancia o no de las normas a las que debe adecuar su comportamiento (calificación de diligencia o negligencia)³², debe tomarse en cuenta que la administrada adoptó las medidas de seguridad necesarias para la preservación de los datos biométricos mencionados, sin perjuicio de que carezca de legitimidad para ello.

En total, los factores de graduación suman un total de 20%, como se muestra en el siguiente cuadro:

Factores de graduación	Calificación
f1. Perjuicio económico causado	0%
f2. Reincidencia	0%
f3. Circunstancias	
f3.2 Cuando la conducta infractora genere riesgo o daño a más de dos personas o grupo de personas	20%
f4. Intencionalidad	0%
f1+f2+f3+f4	20%

³² MORÓN URBINA, Juan Carlos: "Comentarios a la Ley del Procedimiento Administrativo General". Décimo quinta edición. Lima, Gaceta Jurídica, 2020, tomo II, p. 457.

Resolución Directoral N° 2271-2023-JUS/DGTAIPD-DPDP

Considerando lo señalado anteriormente, luego de aplicar la fórmula pre establecida para el cálculo de la multa, el resultado es el siguiente:

Componentes	Valor
Monto base (Mb)	22,50 UIT
Factor de agravantes y atenuantes (F)	1.20
Valor de la multa	27 UIT

Haber efectuado el tratamiento de los datos sensibles (datos biométricos) sin obtener el consentimiento válido de sus titulares

Se ha determinado la comisión de la infracción grave tipificada en el literal b) del numeral 2 del artículo 132 del Reglamento de la LPDP, a la cual, de acuerdo con lo establecido en el numeral 2 del artículo 39 de la LPDP, corresponde una multa desde más de cinco (5) UIT hasta cincuenta (50) UIT.

El beneficio ilícito ha resultado indeterminable, pues en el trámite del procedimiento administrativo sancionador no ha sido posible recabar medios probatorios que evidencien que el infractor haya obtenido o que espere obtener beneficios derivados de no cumplir con las disposiciones establecidas en materia de protección de datos personales, cometiendo la infracción; así como tampoco se tiene información sobre el monto que ahorra, ahoraría o pensaba ahorrar cometiendo la infracción (costos evitados).

En la medida que el beneficio ilícito resulta indeterminable, para determinar el monto de la multa corresponde aplicar la "multa prestablecida", cuya fórmula general es:

$$M = Mb \times F, \text{ donde:}$$

M	Multa pre establecida que corresponderá aplicar en cada caso.
Mb	Monto base de la multa. Depende de la gravedad del daño del bien jurídico protegido: variable absoluta y relativa.
F	Criterios o elementos agravantes o atenuantes.

Bajo la fórmula de la multa prestablecida, el monto de la misma es producto del Monto Base (variable absoluta y la variable relativa) por los factores atenuantes o agravantes que se hayan presentado, conforme al inciso 3 del artículo 248 de la LPAG, así como los artículos 125 y 126 del Reglamento de la LPDP.

La variable absoluta da cuenta del rango en el que se encontraría la multa aplicable, dependiendo de si es una infracción muy grave, grave o leve. Por su parte, la variable relativa determina valores específicos dependiendo de la existencia de condiciones referidas al daño al bien jurídico protegido, como se aprecia en el siguiente gráfico:

Resolución Directoral N° 2271-2023-JUS/DGTAIPD-DPDP

Cuadro 2

Montos base de multas pre establecidas (Mb),
según variable absoluta y relativa de la infracción

Gravedad de la infracción	Multa UIT					Variable relativa y monto base (Mb)	
	Min	Máx	1	2	3	4	5
Leve	0.5	5	1.08	2.17	3.25		
Grave	5	50	7.50	15.00	22.50	30.00	37.50
Muy grave	50	100			55.00	73.33	91.67

Siendo que en el presente caso se ha acreditado la responsabilidad administrativa de la administrada conforme a la tipificación establecida en el literal b) del numeral 2 del artículo 132 del Reglamento de la LPDP, con la circunstancia de tratarse del tratamiento de datos sensibles (datos biométricos), corresponde el grado relativo "4", lo cual significa que la multa tendrá como Mb (Monto base) **30 UIT**, conforme al siguiente gráfico:

N°	Infracciones graves	Grado relativo
2.b	<p>Dar tratamiento a los datos personales sin el consentimiento libre, expreso, inequívoco, previo e informado del titular, cuando el mismo sea necesario conforme a lo dispuesto en la Ley N° 29733 y su Reglamento.</p> <p><u>Datos sensibles (salud y biométricos)</u></p> <p>2.b.8. Consentimiento no cumple con la característica de ser libre.</p>	4

Ahora bien, conforme a lo expuesto, el Mb debe multiplicarse por F, que es el valor atribuido a cada uno de los factores agravantes y atenuantes previstos en la normativa.

Cuadro 3
Valores de factores agravantes y atenuantes

f ₁	Factores agravantes o atenuantes	Valor
f _{1.1}	(d) Perjuicio económico causado	
f _{1.1.1}	No existe perjuicio.	0.00
f _{1.1.2}	Existiría perjuicio económico sobre el denunciante o reclamante.	0.10
f _{1.2}	(e) Reincidencia	
f _{1.2.1}	No hay reincidencia.	0.00
f _{1.2.2}	Primeras reincidencias.	0.20
f _{1.2.3}	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 interés 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}	· Cuando la duración de la infracción es mayor a 24 meses.	0.25
f _{3.6}	· Entorpecimiento en la investigación y/o durante el procedimiento.	0.15
f _{3.7}	· 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

Esta es una copia auténtica imprimible de un documento electrónico archivado por el Ministerio de Justicia y Derechos Humanos, aplicando lo dispuesto por el Art. 25 de D.S. 070-2013-PCM y la Tercera Disposición Complementaria Final del D.S. 026-2016-PCM. Su autenticidad e integridad pueden ser contrastadas a través de la siguiente dirección web: https://sgd.minjus.gob.pe/gesdoc_web/login.jsp e ingresando el Tipo de Documento, Número y Rango de Fechas de ser el caso o https://sgd.minjus.gob.pe/gesdoc_web/verifica.jsp e ingresando Tipo de Documento, Número, Remitente y Año, según corresponda.

Resolución Directoral N° 2271-2023-JUS/DGTAIPD-DPDP

En el presente caso, de los medios probatorios que obran en el expediente no se verifica un perjuicio económico causado. Asimismo, se tiene conocido que la administrada no es reincidente respecto de hechos como el analizado en el presente expediente, dado que se trata del tratamiento de datos biométricos.

Por su parte, de acuerdo con los hechos que subyacen del expediente y de lo comunicado por la administrada, efectúan la recopilación de los datos personales biométricos de un número considerable de personas entre clientes, "clientes intermitentes" y meros usuarios, a través de su libro de reclamaciones, por lo que corresponde aplicar la agravante por el tratamiento ilícito efectuado a datos personales de más de dos personas (factor f3.2, +20%).

El incumplimiento del artículo 13.5 del artículo 13 de la LPDP y de lo dispuesto en el artículo 12 del reglamento de dicha ley, debe señalarse que implica la vulneración de uno de los principios del tratamiento de datos personales, como es el principio de Consentimiento, el cual es la principal garantía de la autodeterminación informativa reconocida por el Tribunal Constitucional en la sentencia recaída en el expediente N° 4387-2011-PHD/TC y que adquiere mayor importancia al tratarse de datos biométricos por el mayor riesgo que conlleva su tratamiento de datos personales.

Por su parte, en el presente caso, la administrada no reconoció responsabilidad alguna ni presentó medios sustentarios de acciones de enmienda.

De otro lado, entendiendo la intencionalidad en personas jurídicas desde la perspectiva de la inobservancia o no de las normas a las que debe adecuar su comportamiento (calificación de diligencia o negligencia), debe tomarse en cuenta que la administrada adoptó las medidas de seguridad necesarias para la preservación de los datos biométricos mencionados, sin perjuicio de que carezca de legitimidad para ello.

En total, los factores de graduación suman un total de 20%:

Factores de graduación	Calificación
f1. Perjuicio económico causado	0%
f2. Reincidencia	0%
f3. Circunstancias	
f3.2 Cuando la conducta infractora genere riesgo o daño a más de dos personas o grupo de personas	20%
f4. Intencionalidad	0%
f1+f2+f3+f4	20%

Considerando lo señalado anteriormente, luego de aplicar la fórmula pre establecida para el cálculo de la multa, el resultado es el siguiente:

Resolución Directoral N° 2271-2023-JUS/DGTAIPD-DPDP

Componentes	Valor
Monto base (Mb)	30 UIT
Factor de agravantes y atenuantes (F)	1.20
Valor de la multa	36 UIT

Por las consideraciones expuestas y de conformidad con lo dispuesto por la LPDP y su reglamento, la LPAG, y el Reglamento del Decreto Legislativo N° 1353;

SE RESUELVE:

Artículo 1.- Sancionar al Banco de Crédito del Perú con la multa ascendente a veintisiete Unidades Impositivas Tributarias (27 UIT) por haber efectuado el tratamiento de datos sensibles (datos biométricos) que resultan excesivos, no necesario, adecuados ni pertinentes para el uso de su libro de reclamaciones virtual, en incumplimiento de lo dispuesto en los artículos 7 y numeral 3 del artículo 28 de la LPDP, configurando la infracción grave tipificada en el literal d) del numeral 2 del artículo 132 del Reglamento de la LPDP.

Artículo 2.- Sancionar al Banco de Crédito del Perú con la multa ascendente a treinta y seis Unidades Impositivas Tributarias (36 UIT) por haber efectuado el tratamiento de datos sensibles (datos biométricos) de los usuarios de su libro de reclamaciones virtual, sin su consentimiento válido contrariando lo dispuesto en el numeral 13.5 y 13.6 del artículo 13 de la LPDP y el artículo 12 del Reglamento de la LPDP; infracción grave tipificada en el literal b) del inciso 2 del artículo 132 del Reglamento de la LPDP.

Artículo 3.- Imponer como medidas correctivas al Banco de Crédito del Perú las siguientes:

- Suprimir los patrones biométricos faciales almacenados en la base de datos "BIOM".
- Cesar el almacenamiento de patrones biométricos obtenidos desde la imagen facial de los usuarios de su libro de reclamaciones virtual, así como el uso de estos para la validación de las identidades de estos.
- Remitir documentación sustentatoria de la implementación de ambas medidas correctivas.

Para el cumplimiento de tales medidas correctivas, se otorga el plazo de cincuenta y cinco días hábiles (55) días hábiles contados a partir de la notificación de la presente resolución. En caso de presentar recurso impugnatorio el plazo para el cumplimiento de la medida correctiva es de cuarenta (40) días hábiles de notificada la resolución que resuelve dicho recurso y agota la vía administrativa.

Artículo 4.- Informar al Banco de Crédito del Perú que el incumplimiento de la medida correctiva dispuesta en el artículo precedente, una vez vencido el plazo señalado, habilita a efectuar las acciones de fiscalización encaminadas al inicio de un procedimiento sancionador por la presunta comisión de la infracción muy grave tipificada en el literal d) del numeral 3 del artículo 132 del Reglamento de la LPDP.

Artículo 5.- Informar al Banco de Crédito del Perú que, contra la presente resolución directoral, de acuerdo con lo indicado en el artículo 218 de la LPAG, proceden

Esta es una copia auténtica imprimible de un documento electrónico archivado por el Ministerio de Justicia y Derechos Humanos, aplicando lo dispuesto por el Art. 25 de D.S. 070-2013-PCM y la Tercera Disposición Complementaria Final del D.S. 026-2016-PCM. Su autenticidad e integridad pueden ser contrastadas a través de la siguiente dirección web: https://sgd.minjus.gob.pe/gesdoc_web/login.jsp e ingresando el Tipo de Documento, Número y Rango de Fechas de ser el caso o https://sgd.minjus.gob.pe/gesdoc_web/verifica.jsp e ingresando Tipo de Documento, Número, Remitente y Año, según corresponda.

Resolución Directoral N° 2271-2023-JUS/DGTAIPD-DPDP

los recursos de reconsideración o apelación dentro de los quince (15) días hábiles posteriores a su notificación³³.

Artículo 6.- Informar al Banco de Crédito del Perú que, vencido el plazo para interponer recurso impugnatorio o, de ser el caso, al día siguiente de recibida la resolución que resuelve el recurso impugnatorio, se entiende que el acto administrativo del resuelve el procedimiento administrativo queda firme conforme a lo dispuesto en el artículo 222 de la LPAG; y que se considera inscrita la sanción impuesta en la presente resolución directoral, en el Registro Nacional de Protección de Datos Personales.

Artículo 7.- Informar al Banco de Crédito del Perú que deberá realizar el pago de la multa en el plazo de veinticinco (25) días hábiles desde el día siguiente de notificada la presente resolución directoral³⁴.

Artículo 8.- En caso se presente recurso impugnatorio, el plazo para pagar la multa es de diez (10) días hábiles de notificada la resolución que agota la vía administrativa, plazo que se contará desde el día siguiente de notificada dicha resolución de segunda instancia administrativa, de acuerdo con lo establecido en el numeral 4 del artículo 143 de la LPAG³⁵.

Artículo 9.- Se entenderá que cumplió con pagar la multa impuesta, si antes de que venzan los plazos mencionados, cancela el sesenta por ciento (60%) de la multa impuesta conforme a lo dispuesto en el artículo 128 del Reglamento de la LPDP³⁶. Para el pago de la multa, se deberá tener en cuenta el valor de la UIT del año 2022.

Artículo 10.- Notificar al Banco de Crédito del Perú la presente resolución directoral.

³³ **Artículo 218. Recursos administrativos**

218.1 Los recursos administrativos son:

a) Recurso de reconsideración

b) Recurso de apelación

Solo en caso que por ley o decreto legislativo se establezca expresamente, cabe la interposición del recurso administrativo de revisión.

218.2 El término para la interposición de los recursos es de quince (15) días perentorios, y deberán resolverse en el plazo de treinta (30) días.

³⁴ El pago de la multa puede ser realizado en el Banco de la Nación con el código 04759.

³⁵ **Artículo 143.- Plazos máximos para realizar actos procedimentales**

A falta de plazo establecido por ley expresa, las actuaciones deben producirse dentro de los siguientes:

(...)

4. Para actos de cargo del administrado requeridos por la autoridad, como entrega de información, respuesta a las cuestiones sobre las cuales deban pronunciarse: dentro de los diez días de solicitados.

³⁶ **Artículo 128.- Incentivos para el pago de la sanción de multa.**

Se considerará que el sancionado ha cumplido con pagar la sanción de multa si, antes de vencer el plazo otorgado para pagar la multa, deposita en la cuenta bancaria determinada por la Dirección General de Protección de Datos Personales el sesenta por ciento (60%) de su monto. Para que surta efecto dicho beneficio deberá comunicar tal hecho a la Dirección General de Protección de Datos Personales, adjuntando el comprobante del depósito bancario correspondiente. Luego de dicho plazo, el pago sólo será admitido por el íntegro de la multa impuesta.

Resolución Directoral N° 2271-2023-JUS/DGTAIPD-DPDP

Artículo 11.- Notificar a la denunciante la presente resolución directoral, con finalidad informativa.

Regístrese y comuníquese.



Firmado digitalmente
por GONZALEZ LUNA
Maria Alejandra FAU
20131371617 soft

María Alejandra González Luna
Directora (e) de Protección de Datos Personales

MAGL/rvr

Esta es una copia auténtica imprimible de un documento electrónico archivado por el Ministerio de Justicia y Derechos Humanos, aplicando lo dispuesto por el Art. 25 de D.S. 070-2013-PCM y la Tercera Disposición Complementaria Final del D.S. 026-2016-PCM. Su autenticidad e integridad pueden ser contrastadas a través de la siguiente dirección web: https://sgd.minjus.gob.pe/gesdoc_web/login.jsp e ingresando el Tipo de Documento, Número y Rango de Fechas de ser el caso o https://sgd.minjus.gob.pe/gesdoc_web/verifica.jsp e ingresando Tipo de Documento, Número, Remitente y Año, según corresponda.