Resolución Directoral N° 655-2022-JUS/DGTAIPD-DPDP

Expediente N°
025-2021-JUS/DGTAIPD-PAS

Lima, 14 de febrero de 2022

VISTOS:

El Informe N° 003-2022-JUS/DGTAIPD-DFI del 13 de enero de 2022[1], 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. El 17 de octubre de 2021 se difundió un reportaje televisivo del programa "Punto Final", en el cual se ponía en conocimiento del público acciones de tratamiento inadecuado de datos personales por parte del personal de la Superintendencia Nacional de Migraciones (en adelante, la administrada), responsable de la atención en los módulos de control migratorio del Aeropuerto Internacional Jorge Chávez; tratamiento que consistía en obtener fotografías de los reportes migratorios arrojados por el Sistema Integrado de Migraciones - SIM y de los pasaportes de ciertas personas públicas, para su posterior transmisión a otros empleados que no habían atendido al titular de la información.

2. Habiendo tomado conocimiento de ello, el 18 de octubre de 2021, la DFI dispuso a través de la Orden de Fiscalización N° 288-2021-JUS/DGTAIPD-DFI[2], el inicio de acciones de fiscalización sobre la administrada, iniciando con una visita de fiscalización a la sede de atención del aeropuerto Jorge Chávez.

3. Durante dicha visita de fiscalización, el personal de la DFI dejó constancia en el Acta de Fiscalización N° 01-2021-DFI[3], respecto del empleo del Sistema Integrado de Migraciones – SIM y de los dispositivos con los que se le utiliza, de lo siguiente:

[1] Folios 500 al 536
[2] Folio 2
[3] Folios 3 al 41

- Dicho sistema es operado por empleados de la administrada en los módulos de control migratorio, cada uno, por medio de 39 computadoras desde las que se puede acceder a la información migratoria de ciudadanos peruanos y extranjeros.
- Dichas computadoras cuentan con los puertos USB y grabador de DVD habilitados, comprobándose la efectiva copia de archivos en un dispositivo USB (Anexo 1)[4].
- Las computadoras mencionadas no restringen el envío de información a correos no institucionales de la administrada, ni emiten alertas respecto del envío de información a correos no autorizados (Anexo 3)[5].
- Se comprobó que no se requiere contraseña para el uso del equipo multifuncional de fotocopiado del área fiscalizada (Anexo 4)[6].
- Por medio del Sistema Integrado de Migraciones - SIM, se puede acceder a los siguientes datos personales: Número de documento de identidad, nombres y apellidos, fecha de nacimiento, nacionalidad, estado civil, ocupación, teléfono, estatura, color de cabello, color de ojos, huella digital, sexo, destino de viaje, motivo de viaje, categoría de pasajero, fechas de ingreso y salida al país, países de procedencia y destino (Anexo 5)[7].

4. Aparte de lo señalado, se incluyeron en un CD adjunto los siguientes elementos[8]:

- Entrevistas a siete inspectores de migración en sus respectivos módulos, respecto del uso de sus teléfonos móviles durante su horario de trabajo.
- Grabaciones del teléfono móvil de la Oficial III de Migraciones, en el que se aprecia las conversaciones de WhatsApp de servidores de la administrada con la Jefe Zonal Callao, en la cual esta solicitaba que se le comparta información sobre “personalidades” y se remitían imágenes de datos de estas, tomadas en los respectivos módulos, al momento de pasar por estos.

5. Por medio del Oficio N° 133-2021-JUS/DGTAIPD-DFI del 19 de octubre de 2021, se solicitó a la administrada informar sobre lo siguiente:

- Si los números de teléfono [redacted] habían sido asignados a quienes ejercieron la Jefatura de la Zonal Callao en el 2021, o si fueron declarados por tales servidoras.
- La identificación de los funcionarios que durante el 2021 laboraron en el puesto migratorio del Aeropuerto Internacional Jorge Chávez, con sus respectivos números de teléfonos móviles, declarado o asignado por la entidad.
- La documentación de los procedimientos de gestión de acceso, de gestión de privilegios y de verificación periódica de privilegios aplicables al Sistema Integrado de Migraciones - SIM.
- La generación de registros de interacción lógica de acciones de inicio y cierre de sesión, así como de acciones relevantes, correspondientes a la trazabilidad de los usuarios del mencionado sistema.

[4] Folios 6 al 13
[5] Folios 18 al 20
[6] Folio 21
[7] Folios 22 al 40
[8] Folio 41

6. De otro lado, mediante el Oficio N° 134-2021-JUS/DGTAIPD-DPDP del 19 de octubre de 2021, se programó una siguiente visita de fiscalización, para el 22 de octubre de 2021.

7. A su vez, por medio del Oficio N° 135-2021-JUS/DGTAIPD-DPDP, se solicitó al Organismo Supervisor de la Inversión Privada en Telecomunicaciones – Osiptel, informar sobre los datos de los titulares de número de teléfonos móviles que habrían sido utilizados para el tratamiento de datos personales cuestionado.

8. Se consignó en el Acta de Fiscalización N° 02-2021-DFI del 22 de octubre de 2021[9], la siguiente declaración de la Jefe Zonal del Callao:

   - En el puesto de control migratorio del Aeropuerto Internacional Jorge Chávez, se dispuso la creación de un grupo de WhatsApp, integrado por esta funcionaria, cuatro supervisores y ocho coordinares de dicha área; teniendo como finalidad, la elaboración de un reporte diario de ocurrencias, sin que haya un informe oficial diario de las mismas, si no que se efectúa un informe puntual al Director de Operaciones, por dicha vía, sobre “personalidades”.
   - Cada supervisor está a cargo de un grupo, sin que se sepa si en el interior de cada grupo se formó otro grupo aparte en WhatsApp para reportar incidencias sobre “personalidades”.
   - Desconoce sobre el uso de teléfonos móviles en el interior de los módulos de dicho puesto de control.
   - Los ciudadanos peruanos que generan una alerta, son reportados sincrónicamente a la Policía Nacional del Perú, en atención a un Oficio que figure en el sistema, informando el motivo de alerta.

9. Asimismo, se consignó la declaración del Director de Operaciones de la administrada, que manifestó lo siguiente:

   - Como encargado de todas las jefaturas zonales de migraciones desde octubre de 2020, informó sobre un grupo de WhatsApp para el reporte de incidencias, integrado por él y los diecisiete jefes zonales.
   - Nunca autorizó la captura fotográfica de los datos personales de los ciudadanos, que se visualizan en el Sistema Integrado de Migraciones – SIM, ni ha coordinado con la Jefe Zonal del Callao, a cargo del puesto de control migratorio del Aeropuerto Internacional Jorge Chávez que se le reporte de forma diaria y en tiempo real el ingreso o salida de “personalidades”.
   - Desconoce la existencia de algún grupo de WhatsApp integrado por los mencionados jefes zonales y sus respectivos subordinados, para coordinación.
   - Desconoce la finalidad del reporte de “personalidad” a través de la imagen de sus datos personales y de su entrada o salida del país.

10. Por su parte, la Oficial de Seguridad de la Información y la Oficial de Protección de Datos Personales declararon que desconocían del uso de la aplicación WhatsApp para transmitir la información tratada a través del Sistema Integrado de

[9] Folios 53 al 162

Migraciones – SIM, motivo por el cual no cuentan con documentos de gestión del empleo de dicha aplicación.

11. Se adjuntó a la mencionada acta de fiscalización la documentación de los procedimientos de gestión de acceso, de gestión de privilegios y de verificación periódica de privilegios, así como los documentos laborales del personal del puesto de control migratorio del Aeropuerto Internacional Jorge Chávez.

12. Mediante el Oficio N° 000223-2021-OTIC/MIGRACIONES, ingresado con la Hoja de Trámite N° 288517 del 5 de noviembre de 2021[10], la administrada dio respuesta al requerimiento que se le hizo, informando lo siguiente:

    - En el Informe N° 000199-2021-RAVUAP/MIGRACIONES, se señala que los números de teléfono móvil [redacted], fueron declarados como números personales, como figura en sus respectivos legajos.
    - En el Informe N° 000037-2021-JMSUST/MIGRACIONES se precisa que a las funcionarias que ejercieron la Jefatura Zonal del Callao, se les asignaron equipos móviles institucionales, de acuerdo con las actas de entrega respectivas.

13. Por medio del Oficio N° 142-2021-JUS/DGTAIPD-DFI del 9 de noviembre, se solicitó a la administrada informar sobre lo siguiente:

    - Los procedimientos regulares para la obtención del reporte migratorio de los ciudadanos peruanos y extranjeros
    - Las funciones específicas de la jefa del puesto de control migratorio de la Superintendencia Nacional de Migraciones de la dependencia del Aeropuerto Internacional Jorge Chávez
    - Las funciones específicas de los supervisores, coordinadores de grupo, y los inspectores u oficiales migratorios
    - La finalidad del reporte diario de ocurrencias de “personalidades”, mediante la aplicación de mensajería WhatsApp y a través de qué medio se ordenó a la Jefa Zonal del Callao obtener estos reportes de ocurrencias.

14. Asimismo, por medio de la Carta N° 523-2021-JUS/DGTAIPD-DFI, se solicitó a la Jefa Zonal del Callao al 18 de octubre de 2021, informar sobre la finalidad del reporte diario de ocurrencias de “personalidades”, mediante la aplicación de mensajería WhatsApp, a través de qué medio se le ordenó obtener estos reportes y cómo remitía estos al Director de Operaciones de la administrada.

15. De otro lado, el 10 de noviembre de 2021, personal de la administrada entregó un USB con información referida a la generación de registros de interacción lógica de las acciones de los usuarios del Sistema Integrado de Migraciones – SIM, registrando tal entrega en el acta firmada por el Analista de Fiscalización en Seguridad de la Información de la DFI[11].

[10] Folios 183 al 271
[11] Folios 282 y 283

16. Por medio de la Carta N° 06244-DAPU.I/2021, ingresada con la Hoja de Trámite N° 297774-2021MSC del 11 de noviembre de 2021[12], el Osiptel remitió la información que se le había requerido.

17. Mediante la carta ingresada con la Hoja de Trámite N° 303776-2021MSC del 16 de noviembre de 2021, la Jefe Zonal del Callao dio respuesta a la Carta N° 523-2021-JUS/DGTAIPD-DFI, indicando que el reporte de ocurrencia que recibían de los supervisores y coordinadores era sobre cualquier incidencia que se presente en el puesto de control migratorio del Aeropuerto Internacional Jorge Chávez y que no hubo una orden expresa por parte de algún superior, sino que obedecía a cuestiones de momento, como detección de incumplimientos de la normativa migratoria, personas involucradas en casos de relieve ("Los dinámicos del centro"), personalidades, peruanos deportados, entre otros. Se adjuntó a esta carta, diez capturas de pantalla de los reportes y comunicaciones sostenidas con el Director de Operaciones[13].

18. En el Informe Técnico N° 273-2021-DFI-VARS del 17 de noviembre de 2021[14], el Analista de Fiscalización en Seguridad de la Información de la DFI indicó los siguiente:

    - La administrada no establece medidas de seguridad y/o procedimientos que restrinjan la generación de copias o reproducción de documentos y/o información de ciudadanos peruanos y extranjeros que ingresan y salen del territorio nacional, generándose un alto riesgo de fuga de información.
    - Se ha vulnerado la confidencialidad de tales ciudadanos, a través del uso de la aplicación WhatsApp, siguiendo la disposición dictada por la Jefe Zonal Callao, a cargo del puesto de control migratorio del Aeropuerto Internacional Jorge Chávez.

19. Por medio del Informe de Fiscalización N° 302-2021-JUS/DGTAIPD-DFI-JYHV del 19 de noviembre de 2021[15], se remitió a la Directora de la DFI el resultado de la fiscalización a la administrada, concluyendo que se han determinado preliminarmente las circunstancias que justifican el inicio de un procedimiento administrativo sancionador contra ella, relativas al supuesto incumplimiento de lo establecido en la Ley N° 29733, Ley de Protección de Datos Personales (en adelante, LPDP) y su reglamento, aprobado por Decreto Supremo N° 003-2013-JUS (en adelante, Reglamento de la LPDP). Dicho informe fue notificado a la administrada a través de la Cédula de Notificación N° 907-2021-JUS/DGTAIPD-DFI, el 22 de noviembre de 2021[16].

20. Por medio de la Resolución Directoral N° 266-2021-JUS/DGTAIPD-DFI del 6 de diciembre de 2021[17], la DFI resolvió iniciar procedimiento administrativo sancionador a la administrada por la supuesta comisión de los siguientes hechos infractores:

[12] Folios 285 al 287
[13] Folios 289 al 299
[14] Folios 300 al 312
[15] Folios 313 al 339
[16] Folio 345
[17] Folios 359 al 383

- **Hecho imputado N° 1:** No haber garantizado la confidencialidad de los datos de las personas que ingresan y salen del país, debido a que estos eran compartidos a través de grupos de WhatsApp desde los teléfonos móviles personales de los trabajadores del área de control migratorio del Aeropuerto Internacional Jorge Chávez, con lo que se habría incumplido el artículo 17 de la LPDP. Dicha situación configuraría la infracción grave tipificada en el literal g) del numeral 2 del artículo 132 del Reglamento de la LPDP: *"Incumplir la obligación de confidencialidad establecida en el artículo 17 de la Ley N° 29733"*.

- **Hecho imputado N° 2:** No haber implementado las medidas de seguridad necesarias en el módulo de control migratorio del Sistema Integrado de Migraciones "SIM" del Aeropuerto Internacional Jorge Chávez, al no restringir la generación de copias o reproducción de los datos personales de ciudadanos peruanos (que incluyen datos sensibles) y extranjeros que ingresan y salen del país, según se dispone en el artículo 43 del Reglamento de la LPDP. Dicha situación configuraría la infracción grave tipificada en el literal c) del numeral 2 del artículo 132 del Reglamento de la LPDP: *"Realizar tratamiento de datos personales sensibles incumpliendo las medidas de seguridad establecidas en la normativa sobre la materia"*.

21. A través de la Cédula de Notificación N° 962-2021-JUS/DGTAIPD-DFI[18] se notificó a la administrada dicha resolución directoral, el 7 de diciembre de 2021.

22. Por medio del escrito ingresado con el Código N° 7861-2021MSC del 4 de enero de 2022[19], la administrada presentó sus descargos ante las imputaciones realizadas, adjuntando documentación y exponiendo lo siguiente:

- En el momento de conocerse los hechos cuestionados, contaban en su Reglamento Interno de Servidores Civiles con prohibiciones de divulgación de la información a la que puedan acceder, dentro o fuera del centro de trabajo; con su "Política de Privacidad, Protección de Datos Personales y No Divulgación", de código E05.GG.POL.001 y habían organizado un curso virtual sobre los alcances de la LPDP el 23 de septiembre de 2021, conjuntamente con el Ministerio de Justicia y Derechos Humanos, habiendo difundido también los Memorándums Múltiples N° 000172-2021- OAJ/MIGRACIONES y N° 000180-2021- OAJ/MIGRACIONES, en el que se exhorta a sus servidores a cumplir con lo establecido en dicha ley, bajo responsabilidad.
- No obra evidencia de que hayan dispuesto alguna norma interna con la que se permita el incumplimiento del artículo 17 de la LPDP.
- La Jefatura Zonal del Callao, en sus comunicaciones, descartó la realización del "reglaje".
- No se ha tenido queja, reclamo o documento alguno referido a alguna actividad ilícita o mal uso de información o mala praxis por parte de los servidores, habiéndose transmitido información en sus grupos de WhatsApp con fines operativos, sin intención de afectar el proceso del control migratorio.

[18] Folio 385
[19] Folios 387 al 494

- Asimismo, la transmisión de dicha información obedecía a la necesidad de mantener reportes rápidos acerca de la inexistencia de problemas y en caso de existir, permitir una intervención inmediata.
- La Oficina de Tecnologías de Información y Comunicaciones, en el Informe N° 000186-2021-OTIC/MIGRACIONES, explica que ha establecido recomendaciones y pautas técnicas para la implementación de medidas de seguridad de la información, así como la Norma Administrativa Interna "S02.OTIC.NAI.007- Seguridad de la Información en el uso de equipos_V01" dirigida a controlar el uso de teléfonos móviles; así como las razones por las que se hallaron las computadoras sin las medidas de seguridad requeridas.

23. En el Informe N° 006-2022-JUS-DFI-ORQR del 12 de enero de 2022[20], el Analista de Fiscalización en Seguridad de la Información concluyó, respecto de la información remitida por la administrada, que no se evidencia la implementación de medidas de seguridad con las que cumpla lo establecido en el artículo 43 del Reglamento de la LPDP.

24. Mediante el Informe N° 099-2021-JUS/DGTAIPD-DFI, la DFI emitió el Informe Final de Instrucción dirigido 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), a fin de remitirle los actuados para que resuelva en primera instancia el procedimiento administrativo sancionador iniciado, recomendando lo siguiente:

- Imponer a la administrada la multa de veintisiete unidades impositivas tributarias (27 UIT) por la comisión de la infracción grave tipificada en el literal g) del numeral 2 del artículo 132 del Reglamento de la LPDP.
- Imponer a la administrada la multa de nueve unidades impositivas tributarias (9 UIT) por la comisión de la infracción grave tipificada en el literal c) del numeral 2 del artículo 132 del Reglamento de la LPDP.

25. Por medio de la Resolución Directoral N° 006-2022-JUS/DGTAIPD-DFI del 12 de enero de 2022[21], la DFI dio por concluidas las actuaciones instructivas correspondientes al procedimiento sancionador.

26. Dichos documentos fueron notificados a la administrada a través de la Cédula de Notificación N° 045-2022-JUS/DGTAIPD-DFI.

27. Mediante el Oficio N° 42-2022-JUS/DGTAIPD-DPDP del 20 de enero de 2022, esta Dirección solicitó a la administrada lo siguiente:

- El documento "Política y Objetivos de Seguridad", aprobado por Resolución de Superintendencia N° 000346-2016-MIGRACIONES
- Cargos de recepción y/o correos electrónicos mediante los cuales se haya remitido dicho documento a los servidores
- Documentos adicionales a las actas de entrega de equipos de telefonía móvil institucionales a dichos servidores, de acuerdo con lo detallado en el

[20] Folios 495 al 499
[21] Folios 536 al 539

expediente, por medio de los cuales se haya impartido instrucciones acerca del uso correcto de los mismos, se haya establecido prohibiciones de su uso (de captación de imágenes de información) y otras limitaciones respecto de la información que podían captar con aquellos, con el cargo de recepción de estos documentos, firmado por cada servidor, de ser el caso
- Cargos de recepción y/o correos electrónicos mediante los cuales se haya remitido a los mencionados servidores el Reglamento Interno de Servidores Civiles de la Superintendencia Nacional de Migraciones
- Cargos de recepción y/o correos electrónicos mediante los cuales se haya remitido a los mencionados servidores el Memorando N° 001381- 2021-ORH/MIGRACIONES
- Cargos de recepción y/o correos electrónicos mediante los cuales se haya remitido a los mencionados servidores la Política de Privacidad, Protección de Datos Personales y No Divulgación
- Correos electrónicos de convocatoria al evento de capacitación en protección de datos personales, por medio del Memorando N° 001381- 2021-ORH/MIGRACIONES
- Cargos de recepción y/o correos electrónicos mediante los cuales se haya remitido a los mencionados servidores los memorandos múltiples N° 000172-2021- OAJ/MIGRACIONES y N° 000180-2021- OAJ/MIGRACIONES
- Información acerca de las acciones de investigación y procedimientos llevados a cabo por la Secretaría Técnica del Procedimiento Administrativo Disciplinario a la fecha de su respuesta, sobre los servidores involucrados en los hechos materia de imputación contra su entidad

28. Dicho requerimiento de información fue reiterado por medio del Oficio N° 146-2022-JUS/DGTAIPD-DPDP, notificado el 8 de febrero de 2022, otorgando tres días hábiles para el cumplimiento; a la fecha, habiéndose vencido tal plazo, la administrada no remitió comunicación alguna referida a la totalidad de la información requerida.

29. Por medio del escrito ingresado con código N° 21168-2022MSC del 21 de enero de 2022[22], la administrada solicitó el uso de la palabra en un informe oral, el que se realizó el 2 de febrero de 2022.

30. A su vez, mediante el escrito ingresado con código N° 20900-2022MSC[23], la administrada presentó sus alegatos ante el informe final de fiscalización.

31. Posteriormente, con el escrito ingresado con código N° 42399 del 9 de febrero de 2022[24], la administrada, de acuerdo con lo señalado en el informe oral, remitió información sobre lo siguiente:

    - Indicación respecto de las capturas fotográficas de las personas en que entran y salen por el puesto de control migratorio, indicando si forma parte de la información que, por motivos de trabajo y control, comparten vía WhatsApp los funcionarios involucrados.

[22] Folios 553 al 557
[23] Folios 559 al 668
[24] Folios 675 al 688

- Sobre la existencia de alguna directiva, o reglamento interno o procedimiento de trabajo, alguna clasificación de las personas que atraviesan los controles migratorios, a fin de decidir qué persona se van a compartir los datos, es decir quiénes son consideradas públicas o de alto riesgo.
- Si es que existe algún procedimiento especial en el caso de alguna ocurrencia con las personas denominadas públicas o "personalidades".

32. Dicho ingreso tiene adjunto el Informe N° 00013-2022-JZ17CALLAO/MIGRACIONES[25], firmado por la Jefe Zonal del Callao actualmente en funciones, en el que se pormenoriza la mencionada información.

II. Competencia

33. 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.

34. 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.

III. Normas concernientes a la responsabilidad de la administrada

35. 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 Nº 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.

36. 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 del hecho imputado como infractor, si es realizada de forma previa a la notificación de imputación de cargos y a iniciativa voluntaria por parte de la administrada[26], sin provenir del mandato de la autoridad a través de algún documento mediante el cual se solicite subsanar el acto calificable como infracción, como señala adecuadamente Morón[27].

37. Por su parte, 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

[25] Folio 685 al 688
[26] **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.
[27] MORÓN URBINA, Juan Carlos: "Comentarios a la Ley del Procedimiento Administrativo General". Décimo quinta edición. Lima, Gaceta Jurídica, 2020, tomo II, p. 522.

LPAG[28], 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, pueden conllevar la reducción motivada de la sanción hasta por debajo del rango previsto en la LPDP[29].

38. 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 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

39. 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.- Caracteres 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.*
> *(…)"*

40. 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*

[28] **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.

[29] **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.

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."

41. 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.

42. 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.

43. 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, y sin que ello conlleve una vulneración de la predictibilidad o de la expectativa legítima del administrado, la cual no encuentra asidero en la normativa referida al procedimiento administrativo.

44. 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: Acerca del tratamiento de la responsabilidad proactiva requerida para el tratamiento de los datos personales de los ciudadanos que entran y salen del país

45. La LPDP contiene la definición de lo que son datos personales, la misma que comprende la categoría de los datos sensibles, según lo transcrito a continuación:

"Artículo 2. Definiciones
Para todos los efectos de la presente Ley, se entiende por:
(…)
4. Datos personales. *Toda información sobre una persona natural que la identifica o la hace identificable a través de medios que pueden ser razonablemente utilizados.*
5. Datos sensibles. *Datos personales constituidos por los datos biométricos que por sí mismos pueden identificar al titular; datos referidos al origen racial*

y étnico; ingresos económicos; opiniones o convicciones políticas, religiosas, filosóficas o morales; afiliación sindical; e información relacionada a la salud o a la vida sexual."

46. Dicha definición, a su vez, guarda evidente relación con la contenida en los Estándares de Protección de Datos Personales para los Estados Iberoamericanos, aprobados por la Red Iberoamericana de Protección de Datos en el 2017 como directrices para la modernización de las normativas vigentes en protección de datos personales (en adelante, EPDP):

> ***"2. Definiciones***
> ***2.1. Para los efectos de los presentes Estándares se entenderá por:***
> *(…)*
> ***d. Datos personales sensibles:*** *aquellos que se refieran a la esfera íntima de su titular, o cuya utilización indebida puedan dar origen a discriminación o conlleve un riesgo grave para éste. De manera enunciativa, se consideran sensibles los datos personales que puedan revelar aspectos como origen racial o étnico; creencias o convicciones religiosas, filosóficas y morales; afiliación sindical; opiniones políticas; datos relativos a la salud, a la vida, preferencia u orientación sexual, datos genéticos o datos biométricos dirigidos a identificar de manera unívoca a una persona física."*

47. Por su parte, el Reglamento 2016/679 del Parlamento Europeo y del Consejo, 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 (en adelante, RGPD), contiene una definición específica de los datos biométricos, transcrita a continuación:

> ***"Artículo 4***
> ***Definiciones***
> *(…)*
> *14. "datos biométricos": 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"*

48. Es menester entender el sentido de los datos biométricos, como datos sensibles, debido a dos razones: Su empleo para identificar de manera unívoca a una persona y su tratamiento por medio de un procedimiento técnico específico para tal autenticación de identidad, de acuerdo con el considerando 51 del RGPD:

> *"(51) (…) 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."*

49. En el presente caso, se aprecia que la administrada almacena, en el Sistema Integrado de Migraciones – SIM, entre otros datos personales cuya confidencialidad debe preservarse, la huella dactilar de los ciudadanos

almacenada electrónicamente, utilizada con la finalidad de identificarlos. Dicha circunstancia implica claramente que la administrada efectúa el tratamiento de un dato biométrico.

50. Por tal motivo, debido a su carácter de dato sensible, el tratamiento de esta clase de dato personal requiere una protección reforzada, que refuerce la garantía para los derechos de sus titulares y haga mayor énfasis en la prevención de posibles hechos perjudiciales; garantía que se extenderá al resto de datos personales que son objeto de tratamiento por parte de la administrada, ya que se realiza a través del mismo medio automatizado (el Sistema Integrado de Migraciones – SIM) y de manera conjunta, en el mismo procedimiento de identificación del ciudadano, siendo visibles todos estos datos personales desde un mismo soporte, como se constató en la primera visita de fiscalización.

51. La necesidad de reforzar la confidencialidad de los datos personales mencionados, sin obviar el carácter sensible de los datos biométricos, se consigue a través de la prevención y del ejercicio de la responsabilidad proactiva de parte de quienes realicen el tratamiento de datos personales, cualidad desarrollada en los principios de protección de datos desde el diseño y por defecto del RGPD, como se transcribe a continuación:

> ***"Artículo 25***
> ***Protección de datos desde el diseño y por defecto***
> *1. Teniendo en cuenta el estado de la técnica, el coste de la aplicación y la naturaleza, ámbito, contexto y fines del tratamiento, así como los riesgos de diversa probabilidad y gravedad que entraña el tratamiento para los derechos y libertades de las personas físicas, el responsable del tratamiento aplicará, tanto en el momento de determinar los medios de tratamiento como en el momento del propio tratamiento, medidas técnicas y organizativas apropiadas, como la seudonimización, concebidas para aplicar de forma efectiva los principios de protección de datos, como la minimización de datos, e integrar las garantías necesarias en el tratamiento, a fin de cumplir los requisitos del presente Reglamento y proteger los derechos de los interesados.*
> *2. El responsable del tratamiento aplicará las medidas técnicas y organizativas apropiadas con miras a garantizar que, por defecto, solo sean objeto de tratamiento los datos personales que sean necesarios para cada uno de los fines específicos del tratamiento. Esta obligación se aplicará a la cantidad de datos personales recogidos, a la extensión de su tratamiento, a su plazo de conservación y a su accesibilidad. Tales medidas garantizarán en particular que, por defecto, los datos personales no sean accesibles, sin la intervención de la persona, a un número indeterminado de personas físicas.*
> *3. Podrá utilizarse un mecanismo de certificación aprobado con arreglo al artículo 42 como elemento que acredite el cumplimiento de las obligaciones establecidas en los apartados 1 y 2 del presente artículo."*
> (el subrayado es nuestro)

52. Trasladando ello al ámbito iberoamericano, que comprende al Perú, los Estándares de Protección de Datos Personales para los Estados Iberoamericanos (en adelante, los EPD-RIPD), aprobados por la Red Iberoamericana de Protección

de Datos en el 2017 como directrices para la modernización de las normativas vigentes en protección de datos personales, establece en sus artículos 20 y 38 lo siguiente:

> ***"20. Principio de responsabilidad***
> *20.1. El responsable implementará los mecanismos necesarios para acreditar el cumplimiento de los principios y obligaciones establecidas en los presentes Estándares, así como rendirá cuentas sobre el tratamiento de datos personales en su posesión al titular y a la autoridad de control, para lo cual podrá valerse de estándares, mejores prácticas nacionales o internacionales, esquemas de autorregulación, sistemas de certificación o cualquier otro mecanismo que determine adecuado para tales fines.*
> *(…)*
> ***38. Privacidad por diseño y privacidad por defecto***
> *38.1. El responsable aplicará, desde el diseño, en la determinación de los medios del tratamiento de los datos personales, durante el mismo y antes de recabar los datos personales, medidas preventivas de diversa naturaleza que permitan aplicar de forma efectiva los principios, derechos y demás obligaciones previstas en la legislación nacional del Estado Iberoamericano que le resulte aplicable.*
> *38.2. El responsable garantizará que sus programas, servicios, sistemas o plataformas informáticas, aplicaciones electrónicas o cualquier otra tecnología que impliquen un tratamiento de datos personales, cumplan por defecto o se ajusten a los principios, derechos y demás obligaciones previstas en la legislación nacional del Estado Iberoamericano que le resulte aplicable. Específicamente, con el fin de que únicamente sean objeto de tratamiento el mínimo de datos personales y se limite la accesibilidad de éstos, sin la intervención del titular, a un número indeterminado de personas."* (sic)
> (el subrayado es nuestro)

53. Ambas disposiciones responden de forma común a la necesidad de establecer obligaciones de prevención, a concretarse con actuaciones proactivas de parte de quien realiza el tratamiento de datos personales, encaminadas al cumplimiento de las obligaciones normativamente previstas y a la observancia de los titulares de los datos personales, debiendo garantizar que el empleo de las herramientas de tratamiento, se ajusten a tales disposiciones y cumplan los objetivos de protección de derechos.

54. En especial, la privacidad o protección de datos personales por defecto establece entre las cualidades esperadas de un tratamiento lícito, la limitación de la accesibilidad a los datos personales, evitando el acceso de una cantidad indeterminada de personas o el acceso por parte de quienes no requieren conocer los datos personales para cumplir con sus funciones; además de aplicar tal limitación según el criterio de minimización del tratamiento a lo necesario para alcanzar sus finalidades, acordes a las funciones de cada entidad.

55. La atención a prestar a estos principios y a su exigencia al tratamiento de los datos personales en el Perú, tiene apoyo también en el propio texto de la LPDP, que establece la apertura de la lista de principios que rigen el tratamiento de los datos personales, en su artículo 12:

> ***"Artículo 12. Valor de los principios***
> *La actuación de los titulares y encargados de tratamiento de datos personales y, en general, de todos los que intervengan con relación a datos personales, debe ajustarse a los principios rectores a que se refiere este Título. Esta relación de principios rectores es enunciativa.*
> *(…)"*

VI. Tercera cuestión previa: Acerca de las funciones que legitiman el tratamiento de datos personales de los ciudadanos por parte de la administrada y sus límites

56. Para determinar la necesidad del tratamiento de datos personales por parte de la administrada en el presente caso, es necesario revisar del artículo 45 del Decreto Legislativo N° 1350, Decreto Legislativo de Migraciones (en adelante, DLM):

> ***"Artículo 45.- Generalidades del control migratorio***
> *45.1. Toda persona nacional o extranjera, sea esta pasajero o tripulante, debe ingresar y salir del país a través de los puestos de control migratorio y/o fronterizo habilitados, con su documento de identidad o viaje correspondiente.*
> *45.2. MIGRACIONES habilita puestos de control migratorio y/o fronterizo de tal manera que garantice el registro de toda persona, nacional o extranjera, que ingresa o salga del país."*

57. Por su parte, los artículos 111 y 115 del Reglamento del DLM, aprobado por el Decreto Supremo N° 007-2017-IN, establece las acciones a efectuar en el control migratorio en circunstancias ordinarias y, en el caso del segundo artículo de ellos, las acciones correspondientes a un control secundario, en casos específicos[30].

---

[30] **Reglamento del Decreto Legislativo N° 1350, Decreto Legislativo de Migraciones, aprobado por el Decreto Supremo N° 007-2017-IN**
Artículo 111.- Actividades de MIGRACIONES para el control migratorio
En el ejercicio del control migratorio, MIGRACIONES podrá efectuar las siguientes acciones:
a) Admitir o impedir el ingreso o salida del territorio nacional, según las disposiciones contenidas en la normativa vigente, debiendo respetarse el Principio de No Devolución y no rechazo en frontera para el caso de solicitudes de refugio y asilo.
b) Entrevistar a las personas que pretenden ingresar o salir del territorio nacional a través de un puesto de control y verificar su documentación.
c) Poner en conocimiento de las autoridades competentes aquellos casos de impedimento de ingreso al territorio nacional, cuando corresponda por mandato legal, judicial, tratados o convenios internacionales de los cuales el Perú es parte u otros análogos.
d) Expedir y entregar el Acta de Inadmisión a la persona impedida de ingresar al territorio nacional, poniéndola a disposición de los operadores o medios de transporte internacional o de las autoridades policiales.
e) Aplicar el Principio de protección del interés superior del niño, niña y adolescente para el control migratorio de menores de edad, tomando en cuenta lo establecido en el artículo 52 del Decreto Legislativo y este Reglamento.
f) Inscribir en el RIM los ingresos y salidas, alertas de impedimento de ingreso e impedimentos de salida, sanciones administrativas impuestas y otros datos relacionados al movimiento migratorio.
g) Exigir la presentación de la visa expedida por Relaciones Exteriores o verificar la exoneración de este requisito.
h) Verificar la autenticidad de las visas expedidas por Relaciones Exteriores. En consideración a lo establecido en el Artículo 48 del Decreto Legislativo, MIGRACIONES podrá impedir el ingreso al territorio nacional de la persona extranjera, aun cuando la persona extranjera cuente con visa válida o esté exonerada de ella.
i) Las demás que correspondan de acuerdo al Decreto Legislativo, al Decreto Legislativo que crea la Superintendencia Nacional de Migraciones - MIGRACIONES, Decreto Legislativo Nº 1130, y/o a la normatividad vigente.
Artículo 115.- Control secundario
115.1. MIGRACIONES, con el apoyo de la autoridad policial si es necesario, realiza un segundo control migratorio a las personas que pretenden entrar o salir del territorio nacional, cuando la autoridad migratoria tenga elementos de sospecha sobre a un presunto delito de trata de personas o tráfico ilícito de migrantes u otros delitos.
115.2. También se procede a un control secundario, en caso que la autoridad migratoria encuentre inconsistencias en la información proporcionada por las personas o sospeche de la autenticidad o veracidad de los documentos de viaje o de

58. Ese mismo reglamento[31] establece una circunstancia especial que permite a la administrada, como institución, compartir la información de un ciudadano con entidades específicas: Las personas de interés especial, por cuestiones de resguardo de la seguridad nacional, orden interno, orden público y salud pública, en atención a información proporcionada por las autoridades policiales, sanitarias, de inteligencia, o de autoridad u organización competente; debiendo compartirse la información de estas con las autoridades competentes para continuar con la verificación.

59. De acuerdo con lo señalado en la comunicación del 9 de febrero de 2022 (Informe N° 00013-2022-JZ17CALLAO/MIGRACIONES), la administrada no incluye en sus procedimientos de control migratorio la toma capturas fotográficas de datos de las personas que transitan por el aeropuerto, ni que se compartan por WhatsApp o algún otro medio, sino lo expuesto en su Directiva M01.DRCM.DI.003 - Lineamientos para el Control Migratorio a nivel nacional[32], dentro de las disposiciones generales del mismo:

> **"4.2 Del control migratorio**
> 4.2.1 El Servidor responsable del Control Migratorio, efectúa el control migratorio de ingreso y salida de las personas nacionales y extranjeras en el Puesto de Control Migratorio o fronterizo, de acuerdo a los requisitos establecidos en la normativa legal vigente, verificando la documentación presentada y, en el caso de que MIGRACIONES posea información de la persona nacional o extranjera, debe contrastar con lo que figura en los sistemas informáticos aplicables para el Control Migratorio.
> 4.2.2 Si el Servidor responsable del Control Migratorio, requiere información respecto a la residencia de la persona extranjera, permiso especial de viaje u otra información adicional vinculada al Módulo de Inmigración del Sistema Integrado de Migraciones (SIM INM), debe solicitar a su superior inmediato la consulta correspondiente.
> 4.2.3 Si el Servidor responsable del Control Migratorio, requiere información respecto a alertas migratorias u otra información vinculada al Módulo de Alerta de Personas y Documentos del Sistema Integrado de Migraciones (SIM NDV), debe solicitar a su superior inmediato la consulta correspondiente.
> (…)"

60. La circunstancia descrita implica que la normativa regente en la organización de la administrada permite compartir información de ciudadanos con los superiores,

---

identidad presentados; o que la persona extranjera tenga la permanencia vencida o sin registro migratorio de ingreso o de salida, según corresponda; u otras circunstancias graves que lo ameriten.
115.3. El control secundario se realiza en un ambiente distinto al usado para el control migratorio estándar.

[31] **Artículo 158.- Personas de interés especial**
158.1. Son aquellas personas que requieren un control secundario, o que son sujetos de actividades de verificación o fiscalización, en resguardo de la seguridad nacional, orden interno, orden público y salud pública, en atención a información proporcionada por las autoridades policiales, sanitarias, de inteligencia, o de autoridad u organización competente.
158.2. La solicitud de una calidad migratoria, su cambio y el otorgamiento de visas a personas de interés especial determinadas por el Estado peruano, debe ser coordinado entre las autoridades migratorias y la autoridad competente.
Artículo 159.- Análisis y procesamiento de información migratoria
Por cuestiones de seguridad nacional, salud pública, orden público u orden interno, las autoridades migratorias pueden compartir información registrada con las entidades públicas competentes, cuidando de proteger los datos personales, conforme a la normatividad vigente, para su análisis y procesamiento.

[32] Disponible en https://cdn.www.gob.pe/uploads/document/file/1500310/M01.SM.DI.003.pdf

solo en caso de que se requiera una consulta, sin que dentro de estos procedimientos, como se señaló en el Informe N° 00013-2022-JZ17CALLAO/MIGRACIONES, se requiera de la toma de fotografías de la información de los ciudadanos, ni su difusión entre otros servidores que no tenga como finalidad la consulta, que debe ser realizada con el superior.

61. De lo expuesto, subyace que los servidores de la administrada, encargados del registro y verificación de los ciudadanos que entran y salen del país, son los únicos responsables de la revisión del cumplimiento de los requisitos para permitir el tránsito de personas desde y hacia el Perú y con ello, cada servidor es el único responsable de la información de estas personas a las que accede en su módulo, sin que se tenga permitido compartir estos datos personales con otro personal, salvo en los casos antes reseñados, constituyendo el acceso por parte de los receptores de esta información, un acceso no autorizado.

VII. Cuestiones en discusión

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

62.1 Si la administrada es responsable los siguientes presuntos hechos infractores:

- No haber garantizado la confidencialidad de los datos de las personas que ingresan y salen del país, debido a que estos eran compartidos a través de grupos de WhatsApp desde los teléfonos móviles personales de los trabajadores del área de control migratorio del Aeropuerto Internacional Jorge Chávez, con lo que se habría incumplido el artículo 17 de la LPDP.
- No haber implementado las medidas de seguridad necesarias en el módulo de control migratorio del Sistema Integrado de Migraciones “SIM” del Aeropuerto Internacional Jorge Chávez, al no restringir la generación de copias o reproducción de los datos personales de ciudadanos peruanos (que incluyen datos sensibles) y extranjeros que ingresan y salen del país, según se dispone en el artículo 43 del Reglamento de la LPDP.

62.2 En el supuesto de resultar responsable en cada caso, 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.

62.3 Determinar en cada caso, la multa que corresponde imponer, tomando en consideración los criterios de graduación contemplados en el numeral 3) del artículo 248 de la LPAG.

VIII. Análisis de las cuestiones en discusión

Sobre la presunta omisión de garantizar la confidencialidad de los datos personales de las personas que entran y salen del país a través del puesto de control migratorio del Aeropuerto Internacional Jorge Chávez, por de la administrada

63. 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.

64. El Tribunal Constitucional, máximo intérprete de la Constitución Política del Perú, ha definido el derecho a la autodeterminación informativa en la STC N° 04739-2007-PHD/TC de la siguiente forma:

> *"[e]l 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 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"*

65. Por su parte, la LPDP tiene como objeto, conforme con su artículo 1, *"garantizar el derecho fundamental a la protección de los datos personales, previsto en el artículo 2 numeral 6 de la Constitución Política del Perú, a través de su adecuado tratamiento, en un marco de respeto de los demás derechos fundamentales que en ella se reconocen".*

66. Con la finalidad de hacer efectivo tal derecho de forma permanente durante las operaciones del tratamiento, se tienen en el Título II de dicha ley, los deberes que toda persona, natural o jurídica, a los que debe sujetarse el accionar del responsable del tratamiento de datos personales, a fin de preservar el derecho a la autodeterminación informativa de los titulares de tal información.

67. Entre tales deberes, se recoge la confidencialidad sobre los datos personales, en el artículo 17 de la misma ley, transcrita a continuación:

> ***"Artículo 17. Confidencialidad de datos personales***
> *El titular del banco de datos personales, el encargado y quienes intervengan en cualquier parte de su tratamiento están obligados a guardar confidencialidad respecto de los mismos y de sus antecedentes. Esta obligación subsiste aun después de finalizadas las relaciones con el titular del banco de datos personales.*
> *El obligado puede ser relevado de la obligación de confidencialidad cuando medie consentimiento previo, informado, expreso e inequívoco del titular de los datos personales, resolución judicial consentida o ejecutoriada, o cuando medien razones fundadas relativas a la defensa nacional, seguridad pública o la sanidad pública, sin perjuicio del derecho a guardar el secreto profesional."*

68. A través de dicho artículo, se exige a cualquiera de los intervinientes en los procesos de tratamiento de datos personales (responsables, titulares de los bancos de datos personales, encargados o cualquier otra persona partícipe) a guardar confidencialidad respecto de los datos personales que estén bajo su control o sobre los que tenga conocimiento.

69. Dicha situación implica el deber de evitar el acceso a los datos personales por parte de quienes no estén autorizados para ello, por un lado, así como el de no transmitir o compartir tal información personal con personas no autorizadas, vale decir, un deber de tomar todas las medidas necesarias para prevenir el acceso no autorizado mencionado y un deber negativo referido a compartir o transmitir los datos personales (no hacerlo y evitarlo).

70. La infracción al deber de confidencialidad contemplado en el artículo 17 de la LPDP se configura con i) la ocurrencia de una difusión consciente y activa desde dentro de la organización que trata los datos hacia terceros no autorizados y/o, (ii) una omisión de seguridad relevante al interior de la organización que facilite y permita que datos que deben estar bajo reserva sean conocibles por personas no autorizados. Esto es así, en tanto, en virtud del principio de causalidad que regula la potestad sancionadora de la Autoridad Administrativa, la responsabilidad por las infracciones cometidas no solo se determinan desde una acción activa o concreta del administrado, sino también a partir de una omisión relevante en el cumplimiento de sus obligaciones.

71. Entonces, quien realiza el tratamiento de datos personales debe implementar un entorno para realizarlo con primacía de la privacidad, evitando la intervención de personas cuyas funciones no se vinculen a las finalidades del tratamiento o cuyas funciones específicas no requieran de tal tratamiento, así como las salidas de los datos personales de tal entorno que impliquen riesgos de acceso no autorizado (muchas veces, desconocido por la entidad o persona que realiza el tratamiento), lo cual, a su vez, conlleva a la pérdida del dominio sobre tales datos que ejercía su titular.

72. En el caso de las entidades que realizan el tratamiento de datos personales, el incumplimiento del mencionado deber se configura en los siguientes supuestos:

- El acceso a los datos personales por parte de personas no autorizadas o no legitimadas, sean terceros externos a la organización, o de personas de la misma que no cumplen algún cargo o función que haga necesario tal acceso.
- Cualquier forma de salida de los datos personales, hacia personas que no se encuentra autorizadas o legitimadas para conocerlos o darles tratamiento, aun cuando no se haya configurado un acceso no autorizado al interior de la entidad.
- Una omisión relevante al interior de la organización, que facilite o permita que los datos personales bajo su responsabilidad o custodia, sean accesibles para terceros no autorizados.

73. De lo expuesto, se desprende que el deber de confidencialidad requiere que la organización, empresa o persona que realice el tratamiento, garantice tomar todas las medidas técnicas, organizativas y legales, asegurándose de evitar los accesos no autorizados a los datos personales, a fin de que se restrinja que terceros que no tengan legitimación alguna puedan efectuar su tratamiento.

74. Por supuesto, en consonancia de la prevalencia de la voluntad del titular de los datos personales, la obligación de evitar tales accesos se dispensa cuando este otorga el consentimiento razonado y válido para ello, emitido al evaluar los riesgos para su privacidad que entrañaría una eventual exposición, transferencia o acceso a sus datos personales por parte de un tercero.

75. Respecto al hecho analizado en el presente caso, se verificó que por medio de la aplicación WhatsApp, personal de la administrada compartía información en tiempo real (imágenes de la interfaz del Sistema Integrado de Migraciones – SIM y de pasaportes) de diversos ciudadanos peruanos y extranjeros, incluidas “personalidades”, siguiendo las disposiciones de los servidores que ejercieron la Jefatura Zonal del Callao durante y hasta el 17 de octubre de 2021.

76. Dicha constatación se complementa con la declaración prestada por la Oficial III de Migraciones durante la visita de fiscalización del 18 de octubre de 2021, así como la Jefe Zonal del Callao en funciones, durante la visita de fiscalización del 22 de octubre de 2021, quienes detallaron que para tales transmisiones de información, se formaron cuatro grupos de WhatsApp, liderado cada uno por un Supervisor, así como un grupo con dichos supervisores y ocho coordinadores, a fin de comunicar a través de dicha aplicación, un reporte diario de ocurrencias que permitían entregar reportes puntuales al superior, el Director de Operaciones, quien en su declaración señaló no haber ordenado la toma de las mencionadas fotografías.

77. Por su parte, durante la primera visita de fiscalización, del 18 de octubre de 2021, se pudo constatar que los servidores responsables de siete módulos de control del Aeropuerto Internacional Jorge Chávez, contaban con sus teléfonos celulares personales sin que hubiera instrucciones o algún tipo de restricción sobre uso, de

acuerdo con lo declarado por dos de ellos, lo que demostraría que no se habría realizado ningún control respecto del uso de tales teléfonos móviles personales.

78. Tales factores, conjuntamente analizados, demuestran que, en la organización de la administrada no se establecieron medidas para prevenir o evitar la transmisión y el acceso no autorizado a la información de los ciudadanos, por parte de servidores que carecían de tal autorización, al no haber sido estos quienes cumplían la función de registrar inmediatamente el ingreso o salida de los ciudadanos titulares de la información en el momento de su ingreso o salida del Perú; acceso que tuvieron gracias a la transmisión de las imágenes vía WhatsApp.

79. Lo explicado en el anterior considerando, respecto de la función de los servidores del control migratorio, tiene sustento en el artículo 45 del DLM, así como en las disposiciones reglamentarias e internas examinadas en la tercera cuestión previa, que establecen las acciones que cada uno de los mencionados servidores podía efectuar, así como las situaciones excepcionales en las que podía transmitir información de las personas, sin que hubiera una previsión que permitiera la toma de fotografías de los datos personales y su posterior transmisión, como se especificó en el Informe N° 00013-2022-JZ17CALLAO/MIGRACIONES.

80. Siendo que el fundamento del tratamiento de datos personales por parte de tales servidores, es el registro y control de las personas que ingresan o salen del Perú, esta Dirección puede concluir que no existe una norma que permita la captura y difusión de datos personales a través de conversaciones de WhatsApp entre servidores de la administrada, salvo las situaciones excepcionales ya desarrolladas.

81. De acuerdo con el análisis de los hechos constatados, se dirigió la primera imputación formulada contra la administrada en la Resolución Directoral N° 266-2021-JUS/DGTAIPD-DFI.

82. En sus descargos del 4 de enero de 2022, así como en sus alegatos del 21 de enero de 2022, la administrada señaló que no recibieron ninguna queja, reclamo o comunicación respecto de un uso ilícito de información por parte de los servidores, descartándose también que se haya efectuado alguna operación de “reglaje”.

83. Sobre este argumento, debe indicarse que la comisión de un hecho ilícito no depende de la reacción que haya respecto a este, pues si bien puede causar un daño efectivo o potencial, este no siempre es conocido oportunamente ni en una circunstancia que permita adoptar alguna acción. En este caso, se tiene que los hechos ilícitos se hicieron conocidos, primero, por un reportaje periodístico difundido por televisión abierta, y luego, sus pormenores, gracias a las actuaciones de fiscalización, que comprobaron su existencia.

84. A su vez, se debe tener claro que el reglaje, como un acto de seguimiento de actividades e itinerario de alguna persona, no constituye en sí mismo el hecho infractor, sino uno de los riesgos que derivan de este, al haber un acceso no autorizado por parte de un grupo de servidores de la administrada, a la información de los ciudadanos, a través del empleo de WhatsApp.

85. De otro lado, la administrada alega también que nunca estableció disposición alguna que permitiera tales actuaciones por parte de sus servidores, sino que, contrariamente a ello, instituyó diversos documentos y actividades encaminadas al cumplimiento de la LPDP y su reglamento.

86. Al respecto, debe indicarse que no se está imputando a la administrada el haber inducido la vulneración de la confidencialidad de los ciudadanos y el acceso indebido a sus datos personales, sino la omisión de implementar medidas necesarias para evitar tales hechos infractores, la cual permitió el acceso no autorizado.

87. Respecto de tales documentos, es pertinente referirse, en primer lugar, al Reglamento Interno de Servidor Civiles de la administrada, que en su artículo 40 establece la siguiente prohibición:

> *"Artículo 40.- PROHIBICIONES DE LOS SERVIDORES*
> *Son prohibiciones para los servidores de la Superintendencia Nacional de Migraciones – MIGRACIONES:*
> *(…)*
> *i) Divulgar, revelar, entregar o poner a disposición de terceros, dentro o fuera del centro de trabajo información de la Superintendencia Nacional de Migraciones - MIGRACIONES."*

88. Si bien dicho reglamento es claro en prohibir la disposición de poner a disposición información de la administrada a terceros, es evidente que tiende más a evitar la salida de información hacia personas ajenas a la entidad, sin hacer referencia a la restricción de accesos no autorizados de parte de su mismo personal, accesos que no se encuentren relacionados con el cumplimiento de una función específica, como sucede con el control migratorio en el caso de los oficiales de los módulos de los puestos migratorios.

89. La administrada también hace referencia a la "Política de Privacidad, Protección de Datos Personales y No Divulgación", cuyo texto íntegro, presentado en los descargos, es el siguiente:

> *"La Superintendencia Nacional de Migraciones es respetuosa de las normas legales respecto de la protección de datos personales y los estándares asociados a la privacidad y no divulgación de información, guardando la confidencialidad respecto de los mismos y de sus antecedentes, en ese marco se compromete a:*
> *01. Cumplir con la protección de los datos personales recopilados y/o registrados como parte de los diversos procesos y/o servicios orientados a brindar una mejor calidad de atención a nuestros usuarios, como parte de nuestras funciones, contribuyendo a la seguridad nacional y orden interno.*
> *02. Implementar diversos mecanismos trasparentes orientados al correcto tratamiento de los datos capturados y procesados por nuestra entidad, protegiendo su privacidad y no divulgación.*
> *03. Comprometer a nuestros aliados y proveedores de servicios informáticos el uso correcto y eficaz de los datos tratados.*

04. Diseñar y configurar los servicios digitales a fin de que, sean de fácil acceso para los ciudadanos y los colaboradores de la entidad.
05. En caso Usted, como usuario requiera de información sobre la protección y privacidad de aquellos datos considerados personales, puede comunicarse con los siguientes canales de atención:
- Correo Electrónico: derechosarco@migraciones.gob.pe
- Teléfono: 200 1000"

90. Se aprecia que dicha política establece un compromiso genérico orientado a un tratamiento de datos personales lícito y seguro, así como a atender los derechos de los ciudadanos, lo cual es más evidente, considerando que está dirigida a estos últimos, a quienes se le facilita medios para ejercer sus derechos.

91. Ahora bien, respecto de los Memorándums Múltiples N° 000172-2021-OAJ/MIGRACIONES y N° 000180-2021-OAJ/MIGRACIONES, debe señalarse que tienen fechas 18 y 22 de octubre de 2021, vale decir, posteriores a la fecha de conocimiento de los actos ilícitos.

92. En el caso del primer memorándum múltiple, desde la Oficina de Asesoría Jurídica de la administrada se exhorta a sus distintos órganos a tener en cuenta la calidad de activos estratégicos de los datos personales y a la responsabilidad a tener sobre ellos, de acuerdo con la LPDP, así como con la normativa de gobierno digital, Decreto Legislativo N° 1412 y su reglamento; el segundo de los mencionados cumplía con remitir adjunto, a cada jefe y director de la administrada, las normas aplicables a la protección de datos personales.

93. Sobre estos documentos, se aprecia por sus fechas, su carácter predominantemente reactivo, que podría servir para evitar futuras repeticiones del hecho infractor.

94. No obstante, debe señalarse que no se presentó medio probatorio alguno de la difusión o socialización de tales documentos, requerida por medio del Oficio N° 42-2022-JUS/DGTAIPD-DPDP, por lo que no se puede tener totalmente sustentado su conocimiento por parte de los servidores como los responsables del registro y control de ciudadanos.

95. En lo concerniente al curso virtual sobre los alcances de la LPDP, conviene señalar que es una actividad necesaria para la sensibilización de su importancia entre los servidores, que debe ser complementada con la implementación de las disposiciones de la LPDP y su reglamento.

96. En este punto, es necesario tomar en cuenta las declaraciones prestadas por los servidores encargados de los módulos del puesto de control migratorio del Aeropuerto Internacional Jorge Chávez durante la visita de fiscalización del 18 de octubre de 2021, siete en total, quienes portaban un teléfono móvil personal, dos de los cuales dieron detalles respecto de las instrucciones que se les dio para su uso en ámbito laboral, señalando que los empleaban para comunicarse con sus supervisores y de transmisión de información sobre temas de trabajo, así como la restricción de mantener el teléfono móvil a la vista de los ciudadanos.

97. Asimismo, respecto del uso de los teléfonos móviles, es pertinente revisar también las actas de entrega de los teléfonos móviles asignados por la administrada[33], del año 2021, los cuales no contienen indicaciones respecto del uso adecuado de tales dispositivos, a fin de evitar vulnerar la confidencialidad de los datos personales.

98. Por su parte, de la revisión de los documentos que conforman los legajos de cada servidor, se aprecia que conjuntamente con sus contratos de servicio, se adjunta una "Declaración jurada de prohibiciones e incompatibilidades en el uso de información privilegiada" con el compromiso de no divulgación ni uso de información que pudiera resultar relevante en perjuicio del estado.

99. Otro argumento de descargo es el referido a la necesidad de mantener reportes rápidos acerca de la existencia o no de situaciones problemáticas de relevancia y en caso de suscitarse, permitir una intervención inmediata, mencionando como ejemplos el caso de una persona implicada en un presunto delito contra la libertad sexual, contra la integridad física de su cónyuge, así como el tránsito de personas presuntamente involucradas en la organización "Los Dinámicos del Centro", en casos mediáticos y políticos haciendo uso de prerrogativas con las que no contaban, que permitieron el impedimento de salida del país de tales personas.

100. Al respecto, es necesario volver a lo desarrollado en la tercera cuestión previa, en la que se explicó, sobre la base de las normas legales, reglamentarias e internas que rigen el funcionamiento de la administrada, que la comunicación de información sobre ciudadanos es una situación excepcional, que obedece a determinaciones previas de su condición riesgosa contra el orden público, la salud pública, seguridad nacional y orden interno, se realiza solo hacia el superior, no hacia otros servidores, responsable del registro y control en módulos, a fin de realizar la consulta necesaria, de acuerdo con la Directiva M01.DRCM.DI.003 - Lineamientos para el Control Migratorio a nivel nacional.

101. También es pertinente tomar en cuenta que la mencionada consulta con el superior no conlleva la necesaria toma fotográfica de los datos personales del ciudadano en tránsito ni la transmisión vía WhatsApp de tal imagen, tal como se señaló en el Informe N° 00013-2022-JZ17CALLAO/MIGRACIONES.

102. Por su parte, el argumento respecto a que el procedimiento de la toma de una fotografía de los datos personales de personas, aunque no cuenten con alguna restricción de tránsito o alerta, así como su difusión por WhatsApp a personal no autorizado para conocer los datos, conlleva a un efecto favorable, se basa en casos de personas mediáticas que constituyen consecuencias aisladas y aleatorias de esa práctica, situaciones excepcionales que en los casos de acceso verificados durante la fiscalización así como en el reportaje periodístico antes referido, no se detectó.

103. Entonces, de acuerdo con lo señalado en este subtítulo, se tiene que la administrada es responsable por la comisión de la infracción grave tipificada en el literal g) del numeral 2 del artículo 132 del Reglamento de la LPDP.

[33] Folios 256 al 270

104. Debe indicarse que para la determinación de la sanción, se evaluarán criterios como las medidas preexistentes y adoptadas después de conocerse los hechos, pese a ser insuficientes para perfeccionar la enmienda (correspondiendo para ello, la imposición de medidas correctivas), a fin de evaluar la atenuación de la responsabilidad prevista en el artículo 126 del mencionado reglamento, conjuntamente con los criterios establecidos por el principio de Razonabilidad de la potestad sancionadora administrativa, del numeral 3 el artículo 248 de la LPAG.

Sobre el presunto tratamiento de los datos personales de los ciudadanos empleando el Sistema Integrado de Migraciones - SIM, sin aplicar las medidas de seguridad correspondientes

105. El Título I de la LPDP establece los principios rectores para la protección de datos personales, entre ellos el principio de Seguridad, regulado en el artículo 9 de dicha ley:

> ***"Artículo 9. Principio de seguridad***
> *El titular del banco de datos personales y el encargado de su tratamiento deben adoptar las medidas técnicas, organizativas y legales necesarias para garantizar la seguridad de los datos personales. Las medidas de seguridad deben ser apropiadas y acordes con el tratamiento que se vaya a efectuar y con la categoría de datos personales de que se trate."*

106. Por su parte, el artículo 16 de la misma ley tiene los siguientes términos:

> ***"Artículo 16. Seguridad del tratamiento de datos personales***
> *Para fines del tratamiento de datos personales, el titular del banco de datos personales debe adoptar medidas técnicas, organizativas y legales que garanticen su seguridad y eviten su alteración, pérdida, tratamiento o acceso no autorizado.*
> *Los requisitos y condiciones que deben reunir los bancos de datos personales en materia de seguridad son establecidos por la Autoridad Nacional de Protección de Datos Personales, salvo la existencia de disposiciones especiales contenidas en otras leyes.*
> *Queda prohibido el tratamiento de datos personales en bancos de datos que no reúnan los requisitos y las condiciones de seguridad a que se refiere este artículo."*

107. Este artículo, que desarrolla las principales acciones a realizar a fin de cumplir con el principio de Seguridad, establece dos tipos de objetivos de la adopción de medidas técnicas, organizativas y legales de seguridad: El objetivo general, que es la garantía de la seguridad de los datos personales, y el objetivo específico, que es la adopción de medidas a través de las cuales se concreta tal garantía, dirigidas a evitar la alteración, pérdida, tratamiento o acceso no autorizado a la información custodiada.

108. En el presente subtítulo se analizará el cumplimiento de las disposiciones respectivas sobre medidas de seguridad en el tratamiento automatizado de datos personales, realizado a través del Sistema Integrado de Migraciones – SIM.

109. Ente las disposiciones específicas referidas a medidas técnicas de seguridad, el artículo 43 del Reglamento de la LPDP dispone lo siguiente:

> ***"Artículo 43.- Copia o reproducción.***
> *La generación de copias o la reproducción de los documentos únicamente podrán ser realizadas bajo el control del personal autorizado.*
>
> *Deberá procederse a la destrucción de las copias o reproducciones desechadas de forma que se evite el acceso a la información contenida en las mismas o su recuperación posterior."*

110. El citado artículo establece la obligatoriedad de controlar la generación de copias o reproducciones de documentos que contengan datos personales, a través de implementación de restricciones de uso como de políticas de asignación y empleo, sin dejar de considerar la destrucción de copias rechazadas, a fin de evitar accesos no autorizados a dicha información.

111. Durante la visita de fiscalización realizada el 18 de octubre de 2021, como se consignó en el considerando 3 de esta resolución directoral, las computadoras de los módulos del puesto migratorio del Aeropuerto Internacional Jorge Chávez no contaban con restricciones sobre los puertos USB, grabador de DVD, el envío de correos electrónicos no institucionales, ni para el equipo multifuncional, constatándose además la efectiva grabación de archivos[34].

112. Tal circunstancia se analizó también respecto del uso de los teléfonos móviles de los servidores de los módulos del puesto migratorio, sobre el cual, de acuerdo con lo verificado, no cuentan con ningún control o restricción.

113. En todos los casos, se aprecia que hay de por medio tratamiento de datos sensibles, como son los datos biométricos (huella dactilar), que son obtenidos en cada computadora desde el Sistema Integrado de Migraciones - SIM operada en cada módulo del puesto fiscalizado, posibilitando su copia, reproducción o salida en el mismo formato que tiene en dicho sistema.

114. Al analizar dichas situaciones en el Informe Técnico N° 273-2021-DFI-VARS y en el Informe de Fiscalización N° 302-2021-JUS/DGTAIPD-DFI-JYHV, se tomó el sustento necesario para la segunda imputación contra la administrada, en la Resolución Directoral N° 266-2021-JUS/DGTAIPD-DFI.

115. En sus descargos, la administrada remitió el Informe N° 000186-2021-OTIC/MIGRACIONES, en el que se señala lo siguiente:

- Mediante el Informe N° 000117-2021-JCH-UPST/MIGRACIONES ha precisado que la habilitación de los puertos USB y grabador de DVD es solicitada por cada área usuaria mediante y que, en el caso del puesto migratorio del Aeropuerto Internacional Jorge Chávez, no ha hecho tal solicitud.

[34] Folios 6 al 21

- Señalan también que de acuerdo a su Norma Administrativa Interna S02.OTIC.NAI.004 “Uso Aceptable de los Activos de Información”, corresponde a cada área supervisar el uso de los bienes utilizados para procesar documentos y reproducciones.
- En el mismo sentido, en el Informe N° 000120-2021-JCH-UPST/MIGRACIONES se precisa que la habilitación o restricción para comunicación con correos no institucionales es una prerrogativa del área usuaria, que había sido utilizada para restringir la recepción de correos externos solo de tres usuarios.
- De acuerdo con la Norma Administrativa Interna S02.OTIC.NAI.004 “Uso Aceptable de los Activos de Información”, el uso del correo electrónico no debe efectuarse para participación en foros, suscripción de aplicaciones o uso en temas ajenos al laboral.
- No se solicitó asignar una contraseña al equipo multifuncional, pero a falta de ello, se ha cumplido con brindar cuatro charlas de sensibilización respecto del empleo de los sistemas de control.
- Asimismo, con la Norma Administrativa Interna S02.OTIC.NAI.004 “Uso Aceptable de los Activos de Información” se establecen las siguientes conductas para el uso de teléfonos móviles: Protección física del equipo, conexión a redes seguras, actualización permanente del antivirus, reporte de los desplazamientos de dicho equipo.

116. Lo expuesto por la administrada en sus descargos (reiterado en su escrito del 22 de enero de 2022), fue evaluado en el Informe N° 006-2022-JUS-DFI-ORQR, en el cual se concluyó que no se adjuntaron medios probatorios que sustenten la implementación efectiva de restricciones sobre el uso de los puertos USB, lector de DVD, correos electrónicos institucionales y los teléfonos móviles de los servidores a cargo del puesto migratorio fiscalizado.

117. No obstante, cabe señalar que mediante el Informe N° 000117-2021-JCH-UPST/MIGRACIONES, la administrada ha esclarecido que cuenta con un procedimiento para implementar las restricciones necesarias, consistentes en la solicitud a la Oficina de Tecnologías de Información y Comunicaciones para la asignación o retiro de privilegios otorgados a determinados usuarios respecto de las mencionadas herramientas.

118. La preexistencia de tales procedimientos satisface la necesidad previa de condicionar el uso de dispositivos de copia y transmisión de archivos automatizados, al cumplimiento de un procedimiento previo que, sin embargo, no había sido aplicado al momento de la visita de fiscalización.

119. En tal sentido, debe entenderse que para perfeccionar la enmienda de esta infracción, la administrada debió sustentar la efectiva implementación de restricciones o bloqueos a la posibilidad de grabación de archivos a través de los puertos USB, lectores de DVD, así como la remisión de archivos a correos electrónicos externos a la entidad y lo referente al uso de los teléfonos móviles.

120. Entonces, dicha implementación será requerida como una medida correctiva encaminada para perfeccionar las enmiendas respecto de las medidas de seguridad.

121. Por lo expuesto, se tiene que la administrada es responsable por la comisión de la infracción grave tipificada en el literal c) del numeral 2 del artículo 132 del Reglamento de la LPDP; debiendo tomar en cuenta, para determinar la atenuación de la misma, las acciones y disposiciones establecidas por la administrada, pese a no perfeccionarse, conjuntamente con los criterios establecidos por el principio de Razonabilidad de la potestad sancionadora administrativa, del numeral 3 del artículo 248 de la LPAG.

VIII. Sobre la determinación de las sanciones a aplicar

122. 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.

123. 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 tributarias[35], sin perjuicio de las medidas correctivas que puedan determinarse de acuerdo con el artículo 118 del Reglamento de la LPDP[36].

124. En el presente caso, se ha establecido la responsabilidad de la administrada por los siguientes hechos infractores:

- No haber garantizado la confidencialidad de los datos de las personas que ingresan y salen del país, que fueron compartidos a través de grupos de WhatsApp desde los teléfonos móviles personales de los trabajadores del área de control migratorio del Aeropuerto Internacional Jorge Chávez, con lo que se ha incumplido el artículo 17 de la LPDP, configurando la infracción grave

[35] Ley N° 29733, Ley de Protección de Datos Personales
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 tr butarias (UIT).
(…)

[36] **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 Nº 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 pos ble, medidas correctivas destinadas a eliminar, evitar o detener los efectos de las infracciones.

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

- No haber implementado las medidas de seguridad necesarias en los módulos de control migratorio del Sistema Integrado de Migraciones "SIM" del Aeropuerto Internacional Jorge Chávez, al no restringir la generación de copias o reproducción de los datos personales de ciudadanos peruanos y extranjeros (que incluyen datos sensibles) que ingresan y salen del país, según se dispone en el artículo 43 del Reglamento de la LPDP, configurando la infracción grave tipificada en el literal c) del numeral 2 del artículo 132 de dicho reglamento.

125. Con el objeto de establecer las pautas y criterios para realizar el cálculo del monto de las multas aplicables 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, mediante Resolución Ministerial N° 0326-2020-JUS, se aprobó la Metodología para el Cálculo de Multas en materia de Protección de Datos Personales[37].

126. En tal contexto, se procederá a calcular la multa correspondiente a cada una de dichas infracciones.

No haber garantizado la confidencialidad de los datos de las personas que ingresan y salen del país

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

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 prestablecida", cuya fórmula general es:

***M = Mb x F**, donde:*

M	Multa preestablecida 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.

[37] Documento disponible en: https://bnl.minjus.gob.pe/bnl/.

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 preestablecidas (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 g) del numeral 2 del artículo 132 del Reglamento de la LPDP, respecto de la presentación de la información sobre el tratamiento de los datos personales, corresponde el grado relativo "3" lo cual significa que la multa tendrá como Mb (Monto base) **22,50 U.I.T.**, conforme al siguiente gráfico:

N°	Infracciones graves	Grado relativo
2.g	Incumplir la obligación de confidencialidad establecida en el artículo 17 de la Ley N° 29733 2.9.3. Datos no sensibles	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	**(d) Perjuicio económico causado**	
$f_{1.1}$	. No existe perjuicio.	0.00
$f_{1.2}$	. Existiría perjuicio económico sobre el denunciante o reclamante.	0.10
f_2	**(e) Reincidencia**	
$f_{2.1}$	. No hay reincidencia.	0.00
$f_{2.2}$	. Primera reincidencia.	0.20
$f_{2.3}$	. Dos o más reincidencias.	0.40

f_n	Factores agravantes o atenuantes	Valor
f_3	**(f) Las circunstancias**	
$f_{3.1}$	. Cuando la conducta infractora genere riesgo o daño a una persona.	0.10
$f_{3.2}$	. Cuando la conducta infractora genere riesgo o daño a más de dos personas o grupo de personas.	0.20
$f_{3.3}$	. Cuando la conducta infractora haya afectado el interes público.	0.30
$f_{3.4}$	. Cuando la infracción es de carácter instantáneo y genera riesgo de afectación de otros derechos.	0.15
$f_{3.5}$	. 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

En el presente caso, no se tiene sustento de que se haya provocado un perjuicio económico con la conducta infractora. Asimismo, se tiene que la administrada no es reincidente por ninguna de las infracciones sancionadas.

En cuanto a las circunstancias de la infracción, el incumplimiento del artículo 17 de la LPDP implica la vulneración del derecho de los titulares de los datos personales a evitar todo acceso no autorizado a tales datos, con lo que se busca proteger tanto su voluntad y autodeterminación informativa reconocida por el Tribunal Constitucional en la sentencia recaída en el expediente N° 04387-2011-PHD/TC, así como evitar el conocimiento de su información por parte de personas no autorizadas (servidores de la administrada que no han atendido el registro de determinados ciudadanos) y los riesgos y consecuencias que pueda acarrear ello, como la fuga de dicha información fuera de la entidad, así como el desarrollo de reglajes sobre tales personas.

Siguiendo el análisis del caso concreto y conforme a lo expuesto en la presente resolución directoral, en relación a los factores relacionados a las circunstancias de la infracción (f3) corresponde aplicar las siguientes calificaciones para efectos del cálculo:

- 0.20 La conducta infractora genera riesgo o daño a más de dos personas o grupo de personas.
- -0.15 Colaboración con la autoridad y acción de enmienda parcial, después de notificado el inicio del procedimiento sancionador.

Cabe señalar que en el reportaje periodístico difundido respecto de los hechos del caso, así como en las actuaciones de fiscalización y de la información declarada por la Jefe Zonal del Callao, se verificó que por medio de la aplicación WhatsApp, empleada por los servidores de la administrada en el puesto de control migratorio del Aeropuerto Internacional Jorge Chávez, se tomaron y difundieron datos personales (entre datos identificativos, imágenes, entradas y salidas del país y otros almacenados en el Sistema de Integrado de Migraciones - SIM) de una cantidad determinada de personas.

De otro lado, es apreciable que la administrada había adoptado ciertas medidas preventivas generales respecto de la difusión de información, a través de su Reglamento Interno de Servidores, así como el desarrollo de actividades de sensibilización, como el curso sobre los alcances de la LPDP y su reglamento, así como los memorándums múltiples recordatorios. Dichas circunstancias, aisladas, no enmiendan el hecho infractor ni demuestran haber implementado un control específico sobre el acceso a los datos personales de ciudadanos, aun cuando implican un avance que requiere de complemento.

De otro lado, entendiendo la intencionalidad en personas jurídicas relacionada a la inobservancia de las normas a las que debe adecuar su comportamiento (negligencia)[38], se desprende de lo actuado que la administrada es una entidad pública que su función principal esta directamente vinculada con el tratamiento de datos referidos al hecho imputado, puesto que de acuerdo al Decreto Legislativo 1350, artículo 5, es la Autoridad Migratoria en materia de migratoria interna.

En ese marco, de acuerdo al articulo 6 de la citada norma debe establecer las normas, procedimientos, técnicas e instrumentos que regulan su función migratoria.[39] Por lo tanto, se observa negligencia ante el conocimiento de las disposiciones, al estar relacionadas directamente con las funciones principales.

En total, los factores de graduación suman un total de 35%, así como se muestra en el siguiente cuadro:

Factores de graduación	**Calificación**
f1. Perjuicio económico causado	0%
f2. Reincidencia	0%
f3. Circunstancias f3.2 La conducta infractora genera riesgo o daño a más de dos personas o grupo de personas f3.8 Colaboración con la autoridad y acción de enmienda parcial, después de notificado el inicio del procedimiento sancionador	 20% -15%
f4. Intencionalidad	30%
f1+f2+f3+f4	**35%**

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

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

[39] **Decreto Legislativo N° 1350:**
"Artículo 6.- Regulación Migratoria
MIGRACIONES y el Ministerio de Relaciones Exteriores, de conformidad con los instrumentos internacionales suscritos por el Perú y normativa nacional, establecen el conjunto de normas, procedimientos, técnicas e instrumentos que regulan su función migratoria, en el marco de sus competencias."

Componentes	Valor
Monto base (Mb)	22,50 UIT
Factor de agravantes y atenuantes (F)	1.35
Valor de la multa	**30,38 UIT**

No haber implementado las medidas de seguridad necesarias al no restringir la generación de copias o reproducción de los datos personales de ciudadanos peruanos y extranjeros (incluyendo datos sensibles)

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

El beneficio ilícito ha resultado indeterminable, pues en el trámite del procedimiento administrativo sancionador no ha sido posible recabar medios probatorios que evidencien que la administrada haya obtenido o que espere obtener beneficios derivados de no cumplir con la disposición señalada; así como tampoco se tiene información sobre el monto que ahorra, ahorraría 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 x F**, donde:*

M	Multa preestablecida 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:

Cuadro 2
Montos base de multas preestablecidas (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 por no haber cumplido con inscribir cuatro bancos de datos personales ante el RNPDP, conforme a la tipificación establecida en el literal a) del numeral 1 del artículo 132 del Reglamento de la LPDP, corresponde el grado relativo "1", lo cual significa que la multa tendrá como Mb (Monto base) **7,50 U.I.T.**, conforme al siguiente gráfico:

N°	Infracciones leves	Grado relativo
2.c	Realizar tratamiento de datos personales sensibles incumpliendo las medidas de seguridad establecidas en la normativa sobre la materia. 2.c.1. Hasta dos medidas de seguridad	**1**

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

f_n	Factores agravantes o atenuantes	Valor
f_3	**(f) Las circunstancias**	
$f_{3.1}$	. Cuando la conducta infractora genere riesgo o daño a una persona.	0.10
$f_{3.2}$	. Cuando la conducta infractora genere riesgo o daño a más de dos personas o grupo de personas.	0.20
$f_{3.3}$	. Cuando la conducta infractora haya afectado el interes público.	0.30
$f_{3.4}$	. Cuando la infracción es de carácter instantáneo y genera riesgo de afectación de otros derechos.	0.15
$f_{3.5}$	. 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

En el presente caso, no se tiene sustento de que se haya provocado un perjuicio económico con la conducta infractora. Asimismo, se tiene que la administrada no es reincidente por la infracción.

En cuanto a las circunstancias de la infracción, debe señalarse que el incumplimiento de las disposiciones sobre medidas de seguridad contenidas en el Reglamento de la LPDP, implica la puesta en riesgo de los datos personales sometidos a tratamiento bajo la responsabilidad de la administrada, exponiéndolos a amenazas diversas contra su integridad, disponibilidad y confidencialidad. En este caso específico, al no tenerse implementados controles sobre los puertos USB, lectores de DVD, correos electrónicos y uso de los teléfonos móviles, se suscita el riesgo de fuga de la información, así como el acceso a esta por parte de terceros no autorizados.

Siguiendo el análisis del caso concreto y de conformidad con lo expuesto en la presente resolución directoral, en relación a los factores relacionados a las circunstancias de la infracción (f3) corresponde aplicar las siguientes calificaciones para efectos del cálculo:

- -0.15 Colaboración con la autoridad y acción de enmienda parcial, después de notificado el inicio del procedimiento sancionador.

Debe señalarse que la administrada cuenta con procedimientos con los cuales, cada unidad usuaria (como las Oficinas Zonales, entre ellas las de puestos fronterizos o de ingreso por vía aérea) puede solicitar la inhabilitación de tales dispositivos, así como la implementación de alertas y restricciones respecto del empleo del correo electrónico. No obstante, nunca se comprobó la solicitud o efectiva implementación de tales medidas, así como ninguna dirigida al control del uso de teléfonos móviles personales; con lo que solo se alcanzan acciones de enmienda parciales, insuficientes para evitar la reiteración del hecho infractor.

De otro lado, entendiendo la intencionalidad en personas jurídicas como la inobservancia de las normas a las que debe adecuar su comportamiento (negligencia), se desprende de lo actuado que al interior de la administrada se cuenta con una oficina especializada y un Oficial de Protección de Datos

Personales, encontrándose en capacidad de entender y aplicar las disposiciones de la LPDP y su reglamento, para garantizar el correcto tratamiento de datos personales; tomando en cuenta además que por las funciones desempeñadas (control de tránsito de personas), el tratamiento de datos personales es una actividad frecuente, cuya práctica requiere una especial diligencia y a la vez, genera un grado de experiencia suficiente para exigir el cumplimiento de la normativa indicada.

Asimismo, se desprende también que la administrada cuenta con los procedimientos y documentos para implementar las medidas de seguridad requeridas, pese a lo cual no se hicieron los requerimientos encaminados a ello, hecho sobre el que se dio cuenta en los Informes N° 000117-2021-JCH-UPST/MIGRACIONES y N° 000120-2021-JCH-UPST/MIGRACIONES, hecho que implica una conducta negligente por parte de la administrada.

En total, los factores de graduación suman un total de 15%, así como se muestra en el siguiente cuadro:

Factores de graduación	Calificación
f1. Perjuicio económico causado	0%
f2. Reincidencia	0%
f3. Circunstancias f3.8 Colaboración con la autoridad y acción de enmienda parcial, después de notificado el inicio del procedimiento sancionador	-15%
f4. Intencionalidad	30%
f1+f2+f3+f4	**15%**

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

Componentes	Valor
Monto base (Mb)	7,50 UIT
Factor de agravantes y atenuantes (F)	1.15
Valor de la multa	**8,63 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 a la Superintendencia Nacional de Migraciones con la multa ascendente a treinta coma treinta y ocho Unidades Impositivas Tributarias (30,38 U.I.T.) por la comisión de la infracción grave tipificada en el literal g) del numeral 2 del artículo 132 del Reglamento de la LPDP: *"Incumplir la obligación de confidencialidad establecida en el artículo 17 de la Ley N° 29733"*, de acuerdo con lo desarrollado en la presente resolución directoral.

Artículo 2.- Sancionar a la Superintendencia Nacional de Migraciones con la multa ascendente a ocho coma sesenta y tres Unidades Impositivas Tributarias (8,63 U.I.T.), por la comisión de la infracción grave tipificada en el literal c) del numeral 2 del artículo 132 del Reglamento de la LPDP: *"Realizar tratamiento de datos personales sensibles incumpliendo las medidas de seguridad establecidas en la normativa sobre la materia".*

Artículo 3.- Imponer a la Superintendencia Nacional de Migraciones las siguientes medidas correctivas:

- Establecer y difundir entre su personal, documentos de gestión mediante los cuales se imponga controles al acceso, captación, uso, difusión y transmisión de la información a la que se accede a través del Sistema Integrado de Migraciones – SIM, así como lo referido a la seguridad y confidencialidad de los datos personales de los ciudadanos que entran y salen del país.

- Implementar las medidas de seguridad consistentes en el bloqueo de la función de grabado de archivos, de los puertos USB y los lectores de DVD de las computadoras donde se opere el Sistema Integrado de Migraciones – SIM, así como restricciones en las cuentas de correo electrónicos de los servidores de envío de documentos a cuentas de correo electrónico no institucionales, e implementar y difundir instrucciones para el uso de teléfonos móviles, a fin de impedir la extracción de documentos e imágenes de datos personales, a través del empleo de su almacenamiento o aplicaciones (cámara o escáner).

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 a la Superintendencia Nacional de Migraciones que el incumplimiento de alguna de las medidas correctivas dispuestas 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 tipificada en el literal d) del numeral 3 del mismo artículo reglamentario.

Artículo 5.- Informar a la Superintendencia Nacional de Migraciones que, contra la presente resolución, de acuerdo con lo indicado en el artículo 218 de la LPAG, proceden los recursos de reconsideración o apelación dentro de los quince (15) días hábiles posteriores a su notificación[40].

[40] **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.

Artículo 6.- Informar a la Superintendencia Nacional de Migraciones que deberá realizar el pago de las multas en el plazo de veinticinco (25) días útiles desde el día siguiente de notificada la presente resolución[41].

Artículo 7.- 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.

Artículo 8.- 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 LPDP[42]. Para el pago de la multa, se deberá tener en cuenta el valor de la U.I.T. del año 2021.

Artículo 9.- Notificar a la Superintendencia Nacional de Migraciones la presente resolución directoral.

Regístrese y comuníquese.

MINISTERIO DE JUSTICIA Y DERECHOS HUMANOS

Firmado por
GONZALEZ LUNA Maria Ale andra FAU 20131371617 hard

CN = GONZALEZ LUNA Maria Ale andra FAU 20131371617 hard
O = MINIS ERIO DE JUS ICIA Y DERECHOS HUMANOS
C = PE
Da e 14/02/2022 16 06

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

MAGL/rvr

[41] El pago de la multa puede ser realizado en el Banco de la Nación con el código 04759 o a la cuenta del Banco de la Nación: CTA.CTE R.D.R. N° 0000-281778 o CCI N° 01800000000028177801.

[42] **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.