Resolución Directoral N° 2077 -2020-JUS/DGTAIPD-DPDP

Expediente N°
154-2019-JUS/DGTAIPD-PAS

Lima, 01 de diciembre de 2020

VISTOS:

El Informe Nº 033-2020-JUS/DGTAIPD-DFI del 13 de marzo de 2020[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), junto con los demás documentos que obran en el respectivo expediente; y,

CONSIDERANDO:

I. Antecedentes

1. Mediante Hoja de Trámite N° 48612-2019MSC[2] presentada el 9 de julio de 2019, la señora [redacted] (en adelante, la "denunciante") interpuso denuncia por actos contrarios a la Ley N° 29733, Ley de Protección de Datos Personales (en adelante, la "LPDP") y su reglamento, aprobado por Decreto Supremo N° 003-2013-JUS (en adelante, el "Reglamento de la LPDP") contra el HOSPITAL DE EMERGENCIAS JOSE CASIMIRO ULLOA (en adelante, la "administrada" y/o el "administrado").

La denunciante manifestó, principalmente, lo siguiente:

- Que, se ha vulnerado el derecho a la protección de datos personales de su padre, el sr. [redacted], al haberse obtenido y divulgado imágenes suyas mientras se encontraba en la sala de Traumashock del Hospital Casimiro Ulloa, mientras que se encontraba con vida y antes de entrar a sala de operaciones.
- Que, el tratamiento de los datos personales del titular (imagen e información sensible que puede inferirse de la imagen y contexto en que fueron tomadas) se realizó sin su consentimiento ni de sus familiares, no encontrándose tampoco bajo ninguna de las excepciones permitidas por la LPDP.

[1] Folios 318 a 328
[2] Folios 1 a 10

- Que, el Hospital Casimiro Ulloa al ser el titular del banco de datos de pacientes en él tratados está sujeto al cumplimiento de la normativa de protección de datos.
- Que, solamente funcionarios del Hospital Casimiro Ulloa se encontraban en dicha sala, siendo entonces que los mismos tienen responsabilidad directa sobre el tratamiento al igual que el Hospital Casimiro Ulloa que debería contar con directivas sobre tratamiento de la imagen de los pacientes, así como de información de datos personales médicos (tales como placas radiográficas, tomografías -imagen y video, información de partes médicos, entre otros), y con ello responsabilidad directa sobre el tratamiento de los datos personales en todo su espectro de pacientes por parte de sus funcionarios.
- Que, durante el lapso de tiempo que su padre ingresó al Hospital y su fallecimiento se circularon en diversos grupos de WhatsApp y redes sociales información médica, imágenes de éste en la sala de Traumashock, así como información de carácter médico, siendo que dicho tratamiento en su calidad de difusión ha sido contraria a ley.
- Que, la toma de imágenes de su padre se realiza dentro del nosocomio y la divulgación de las mismas se realizó antes del anuncio formal de su deceso, siendo que solo los familiares, al no poder expresar el titular su consentimiento para el tratamiento de sus datos personales (sensibles y no sensibles), son quienes hubieran podido brindar dicha autorización, hecho que no ocurrió.

2. Mediante Oficio N° 720-2019-JUS/DGTAIPD-DFI[3] de 2 de setiembre de 2019, la DFI solicitó a la denunciante documentación que sustente la divulgación de la imagen e información de carácter médico antes del fallecimiento de su padre.

3. Mediante escrito ingresado con Hoja de Trámite N°65192-2019MSC[4] el 13 de setiembre de 2019, la denunciante absolvió requerimiento de información realizado mediante Oficio N° 720-2019-JUS/DGTAIPD-DFI.

4. Con fecha 17 de setiembre de 2019, la DFI registró en un CD[5] la evidencia contenida en los enlaces de las páginas web proporcionados por la denunciante.

5. Mediante la Orden de Visita de Fiscalización Nº 109-2019-JUS/DGTAIPD-DFI[6], notificada el 20 de setiembre de 2019, la DFI dispuso la realización de una visita de fiscalización a la administrada, en atención a la denuncia interpuesta en su contra, a fin de determinar si existió la vulneración de la obligación de confidencialidad señalada en el artículo 17° de la LPDP.

6. El 20 de setiembre de 2019 se realizó la primera visita de fiscalización, dejándose constancia de los hechos en el Acta de Fiscalización N°01-2019[7].

7. El 25 de setiembre de 2019, se realizó la segunda visita de fiscalización, dejándose constancia de los hechos en el Acta de Fiscalización N°02-2019[8].

[3] Folio 14
[4] Folios 19 a 23
[5] Folio 25
[6] Folio 26
[7] Folios 27 a 36
[8] Folios 39 a 57

8. Mediante escrito ingresado por Hoja de Trámite N° 69049-2019MSC[9] el 30 de setiembre de 2019, la denunciante remitió documentación complementaria.

9. Mediante Oficio Nº 806-2019-JUS/DGTAIPD-DFI[10], la DFI requirió a la denunciante tomografía tomada el 17 de abril de 2019 a su padre, a fin de poder verificar si existe coincidencia con la difundida en los medios.

10. Mediante escrito ingresado por Hoja de Trámite N° 70041-2019MSC[11] el 2 de octubre de 2019, la administrada remitió información requerida mediante Acta de Fiscalización N° 02-2019.

11. Mediante escrito ingresado con Hoja de Trámite N°74262-2019MSC[12] el 18 de octubre de 2019, la denunciante absolvió requerimiento de información realizado mediante Oficio N° 806-2019-JUS/DGTAIPD-DFI, adjuntando para ello solicitud de tomografía y otra documentación relacionada al administrado, a efectos de que dicha documentación le sea remitida a la DFI.

12. El 22 de octubre de 2019, se realizó la tercera visita de fiscalización, dejándose constancia de los hechos en el Acta de Fiscalización N°03-2019[13]

13. Por medio del Informe de Fiscalización N° 163-2019-JUS/DGTAIPD-DFI-AARM de 11 de noviembre de 2019[14], el analista legal de fiscalización de la DFI, por los argumentos que desarrolla y la documentación que obra en el expediente, concluye que se han determinado con carácter preliminar las circunstancias que justifican la instauración de un procedimiento administrativo sancionador, el mismo que fue notificado al administrado mediante Oficio N°923-2019-JUS/DGTAIPD-DFI[15], notificado el 13 de noviembre de 2019[16].

14. Mediante Informe Técnico N° 271-2019-DFI-ORQR de 12 de diciembre de 2019[17], el analista de fiscalización en seguridad de la información de la DFI, por las razones que detalla, formula las siguientes conclusiones sobre la evaluación de la implementación de las medidas de seguridad:

- El administrado no cuenta con procedimientos documentados respecto a la gestión accesos, gestión de privilegios y verificación periódica de privilegios asignados, incumpliendo con lo establecido en el numeral 1 del artículo 39° del Reglamento de la LPDP.
- El administrado no genera ni mantiene registros de evidencias producto de la interacción lógica, incumpliendo con lo establecido en el numeral 2 del artículo 39° del Reglamento de la LPDP.

[9] Folio 63 a 65
[10] Folio 66
[11] Folio 67 a 178
[12] Folios 179 a 183
[13] Folios 185 a 194
[14] Folios 195 a 199
[15] Folio 202
[16] Folio 203
[17] Folios 205 a 206

15. Mediante Resolución Directoral Nº 251-2019-JUS/DGTAIPD-DFI de 19 de diciembre de 2019[18] (en adelante, la "RD de Inicio"), la DFI dispone el inicio del procedimiento administrativo sancionador al administrado; resolución que fue, finalmente, notificada a la Procuraduría Pública del Ministerio de Salud mediante Oficio N°80-2020-JUS/DGTAIPD-DFI el día 27 de enero de 2020[19].

La DFI resolvió iniciar procedimiento administrativo sancionador al administrado, por la presunta comisión de los siguientes hechos infractores:

i) El administrado no habría cumplido con implementar las medidas de seguridad para el tratamiento de datos personales sensibles que realiza a través de los sistemas denominados "RIS" y "PACS" que utiliza para programar y visualizar tomografías, radiografías y otros diagnósticos por imágenes, al: i) No documentar los procedimientos de gestión de accesos, privilegios y verificación periódica de privilegios. Obligación establecida en el numeral 1 del artículo 39 del Reglamento de la LPDP; y ii) No generar ni mantener registros de interacción lógica con el banco de datos personales de pacientes. Obligación establecida en el numeral 2 del artículo 39 del Reglamento de la LPDP.
ii) El administrado habría realizado tratamiento de datos personales incumpliendo la obligación de confidencialidad, establecida en el artículo 17 de la LPDP, al haberse filtrado datos personales sensibles del padre de la denunciante sin consentimiento.

16. Mediante Proveído de fecha 27 de enero de 2020[20] emitido por la DFI, sobre el escrito ingresado mediante Hoja de Trámite N° 4256-2020MSC el 21 de enero de 2020[21] que contiene la solicitud de nulidad de la RD de Inicio por no haber sido debidamente emplazada al domicilio oficial de la Procuraduría Pública del Ministerio de Salud, señaló principalmente lo siguiente:

16.1. Que, por Oficio 80-2020-JUS/DGTAIPD-DFI, se dispuso la notificación de la RD de Inicio y el expediente N° 154-2019-JUS/DGTAIPD-PAS de 206 folios, en la dirección de la PROCURADURIA PUBLICA DEL MINISTERIO DE SALUD sito en Av. Arequipa n.° 810, Piso 9, Distrito, Provincia y Departamento de Lima, notificación que fue realizada el 27 de enero de 2020, fecha en la que se comenzará a contabilizar el plazo establecido en el artículo 120° del Reglamento de la LPDP para la presentación de los descargos respectivos.
16.2. Que, la facultad de contradicción se encuentra prevista en el artículo 217 del TUO de la LPAG y en ella se señala que solo son impugnables los actos definitivos que ponen fin a la instancia y los actos de trámite que determinen la imposibilidad de continuar el procedimiento o produzcan indefensión.
16.3. Que, el presente recurso ha sido interpuesto contra la resolución que da inicio al procedimiento administrativo sancionador, por lo que no se ha puesto fin a la instancia, asimismo, las actuaciones no han generado

[18] Folios 207 a 214
[19] Folio 238
[20] Folio 239
[21] Folios 224 a 237

efectos sobre los derechos, intereses u obligaciones del administrado, debido a que a la fecha no ha sido sancionado por ninguna infracción, ni se le ha requerido el cumplimiento de alguna multa impuesta, por el contrario, el procedimiento continúa en trámite.

17. Dicho Proveído fue notificado mediante Oficio N°81-2020-JUS/DGTAIPD-DFI[22] el día 29 de enero de 2020[23].

18. Mediante escrito ingresado con Hoja de Trámite N°10870-2019MSC el 17 de febrero de 2020[24], el administrado presentó sus descargos, señalando principalmente lo siguiente:

18.1. Sobre el Hecho Imputado N° 1:

18.1.1. Señaló que en la visita de fiscalización N°02-2019, se manifestó que los programas RIS y PACS no contaban con registros de interacción lógica, y que existe un proyecto de actualización del RIS y PACS en el cual se está considerando la interacción lógica, tal como se establece en la LPDP.

18.1.2. Señaló que dichos sistemas tienen limitaciones del registro de interacción lógica de visualización de imágenes, teniendo los médicos radiólogos, tecnólogos médicos su propio usuario y contraseña, permitiendo su finalidad, la atención de los pacientes.

18.2. Sobre el hecho imputado N°2:

18.2.1. Señaló que SUSALUD ha instaurado un procedimiento administrativo sancionador por el mismo hecho imputado, por lo que corresponde que se tome en consideración el principio de non bis in ídem, recogido en el artículo 230° del TUO de la LPAG.

18.2.2. Existe una indebida motivación de la RD de Inicio, ya que para que exista una debida fundamentación debe existir conexión lógica entre los hechos alegados y las pruebas aportadas u obtenidas, así como coherencia y consistencia en sus razonamientos.

18.2.3. Existe una indebida tipificación del hecho imputado ya que imputa al hospital haber incurrido en la infracción contenida en el artículo 17° de la LPDP; sin embargo, tal tipo infractor debe imputarse siempre que la exhibición o difusión de las imágenes del asegurado o la información relacionada a su enfermedad debió haberlo hecho en representación de la entidad o por su intermedio. En el presente caso, las personas involucradas en dicha infracción han sido identificadas y vienen siendo objeto de procedimientos administrativos disciplinarios, por tanto no han actuado ni en su representación, ni por su intermedio.

18.2.4. Dicha infracción podría haberse atribuido a la entidad si el titular del banco de datos personales hubiera sido el responsable de la difusión; sin embargo, esto no ha sido así, alegar lo contrario implicaría la vulneración al principio de causalidad.

18.2.5. A través de diversos documentos del expediente (el Informe N°194-2019-STPAYD-OP-HECJU, Informe N°383-2019-OP-HEJCU, entre

[22] Folio 240
[23] Folio 241
[24] Folios 243 a 311

otros) las personas involucradas en la infracción han sido objeto de procedimientos disciplinarios y procesos ante OSCE (esto último respecto de quienes mantenían contratos de locación de servicios), no habiendo actuado en representación ni por intermedio del administrado.

18.2.6. Sin perjuicio de lo mencionado, debe tomarse en consideración lo mencionado en el Acta de Fiscalización N° 02-2019, en la que se señala que actualmente existe una directiva interna donde se restringe el uso de los teléfonos celulares implementado antes del inicio del presente procedimiento.

19. Mediante Informe Técnico N° 60-2020-DFI-ORQR de 27 de febrero de 2020[25], el analista de fiscalización en seguridad de la información de la DFI emitió informe complementario de evaluación de la implementación de las medidas de seguridad por parte del administrado, en función a la información remitida por éste en sus descargos presentados el 17 de febrero de 2020, concluyendo lo siguiente:

- El administrado no ha evidenciado contar con procedimientos documentados respecto a la gestión accesos, gestión de privilegios y verificación periódica de privilegios asignados, incumpliendo con lo establecido en el numeral 1 del artículo 39° del Reglamento de la LPDP.
- El administrado no genera ni mantiene registros de evidencias producto de la interacción lógica, incumpliendo con lo establecido en el numeral 2 del artículo 39° del Reglamento de la LPDP.

20. Por medio de la Resolución Directoral N°046-2020-JUS/DGTAIPD-DFI del 13 de marzo de 2020[26], la DFI dio por concluidas las actuaciones instructivas correspondientes al procedimiento sancionador.

21. Mediante Informe Final de Instrucción N°033-2020-JUS/DGTAIPD-DFI del 13 de marzo de 2020[27], la DFI remitió a la Dirección de Protección de Datos Personales de la Dirección General de Transparencia, Acceso a la Información Pública y Protección de Datos Personales (en adelante, la "DPDP") los actuados para que resuelva en primera instancia el procedimiento administrativo sancionador iniciado, recomendando lo siguiente:

- Imponer una sanción administrativa de multa ascendente a cinco unidades tributarias impositivas (5UIT) al administrado por el cargo acotado en el Hecho Imputado N° 01, por 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 norma sobre la materia".*
- Imponer sanción administrativa de multa ascendente a veinte unidades impositivas tributarias (20 UIT) al administrado por el cargo acotado en el Hecho Imputado N°02, por 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".*

[25] Folios 312 a 313
[26] Folios 314 a 315
[27] Folios 318 a 328

22. El Informe Final de Instrucción N° 033-2020-JUS/DGTAIPD-DFI así como la Resolución Directoral N°046-2020-JUS/DGTAIPD-DFI fueron notificados al administrado mediante Oficio N°351-2020-JUS/DGTAIPD-DFI[28] con fecha 30 de junio de 2020 al administrado al correo electrónico tramitedocumentario@hejcu.gob.pe[29]

23. Por medio de la Resolución Directoral N°109-2020-JUS/DGTAIPD-DFI del 17 de setiembre de 2020[30] resuelve corregir los errores materiales incurridos en el Informe de Final de Fiscalización N.° 033-2020-JUS/DGTAIPD-DFI, y la Resolución Directoral N° 046-2020-JUS/DGTAIPD-DFI, ambos emitidos el 13 de marzo de 2020, conforme expuso en los considerandos segundo y tercero siguientes:

"(…)
Segundo: Mediante el Informe de Final de Fiscalización N.° 033-2020-JUS/DGTAIPD-DFI de 13 de marzo de 2020 (f. 318 a 328), se realizó el análisis de los descargos presentados por la administrada y los medios probatorios aportados; en ese sentido, respecto al primer hecho imputado, sobre el incumplimiento de las medidas de seguridad para el tratamiento de datos personales sensibles, se recomendó la imposición de una multa de ocho (08) UIT; no obstante, en el punto número 8 referente a las conclusiones, se ha incurrido en un error material, y se ha consignado como monto de la sanción cinco (05) UIT, debiendo ser lo correcto ocho (08) UIT.

ASÍ, EN EL INFORME DICE:

8) CONCLUSIONES.

1. Se recomienda imponer sanción administrativa de multa ascendente a cinco (05) U.I.T. a HOSPITAL DE EMERGENCIA JOSÉ CASIMIRO ULLOA por el cargo acotado en el imputado Hecho N.°01, por infracción grave tipificada en el literal c), numeral 2, del artículo 132° del Reglamento de la LPDP: *"Realizar tratamiento de datos personales sensibles incumpliendo las medidas de seguridad establecidas en la norma sobre la materia".*

DEBE DECIR:

8) CONCLUSIONES.

1. Se recomienda imponer sanción administrativa de multa ascendente a ocho (08) U.I.T. a HOSPITAL DE EMERGENCIA JOSÉ CASIMIRO ULLOA por el cargo acotado en el imputado Hecho N.° 01, por infracción grave tipificada en el literal c), numeral 2, del artículo 132° del Reglamento de la LPDP: *"Realizar tratamiento de datos personales sensibles incumpliendo las medidas de seguridad establecidas en la norma sobre la materia".*

Tercero: asimismo, en la Resolución Directoral N.°046-2020-JUS/DGTAIPD-DFI de 13 de marzo de 2020, en el punto 10 se ha consignado las conclusiones a las que se arribó en el Informe de Final de Fiscalización N° 033-2020-JUS/DGTAIPD-DFI, habiéndose consignado por error los montos de las multas recomendadas, en cinco (05) UIT y doce (12) UIT, por los incumplimientos relacionados a las medidas de seguridad para el tratamiento de datos sensibles, y el deber de confidencialidad respectivamente; siendo lo correcto ocho (08) y veinte (20) respectivamente.

[28] Folio 316
[29] Folio 317
[30] Folios 332 a 333

ASÍ, EN LA RESOLUCIÓN DICE:

"***8) CONCLUSIONES.***

1) *Se recomienda imponer sanción administrativa de multa ascendente a cinco (05) U.I.T. a HOSPITAL DE EMERGENCIA JOSÉ CASIMIRO ULLOA por el cargo acotado en el imputado Hecho N.° 01, por infracción grave tipificada en el literal c), numeral 2, del artículo 132° del Reglamento de la LPDP: "Realizar tratamiento de datos personales sensibles incumpliendo las medidas de seguridad establecidas en la norma sobre la materia".*

2) *Se recomienda imponer sanción administrativa de multa ascendente a doce (12) U.I.T. a HOSPITAL DE EMERGENCIA JOSÉ CASIMIRO ULLOA por el cargo acotado en el imputado Hecho N.° 02, por infracción grave tipificada en el literal g), 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".*

DEBE DECIR:

"8) CONCLUSIONES.

1) *Se recomienda imponer sanción administrativa de multa ascendente a ocho (08) U.I.T. a HOSPITAL DE EMERGENCIA JOSÉ CASIMIRO ULLOA por el cargo acotado en el imputado Hecho N.° 01, por infracción grave tipificada en el literal c), numeral 2, del artículo 132° del Reglamento de la LPDP: "Realizar tratamiento de datos personales sensibles incumpliendo las medidas de seguridad establecidas en la norma sobre la materia".*

2) *Se recomienda imponer sanción administrativa de multa ascendente a veinte (20) U.I. T. a HOSPITAL DE EMERGENCIA JOSÉ CASIMIRO ULLOA por el cargo acotado en el imputado Hecho N.° 02, por infracción grave tipificada en el literal g), 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".*

(…)"

Asimismo, la Resolución Directoral N°109-2020-JUS/DGTAIPD-DFI dispuso volver a notificar el Informe de Final de Fiscalización N°033- 2020-JUS/DGTAIPD-DFI, y la Resolución Directoral N°046-2020-JUS/DGTAIPD-DFI, así como esta resolución, al domicilio procesal electrónico de la Procuraduría Pública del Ministerio de Salud en los siguientes correos electrónicos: procuraduria@minsa.gob.pe y procuraduriapublicaminsa@gmail.com

24. La Resolución Directoral N°109-2020-JUS/DGTAIPD-DFI, el Informe Final de Instrucción N° 033-2020-JUS/DGTAIPD-DFI y la Resolución Directoral N°046-2020-JUS/DGTAIPD-DFI fueron notificados al administrado mediante Oficio N°870-2020-JUS/DGTAIPD-DFI[31] con fecha 18 de setiembre de 2020[32].

25. La administrada presentó sus descargos al Informe Final de Instrucción con fecha 25 de setiembre de 2020, los mismos que fueron ingresados con códigos 2020MSC-

[31] Folio 331
[32] Folio 334

041006 y 2020MSC-041010, a través de la Mesa de Partes Virtual del Ministerio de Justicia y Derechos Humanos[33].

Los descargos principales de la administrada fueron los siguientes:

25.1. Respecto a la aplicación del principio del Non Bis In Ídem

- Los hechos imputados por SUSALUD como por la DFI refieren sobre los mismos hechos y similitud de imputaciones al tener como materia de imputación la divulgación de imagen e información de carácter médico ante el fallecimiento del padre de la denunciante, conforme se advierte del Oficio N.°720-2019-JUS/DGTAIPD-DFI que obra en el Folio14 del expediente.
- No puede vulnerarse este principio, pues no solo presupone una identidad en la persona y los hechos, sino que la pretensión es la misma, la aplicación de una multa por la imputación descrita en el punto anterior. La Ley de Procedimiento Administrativo General sobre el principio de Non Bis In Ídem, establece: *"No se podrán imponer sucesiva o simultáneamente una pena y una sanción administrativa por el mismo hecho en los casos en que se aprecie la identidad del sujeto, hecho y fundamento. (…)"*

25.2. Respecto a la aplicación del principio de licitud

Sobre el hecho imputado N°1:

- Mediante Oficio 1359-2019 DGHEJCU señaló que viene realizando actos preparatorios para la adquisición del sistema electrónico de archivo y comunicación de imágenes médicas (PACS) con sistema de administración radiológico (RIS) y digitalización con impresión de imágenes.
- Existe un proyecto de actualización del RIS y PACS que está considerando la interacción lógica, conforme a la LPDP, aseveración que recae en el principio de presunción de veracidad; siendo prueba de ello que mediante el Oficio 1359-2019 DGHEJCU de 13/08/2019 se le solicitó a la Oficina General de Tecnología de la Información - OGTI del MINSA el apoyo para la evaluación de especificaciones técnicas sobre la adquisición de los referidos sistemas.
- Señala que los trámites administrativos conducentes para el mejoramiento de los referidos sistemas, además del plan de adquisición del sistema electrónico de archivo y comunicación de imágenes médicas (PACS) con sistema de administración radiológico (RIS) y digitalización con impresión de imágenes no han sido debidamente valorados, los cuales fueron realizados antes de la notificación del inicio del presente procedimiento sancionador (es decir, antes del 27 de enero de 2020), encontrándose dentro del supuesto del literal f) del artículo 257 del TUO de la LPAG.
- Respecto al extremo de incumplimiento del numeral 1 del artículo 39 del Reglamento de la LPDP, reiteró lo descrito en el considerando 18.1.2, agregando que no es cierto que no haya acreditado contar con dichos sistemas.

[33] Folios 336 a 373

25.3. Respecto a la adecuada interpretación del principio de razonabilidad

- El objetivo de la implementación de medidas de seguridad es la creación de un entorno seguro y confiable para el tratamiento de datos personales, donde el responsable tenga la capacidad para mitigar los riesgos mencionados (riesgos de pérdida, alteración, tratamiento o acceso no autorizado a los datos personales) y contrarrestar sus efectos dañinos. Solo la ausencia de tal entorno, que puede ser por causa de una brecha de seguridad implica el incumplimiento del principio de seguridad; al respecto la administrada señaló que demostró en todo momento que evita brechas de seguridad, estableciendo un entorno para que las mismas no sucedan.

25.4. Sobre el hecho imputado N°2 y respecto al principio de causalidad:

- Reiteró los alegatos presentados contra la RD de Inicio (descritos en los considerandos 18.2.2 a 18.2.6 de la presente Resolución).

25.5. Adjuntó los siguientes anexos:
Anexo A: Copia de Oficio N°01703-2019-SUSALUD/IFIS y Res. 01 de Inicio de procedimiento administrativo sancionador
Anexo B: Copia de Oficio N°600-2020-DG-HECU, respecto a procedimientos administrativos disciplinarios
Anexo C: Copia del Informe N°70-2020-STPAYD-OP-HEJCU emitido por la Secretaría Técnica de Procesos Administrativos y Disciplinarios.

II. Competencia

26. 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.

27. 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

28. Acerca de la responsabilidad del administrado, se deberá tener en cuenta que el literal f) del numeral 1 del artículo 257 del Texto Único Ordenado de la Ley del Procedimiento Administrativo General (en adelante, la "LPAG"), establece como una causal eximente de la responsabilidad por infracciones, la subsanación voluntaria del hecho imputado como infractor, si es realizada de forma previa a la notificación de imputación de cargos[34].

[34] **Texto Único Ordenado de la Ley N° 27444, Ley del Procedimiento Administrativo General, aprobado por Decreto Supremo Nº 004-2019-JUS**

29. Asimismo, se debe atender a lo dispuesto en el artículo 126 del Reglamento de la LPDP, que considera como atenuantes la colaboración con las acciones de la autoridad y el reconocimiento espontáneo de las infracciones conjuntamente con la adopción de medidas de enmienda; dichas atenuantes, de acuerdo con la oportunidad del reconocimiento y las fórmulas de enmienda, pueden permitir la reducción motivada de la sanción por debajo del rango previsto en la LPDP[35].

30. Dicho artículo debe leerse conjuntamente con lo previsto en el numeral 2 del artículo 257 de la LPAG[36], que establece como condición atenuante el reconocimiento de la responsabilidad por parte del infractor de forma expresa y por escrito, debiendo reducir la multa a imponérsele hasta no menos de la mitad del monto de su importe; y por otro lado, las que se contemplen como atenuantes en las normas especiales.

IV. Primera Cuestión Previa: Sobre el Non Bis In Ídem aplicable al ejercicio de la potestad sancionadora administrativa respecto al hecho imputado N°2

31. Los argumentos expuestos por el administrado, recogidos en los considerandos 18.2.1 y 25.1 de la presente Resolución Directoral, refieren que se estarían configurando imputaciones que cumplen con la identidad de sujeto, hecho y fundamento, respecto a los procedimientos seguidos por la Autoridad Nacional de Protección de Datos Personales (en adelante, la "ANPDP") y la Superintendencia Nacional de Salud (en adelante, "SUSALUD") por el mismo hecho y bajo la misma identidad de fundamento,

32. Conforme lo ha señalado el Tribunal Constitucional en reiteradas oportunidades solo en aquellos casos donde se haya verificado la concurrencia de la identidad de sujeto, hecho y fundamento jurídico se podrá alegar a favor el principio del *Non bis in ídem* y, consecuentemente, la aplicación de una sola sanción administrativa procedente de un único procedimiento administrativo sancionador. Basta que una de las tres identidades de los elementos antes referidos, los cuales deben concurrir simultáneamente, no se configure para que dicha garantía del Non bis in ídem sea desestimada, siendo procedente la tramitación de dos procedimientos en paralelo para

---

"**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."

[35] **Reglamento de la Ley de Protección de Datos Personales, aprobado por Decreto Supremo Nº 003-2013-JUS**
"**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"

[36] **Texto Único Ordenado de la Ley N° 27444, Ley del Procedimiento Administrativo General, aprobado por Decreto Supremo Nº 004-2019-JUS**
"**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."

la imposición de sanciones independientes, provenientes del análisis que se efectúe en cada procedimiento.

33. Este Despacho concuerda con la DFI respecto a la no configuración de la triple identidad de los elementos que sustentan la aplicación del principio del Non bis in ídem, toda vez que, no se da dicha identidad en el fundamento. Ello, en tanto, los fundamentos jurídicos que respaldan la potestad sancionadora de cada una de las autoridades, SUSALUD y la ANPD, ejercidas indistintamente dentro del marco de sus procedimientos administrativos sancionadores son distintos.

34. En efecto, cada una de estas autoridades protege bienes jurídicos diferentes, siendo que para el caso de la ANPD el bien jurídico a proteger son los datos personales a todo nivel, garantizando con ello un adecuado tratamiento de los mismos por parte de todo titular de banco de datos personales y/o responsable para dicho tratamiento, siendo que esta protección de datos personales, también conocido como "autodeterminación informativa", ha sido amparada constitucionalmente como derecho fundamental de toda persona natural en el artículo 2 numeral 6 de la Constitución Política.

Este derecho a la autodeterminación informativa ha sido desarrollado por el Tribunal Constitucional y referido en reiteradas ocasiones en diversos pronunciamientos, en tal sentido es oportuno señalar la STC 04739-2007-PHD/TC (fundamentos 2-4) que *"[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 (…)"* (Subrayado propio)

35. El objetivo principal de la LPDP es garantizar al titular del dato personal la protección de sus datos personales, orientándolo para el ejercicio de sus derechos de acceso, rectificación, cancelación y oposición al tratamiento de sus datos, estableciendo deberes y obligaciones mínimos a los titulares de banco de datos personales y responsables de su tratamiento, en observancia de los principios rectores reconocidos en dicha ley, para cautelar un uso adecuado de los datos personales a los cuales se accede bajo diversas modalidades de tratamiento. En tal sentido, el artículo 1 de la LPDP establece como objeto de protección a los datos personales, previamente reconocido a nivel constitucional:

"Artículo 1. Objeto de la Ley

La presente Ley tiene el objeto de 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."

36. Asimismo, resulta oportuno hacer mención a la regla general respecto al alcance que tiene la LPDP y su reglamento a todo tratamiento de datos personales, contenido o destinado a ser contenido en bancos de datos personales, sean administrados por entidades públicas o privadas dentro de territorio peruano, no encontrándose ajeno a ello las entidades del sector salud, más aún cuando realizan tratamiento de datos sensibles constituidos estos últimos por aquellos datos relacionados al estado de salud, enfermedades, diagnósticos, resultados de laboratorio, tratamientos y/o procedimientos médicos, entre otros, vinculados a una persona y/o que formen parte de su historia clínica.

En este orden de ideas, es pertinente citar este ámbito de aplicación de la normativa de protección de datos personales, el mismo que le resulta oponible a toda entidad que efectúe tratamiento de datos personales, revistiendo mayor importancia su obligatoriedad para aquellas que traten datos de especial protección como son aquellos relacionados a la salud de las personas:

"Artículo 3 de la LPDP. Ámbito de aplicación
La presente Ley es de aplicación a los datos personales contenidos o destinados a ser contenidos en bancos de datos personales de administración pública y de administración privada, cuyo tratamiento se realiza en el territorio nacional. Son objeto de especial protección los datos sensibles.
(…)" (Subrayado propio)

"Artículo 3 del Reglamento de la LPDP.- Ámbito de aplicación.
El presente reglamento es de aplicación al tratamiento de los datos personales contenidos en un banco de datos personales o destinados a ser contenidos en bancos de datos personales.
Conforme a lo dispuesto por el numeral 6 del artículo 2 de la Constitución Política del Perú y el artículo 3 de la Ley, el presente reglamento se aplicará a toda modalidad de tratamiento de datos personales, ya sea efectuado por personas naturales, entidades públicas o instituciones del sector privado e independientemente del soporte en el que se encuentren.
La existencia de normas o regímenes particulares o especiales, aun cuando incluyan regulaciones sobre datos personales, no excluye a las entidades públicas o instituciones privadas a las que dichos regímenes se aplican del ámbito de aplicación de la Ley y del presente reglamento.
Lo dispuesto en el párrafo precedente no implica la derogatoria o inaplicación de las normas particulares, en tanto su aplicación no genere la afectación del derecho a la protección de datos personales." (Subrayado propio)

37. Respecto a los datos sensibles como objeto especial de protección, la LPDP reconoce como tales en el numeral 5 de su artículo 2 a toda información relacionada a la salud, siendo que en el Reglamento de la LPDP se desarrollan de forma complementaria estas definiciones, conforme al siguiente tenor:

Artículo 2 del Reglamento de la LPDP:

"Artículo 2.- Definiciones.

Para los efectos de la aplicación del presente reglamento, sin perjuicio de las definiciones contenidas en la Ley, complementariamente, se entiende las siguientes definiciones:
(…)
5. Datos personales relacionados con la salud: *Es aquella información concerniente a la salud pasada, presente o pronosticada, física o mental, de una persona, incluyendo el grado de discapacidad y su información genética.*
6. Datos sensibles: *Es aquella información relativa a datos personales referidos a las características físicas, morales o emocionales, hechos o circunstancias de su vida afectiva o familiar, los hábitos personales que corresponden a la esfera más íntima, la información relativa a la salud física o mental u otras análogas que afecten su intimidad.*
(…)" (Subrayado propio)

38. Por su lado, el bien jurídico tutelado por SUSALUD, en observancia del Decreto Legislativo N° 1158, "Decreto Legislativo que dispone medidas destinadas al fortalecimiento y cambio de denominación de la Superintendencia Nacional de Aseguramiento en Salud" (en adelante, el "D.L 1158") es la protección y defensa de los derechos de las personas al acceso a los servicios de salud, tal y como lo señala en su artículo 1, lo cual se condice con la protección del derecho a la salud y de los usuarios que acceden a la prestación de servicios de atención médica:

*"**Artículo 1.- Objeto de la norma***
El presente Decreto Legislativo tiene por objeto disponer las medidas destinadas al fortalecimiento de las funciones que actualmente desarrolla la Superintendencia Nacional de Aseguramiento en Salud, con la finalidad de promover, proteger y defender los derechos de las personas al acceso a los servicios de salud, supervisando que las prestaciones sean otorgadas con calidad, oportunidad, disponibilidad y aceptabilidad, con independencia de quien la financie." (Subrayado propio)

Y, es que ello responde a los parámetros base establecidos en la Ley General de Salud, Ley N°26842, siendo los principales aquellos descritos en los siguientes artículos de su Título Preliminar, los que a su vez sustentan la protección del derecho de toda persona a acceder y recibir servicios de salud que cumplan con los debidos estándares de calidad en los procedimientos y prácticas a nivel profesional e institucional.

"I. La salud es condición indispensable del desarrollo humano y medio fundamental para alcanzar el bienestar individual y colectivo.
II. La protección de la salud es de interés público. Por tanto, es responsabilidad del Estado regularla, vigilarla y promoverla.
III. Toda persona tiene derecho a la protección de su salud en los términos y condiciones que establece la ley. El derecho a la protección de la salud es irrenunciable (…)
VI. Es de interés público la provisión de servicios de salud, cualquiera sea la persona o institución que los provea. Es responsabilidad del Estado promover las condiciones que garanticen una adecuada cobertura de prestaciones de salud a la población, en términos socialmente aceptables de seguridad, oportunidad y calidad.
(…)
IX. La norma de salud es de orden público y regula materia sanitaria, así como la protección del ambiente para la salud y la asistencia médica para la recuperación y rehabilitación de la salud de las personas.
(…)"

39. Es siguiendo dicha línea dirigida a la protección de los usuarios del servicio de salud, dentro de un contexto de acceso universal a una prestación oportuna y de

calidad, es que se recoge a nivel normativo el alcance de los derechos de tales usuarios al acceso a los servicios de salud, a la atención integral de la salud, al acceso a la información relacionada a su salud, incluyendo los derechos que le asisten como paciente, y consentimiento informado respecto a los tratamientos médicos.

40. Respecto al resguardo de los derechos de los usuarios de los servicios de salud, estos se encuentran regulados en la Ley N° 29414, "Ley que establece los Derechos de las Personas Usuarias de los Servicios de Salud" y su Reglamento, aprobado por Decreto Supremo Nº 027-2015-SA; siendo que el artículo 19 de este Reglamento resalta el derecho al respeto de la dignidad e intimidad del paciente y/o usuario del servicio de salud dentro del contexto de una atención médica:

"Artículo 19.- Derecho al respeto de su dignidad e intimidad
Toda persona tiene derecho a ser atendida por personal de salud autorizado por la normatividad vigente, y con pleno respeto a su dignidad e intimidad, sin discriminación por acción u omisión de ningún tipo.
El personal profesional de la salud y administrativo de la IPRESS debe brindar una atención con buen trato y respeto a las personas usuarias de los servicios de salud, garantizando el pleno ejercicio de sus derechos.
Ninguna persona usuaria puede ser discriminada en el acceso a los servicios de salud, la atención o tratamiento por motivo de origen, etnia, sexo, género, idioma, religión, opinión, condición económica, orientación sexual, discapacidad o de cualquier otra índole.
En caso el paciente haya autorizado, previa firma de consentimiento informado, la exploración, tratamiento o exhibición de imágenes con fines docentes, el médico tratante debe garantizar el respeto a la privacidad y pudor del paciente.
En caso de menores de edad o de personas cuyas condiciones particulares le impidan ejercer este derecho, el consentimiento a que se refiere el párrafo precedente, será expresado de acuerdo a lo establecido en el artículo 5 del presente Reglamento." (Subrayado propio)

41. Es en atención a esta necesidad de velar por la protección del usuario de los servicios de salud, para que estos accedan a- y reciban- prestaciones que sean otorgadas con calidad, oportunidad, disponibilidad y aceptabilidad, motivo por el cual se dota de autoridad a SUSALUD como ente supervisor del funcionamiento del sistema prestacional de salud a nivel nacional, debiendo intervenir en defensa de los usuarios cuando sus derechos enmarcados en una relación paciente-médico o paciente-IPRESS (Instituciones Prestadoras de Servicios de Salud) sean vulnerados.

En tal sentido, el Reglamento de Organización y Funciones de SUSALUD, aprobado por Decreto Supremo Nº 008-2014-SA en su artículo 2 establece como finalidad de esta Superintendencia:

*"**Artículo 2.- Finalidad***
SUSALUD tiene por finalidad promover, proteger y defender los derechos de las personas al acceso a los servicios de salud, supervisando que las prestaciones sean otorgadas con calidad, oportunidad, disponibilidad y aceptabilidad, con independencia de quien las financie, así como los que correspondan en su relación de consumo con las Instituciones Administradoras de Fondos de Aseguramiento en Salud (IAFAS) o las Instituciones Prestadoras de Servicios de Salud (IPRESS), incluyendo aquellas previas y derivadas de dicha relación de consumo." (Subrayado propio)

42. Como podrá apreciar la administrada estamos frente a fundamentos u objetos de protección de bienes jurídicos e intereses distintos que soportan la intervención de la ANPDP y SUSALUD, respecto a sus propias actividades de supervisión y ejercicio independiente de su potestad sancionadora. Por un lado, la ANPD busca garantizar y

velar por el derecho constitucional a la protección de los datos personales en su máxima expresión y SUSALUD se centra en promover y supervisar el correcto funcionamiento del sistema prestacional de servicios de salud, debiendo desplegar su potestad sancionadora ante la existencia de un defecto u omisión en la forma de prestación de los servicios a los usuarios. Justamente, es en su búsqueda de garantizar y velar por una adecuada y digna prestación de servicios de atención de salud que SUSALUD inició su propio procedimiento administrativo sancionador contra la administrada, bajo el siguiente hecho imputado:

"La Administrada no habría brindado una adecuada prestación de salud, al haber incumplido con resguardar la confidencialidad y protección de los datos personales calificados como sensibles correspondientes al Paciente, en la medida que se tomó conocimiento el 17 de abril del 2019 que en las redes sociales (Facebook, WhatsApp) se encontraban circulando imágenes y videos no autorizados de la atención otorgada a Paciente durante su estancia en el servicio de emergencia de la Administrada, tales como imágenes (fotografía en camilla: f. 44 al 47) y estudios de diagnóstico (video de tomografía: f. 48), hechos que no se condicen con una adecuada atención de salud." (Folio 253 reverso) (Subrayado propio)

43. En tal sentido, -y contrariamente a lo alegado por la administrada al invocar que existe identidad en la persona, los hechos, así como en la pretensión de la imposición de una sanción de multa (siendo que esto último se aleja de la identificación del bien jurídico o fundamento jurídico de protección)-, conforme a lo expuesto en la presente Primera Cuestión Previa este Despacho concluye que sí es factible sancionar dos veces a un mismo sujeto por el mismo hecho, pero con la salvedad de proteger un bien jurídico distinto, que es la situación en la cual se encuentra la administrada. Consecuentemente, de la evaluación del presente caso, esta Dirección concluye que no se atenta contra el principio del Non bis in ídem, al no concurrir las tres identidades requeridas para la activación de esta garantía.

44. A pesar de lo señalado anteriormente, si bien esta Dirección considera que en este caso no se cumplen los requisitos para fundamentar el Non bis in ídem, ya que no concurre el bien jurídico protegido; es preciso resaltar que si bien el administrado alega que SUSALUD ha iniciado procedimiento sancionador por el mismo hecho, a la fecha no ha impuesto sanción, por lo que no se puede alegar que está siendo doblemente sancionado por el mismo hecho.

45. En todo caso, si la administrada considera que una posible sanción afectaría el principio de Non bis ídem, deberá alegar los fundamentos que considere pertinentes una vez que haya sido sancionado por los hechos señalados.

V. Segunda Cuestión Previa: Sobre la aplicación de los Principios de Tipicidad y Causalidad respecto a la infracción del artículo 17 de la LPDP

45. La administrada considera que se está vulnerando el principio de tipicidad respecto a la imputación por la presunta violación del deber de confidencialidad, al considerar que no corresponde la imputación contenida en el literal g) del artículo 132 del Reglamento de la LPDP debido a que no ha sido el hospital y tampoco ningún representante del mismo quienes han efectuado la publicación de las imágenes del paciente.

46. Como punto de partida es importante señalar que la infracción al deber de confidencialidad contemplado en el artículo 17 de la LPDP se puede configurar a través de los siguientes supuestos: i) la ocurrencia de una difusión consciente y activa desde dentro de la organización que trata los datos hacia terceros no autorizados y, (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 terceros 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.

De lo expuesto en el párrafo anterior, a criterio de este Despacho se han configurado ambos supuestos que conllevan al incumplimiento de la obligación de confidencialidad contenida en el artículo 17 de la LPDP, toda vez que fue personal vinculado contractualmente con la administrada (profesionales médicos, técnico y licenciadas en enfermería) quien trató indebidamente la información y datos personales de carácter sensible del paciente a los que tuvieron acceso para el ejercicio de sus funciones y , adicionalmente, porque la administrada al no contar con mecanismos de seguridad de la información previamente implementados que restrinja los accesos a sus sistemas sobreexpone negativamente los datos personales (sea a su eliminación, obtención de copias no autorizadas, usos indiscriminados y contrarios a la voluntad del titular, entre otros)

47. Al respecto, esta Dirección concuerda y suscribe lo establecido por la DFI en el Informe Final de Instrucción al señalar que las personas jurídicas responderán por su capacidad de cometer infracciones partiendo de la culpabilidad por defectos de organización, siendo que en el presente caso la falta de cuidado se evidencia por no haber tomado las medidas necesarias para el correcto desarrollo de sus actividades de conformidad con la normativa de protección de datos personales, conforme se desarrolla en el en el acápite VIII. Análisis de las cuestiones en discusión.

48. Independientemente de ello, la LPAG establece que se prescindirá del factor subjetivo en la responsabilidad si es que por ley o decreto legislativo se dispone responsabilidad administrativa objetiva por la comisión de infracciones, así el artículo 38 de la LPDP señala lo siguiente: "(...) Los administrados son responsables objetivamente por el incumplimiento de obligaciones derivadas de las normas sobre protección de datos personales". En tal sentido, la responsabilidad objetiva es aquella que no requiere el análisis de ningún factor subjetivo del sujeto infractor, prescindiéndose de los elementos de intencionalidad o imprudencia, y configurándose con la producción de la conducta calificada como infractora para la imposición de la sanción.

49. La confidencialidad de los datos personales debe ser entendida como uno de los fines de la seguridad que implica que no solamente se divulgue activamente datos personales a terceros no autorizados, sino que además se garantice que la información y/o datos personales necesarios para el tratamiento autorizado por sus titulares, así como la intervención para su tratamiento, sean accesibles únicamente a aquellos estrictamente necesarios y legitimados para realizar dicho tratamiento, para lo cual es imprescindible que todo titular de banco de datos y/o responsable de su tratamiento cuente con un nivel de protección suficiente, adecuado y pertinente más

aún cuando involucra un tratamiento de datos personales de carácter especial como son los datos relacionados a la salud. En tal sentido, la LPDP, en el numeral 12 de su artículo 1, ha contemplado como definición de "Nivel suficiente de protección para los datos personales" al *"Nivel de protección que abarca por lo menos la consignación y el respeto de los principios rectores de esta Ley, así como medidas técnicas de seguridad y confidencialidad, apropiadas según la categoría de datos de que se trate."*

50. Este nivel suficiente de protección que todo administrado debe buscar garantizar en sus instalaciones y por parte de aquellos de los cuales se valga para la prestación de sus servicios proviene del reconocimiento del principio rector de seguridad que debe primar en el marco de actuación de los titulares de bancos de datos personales, encargados y/o responsables de realizar el tratamiento de los mismos para el resguardo de la integridad, disponibilidad y confidencialidad de todo dato personal involucrado en alguna de las etapas o formas de tratamiento que realicen.

51. El principio de seguridad está contemplado en el artículo 9 de la LPDP y complementado por lo dispuesto en el artículo 16 de la misma 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."

*"**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." (Subrayado propio)

52. La obligación de guardar confidencialidad contemplada en el artículo 17 de la LPDP, debe ser interpretada conjuntamente y en observancia del principio de seguridad antes referido, teniendo como propósitos regular tanto la obligación a no divulgar o dar a conocer los datos personales con los que alguien se relaciona en el desempeño de sus funciones, como la obligación de contar con medidas de seguridad que garanticen el nivel de protección esperado tanto por la LPDP y su Reglamento. Tales medidas de seguridad deben buscar evitar el acceso de terceros y tratamientos no autorizados o ajenos al tratamiento y finalidad para los cuales fueron recopilados, siendo en el presente caso la prestación oportuna e inmediata de los servicios de salud para la atención de una emergencia médica.

53. Por lo expuesto, esta Dirección concluye que no existe vulneración alguna al principio de tipicidad, toda vez que la vulneración al deber de confidencialidad también implica una omisión de seguridad relevante que permita o facilite el acceso y

tratamiento no autorizados, conforme ha quedado acreditado en el expediente materia de pronunciamiento.

VI. Cuarta Cuestión Previa: Sobre la vinculación entre el Informe Final de Instrucción y el pronunciamiento de esta Dirección

54. 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.
(…)"

55. Por su parte, el artículo 255 de la LPAG, establece lo siguiente:

"Artículo 255.- Procedimiento sancionador
Las entidades en el ejercicio de su potestad sancionadora se ciñen a las siguientes disposiciones:
(…)
5. Concluida, de ser el caso, la recolección de pruebas, la autoridad instructora del procedimiento concluye determinando la existencia de una infracción y, por ende, la imposición de una sanción; o la no existencia de infracción. La autoridad instructora formula un informe final de instrucción en el que se determina, de manera motivada, las conductas que se consideren probadas constitutivas de infracción, la norma que prevé la imposición de sanción; y, la sanción propuesta o la declaración de no existencia de infracción, según corresponda.
Recibido el informe final, el órgano competente para decidir la aplicación de la sanción puede disponer la realización de actuaciones complementarias, siempre que las considere indispensables para resolver el procedimiento. El informe final de instrucción debe ser notificado al administrado para que formule sus descargos en un plazo no menor de cinco (5) días hábiles."

56. 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 implican la autonomía de criterios de ambas, siendo que la autoridad sancionadora o resolutora puede hacer suyos todos los argumentos, conclusiones y recomendaciones expuestos por la autoridad instructora en su informe final de instrucción, así como, en sentido distinto, 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 fueron evaluadas al finalizar la instrucción.

57. 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, considerando su naturaleza no vinculante, y sin que ello implique una vulneración de la predictibilidad o de la expectativa legítima del administrado, la cual no encuentra asidero en la normativa referida al procedimiento administrativo.

58. 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.

VII. Quinta Cuestión Previa: Sobre el Concurso de Infracciones

59. El numeral 6 del artículo 248 de la LPAG establece como uno de los principios de la potestad sancionadora el del Concurso de Infracciones, en los siguientes términos:

"Artículo 248.- Principios de la potestad sancionadora administrativa
La potestad sancionadora de todas las entidades está regida adicionalmente por los siguientes principios especiales:
(…)
6. Concurso de Infracciones.- Cuando una misma conducta califique como más de una infracción se aplicará la sanción prevista para la infracción de mayor gravedad, sin perjuicio que puedan exigirse las demás responsabilidades que establezcan las leyes."

60. La Autoridad Administrativa tiene la obligación, en casos de concurso de infracciones, de aplicar la sanción por la infracción que considere más grave, sin que ello, necesariamente, deba determinarse solo por lo gravoso de la sanción -como bien señala Morón- sino por diversas cuestiones como la trascendencia de la norma infringida, de las obligaciones incumplidas o su influencia en los derechos de terceros.

61. En el presente caso, se ha evidenciado que la administrada no contó con el nivel suficiente de protección para resguardar la confidencialidad de los datos personales sensibles del padre de la denunciante, en tanto la filtración de los mismos se materializó por accesos y tratamientos no autorizados como consecuencia de la falta de medidas de seguridad adecuadas y oportunas, las mismas que debieron estar previamente implementadas y en ejecución por parte de la administrada.

62. Al respecto, esta Dirección advierte que la configuración del incumplimiento del deber de confidencialidad también es consecuencia de una omisión de nivel de protección adecuado y oportuno por falta de medidas de seguridad suficientes que busquen resguardar la reserva de los datos personales de los pacientes de la administrada.

63. Considerando el nivel de complejidad que reviste el tipo de tratamiento que realizan las entidades prestadoras de servicios de atención médica (así como el volumen de datos personales que administra), se encuentran obligados a garantizar que cualquier trabajador o persona vinculada al mismo, independientemente de su relación contractual, y que pueda tener acceso a los datos sensibles de los usuarios lo haga bajo la estricta necesidad de conocer los mismos, únicamente, para la ejecución de la prestación de salud. Para poder lograr esto las entidades sanitarias deben establecer protocolos y medidas de seguridad efectivos destinados a prevenir y bloquear la concreción de accesos indiscriminados y usos indebidos a los datos de los pacientes dentro de sus instalaciones.

64. Conforme se ha desarrollado en numerales anteriores, la LPDP contempla dentro de los principios rectores de obligatoria observancia para garantizar la debida

protección de los datos personales, sea por el titular de los bancos de datos personales, responsables y/o encargados de su tratamiento, al principio de seguridad, recogido en su artículo 9 y complementado por su artículo 16. Dichos artículos establecen que, independientemente, del tipo de tratamiento que realicen los responsables es obligación de los mismos establecer y mantener medidas técnicas, organizativas y legales necesarias y suficientes para garantizar la seguridad de los datos personales en su máxima expresión, evitando su alteración, pérdida, tratamiento o acceso no autorizado.

65. En este sentido, el principio de seguridad busca garantizar y resguardar la confidencialidad de los datos personales que debe primar en todo tratamiento que no haya sido liberado de dicha carga por parte de su titular. En consecuencia, la omisión referida afecta a más de una norma jurídica, al incumplir la administrada con el mismo hecho obligaciones recogidas de forma autónoma por la LPDP, pero estrechamente vinculadas entre sí para la aplicación al presente caso.

66. Resulta pertinente tomar en cuenta que los principios rectores representan obligaciones que determinan la licitud del tratamiento de los datos personales, tanto en lo que concierne a los tipos, cantidades u oportunidad de los datos personales (principio de Finalidad, Proporcionalidad y Calidad), como a los requisitos para efectuar tal tratamiento (principio de Consentimiento, principio de Seguridad y entendido como principio, el deber de Confidencialidad)

En tal sentido, esta Dirección considera que si bien solo el principio de Seguridad se encuentra literalmente reconocido como un principio rector en el artículo 9 de la LPDP y complementado por el artículo 16 de la misma ley y el artículo 10 del Reglamento de la LPDP, no se excluye la posibilidad de admitir la misma calidad al artículo 17 de la LPDP, debiendo entenderse también que el listado de principios rectores es enunciativo, no cerrado, de acuerdo con el artículo 12 de la LPDP:

"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.
Los principios rectores señalados sirven también de criterio interpretativo para resolver las cuestiones que puedan suscitarse en la aplicación de esta Ley y de su reglamento, así como de parámetro para la elaboración de otras disposiciones y para suplir vacíos en la legislación sobre la materia."

67. Considerando factores generales, como el mayor ámbito de exigibilidad del cumplimiento del artículo 17 de la LPDP, así como su también valoración como principio rector del tratamiento de datos personales, es que el incumplimiento de tal artículo, que se subsume como infracción en la tipificación del literal g) del numeral 2 del artículo 132 del Reglamento de la LPDP, constituye la infracción de mayor gravedad.

68. En tal sentido, en caso de verificarse el incumplimiento de las medidas de seguridad para tratamiento de datos sensibles sobre i) no documentar los procedimientos de gestión de accesos, privilegios y verificación periódica de privilegios (numeral 1 del artículo 39° del RLPDP) y ii) no generar ni mantener registros de interacción lógica con el banco de datos personales de pacientes (numeral 2 del

artículo 39° del RLPDP); tales extremos integrantes del hecho imputado N°1 no serán tomados en cuenta al momento de aplicar la sanción correspondiente a la infracción tipificada en el literal c) del numeral 2 del artículo 132 del Reglamento de la LPDP.

VIII. Cuestiones en discusión

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

69.1. Si la administrada es responsable por los siguientes hechos infractores:

i) La administrada no habría cumplido con implementar las medidas de seguridad para el tratamiento de datos personales sensibles que realiza a través de los sistemas denominados “RIS” y “PACS” que utiliza para programar y visualizar tomografías, radiografías y otros diagnósticos por imágenes, al: i) No documentar los procedimientos de gestión de accesos, privilegios y verificación periódica de privilegios. Obligación establecida en el numeral 1 del artículo 39 del Reglamento de la LPDP; y ii) No generar ni mantener registros de interacción lógica con el banco de datos personales de pacientes. Obligación establecida en el numeral 2 del artículo 39 del Reglamento de la LPDP.

ii) La administrada habría realizado tratamiento de datos personales incumpliendo la obligación de confidencialidad, establecida en el artículo 17 de la LPDP, al haberse filtrado datos personales sensibles del padre de la denunciante sin consentimiento.

69.2. En el supuesto de resultar responsable, si debe aplicarse la exención de responsabilidad por la subsanación de la infracción, prevista en el literal f) del 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.

69.3. 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.

VI. Análisis de las cuestiones en discusión

Sobre el presunto incumplimiento de las medidas de seguridad contempladas en los numerales 1 y 2 del artículo 39 del Reglamento de la LPDP

70. El 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."

71. A mayor abundamiento, el artículo 16 de la LPDP y el artículo 10 del Reglamento de la LPDP señalan como objetivo de la adopción de tales medidas técnicas, organizativas y legales, evitar la alteración, pérdida, tratamiento o acceso no autorizado a los datos personales, en los siguientes términos:

Artículo 16 de la LPDP:

"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."

Artículo 10 del Reglamento de la LPDP:

"Artículo 10.- Principio de seguridad.
En atención al principio de seguridad, en el tratamiento de los datos personales deben adoptarse las medidas de seguridad que resulten necesarias a fin de evitar cualquier tratamiento contrario a la Ley o al presente reglamento, incluyéndose en ellos a la adulteración, la pérdida, las desviaciones de información, intencionales o no, ya sea que los riesgos provengan de la acción humana o del medio técnico utilizado."

72. Por su parte, sobre el tratamiento automatizado de datos personales, el artículo 39 del Reglamento de la LPDP contempla el requisito de tener documentados los procedimientos de gestión de accesos, de privilegios, de verificación periódica de privilegios, así como los registros de interacción lógica:

"Artículo 39.- Seguridad para el tratamiento de la información digital.
Los sistemas informáticos que manejen bancos de datos personales deberán incluir en su funcionamiento:

1. El control de acceso a la información de datos personales incluyendo la gestión de accesos desde el registro de un usuario, la gestión de los privilegios de dicho usuario, la identificación del usuario ante el sistema, entre los que se encuentran usuario-contraseña, uso de certificados digitales, tokens, entre otros, y realizar una verificación periódica de los privilegios asignados, los cuales deben estar definidos mediante un procedimiento documentado a fin de garantizar su idoneidad.

2. Generar y mantener registros que provean evidencia sobre las interacciones con los datos lógicos, incluyendo para los fines de la trazabilidad, la información de cuentas de usuario con acceso al sistema, horas de inicio y cierre de sesión y acciones relevantes. Estos registros deben ser legibles, oportunos y tener un procedimiento de disposición, entre los que se encuentran el destino de los registros, una vez que éstos ya no sean útiles, su destrucción, transferencia, almacenamiento, entre otros.

Asimismo, se deben establecer las medidas de seguridad relacionadas con los accesos autorizados a los datos mediante procedimientos de identificación y autenticación que garanticen la seguridad del tratamiento de los datos personales."

73. En la RD de Inicio se le imputó a la administrada el incumplimiento de la obligación contenida en ambos supuestos del artículo 39 del Reglamento de la LPDP, respecto a

los sistemas denominados "RIS" y "PACS" que utiliza para programar y visualizar tomografías, radiografías y otros diagnósticos por imágenes.

74. La imputación se sustentó en los resultados de las actividades de fiscalización llevadas a cabo en las instalaciones de la administrada en el mes de setiembre de 2019, así como de la evaluación de la documentación remitida por la administrada, siendo que a través del Informe de Fiscalización N°163-2019-JUS/DGTAIPD-DFI-AARM de 11 de noviembre de 2019 (Folios 195 a 199), se advirtió lo siguiente:

*"**V. ANÁLISIS DE LOS HECHOS IMPUTADOS Y PRESUNTAS INFRACCIONES***
(...)
16. En atención a la denuncia presentada esta Dirección procedió a realizar actuaciones de investigación, así, se realizaron tres visitas de fiscalización a la administrada, constando en el Acta de Fiscalización n° 2, que el personal del hospital que atendió la visita, reconoció que la tomografía difundida del paciente fue visualizada en el área de servicio de medicina de hospitalización del quinto piso. Al respecto, el personal fiscalizador inspeccionó dicha área verificando que cuenta con una computadora que está visible al público, la cual para el acceso tiene un usuario genérico denominado "quinto piso" y una contraseña única utilizada por los médicos y residentes de turno (f. 51).

17. En atención a lo verificado en la mencionada visita, se solicitó a la administrada documentación referente a la gestión de accesos, privilegios y verificación periódica de privilegios, documentación que no presentó, debido a que según el Informe n.°159-2019-ET.INFORMATICA-OEI-HEJCU del Jefe de Equipo de Informática y Telecomunicaciones indica que: "(...) el sistema FUJIFILM implementado el año 2009 no evidencia las interacciones de los datos lógicos, incluyendo la trazabilidad, la información de cuentas de usuario con acceso al sistema, horas de inicio y cierre de sesión y acciones relevantes de acuerdo a lo que establece la Ley de Protección de Datos Personales". Asimismo, lo remitido por la administrada (fojas 128 a 133), solo hace referencia a un proyecto de revisión y aprobación para su posterior implementación, por lo cual no contaría con las medidas de seguridad necesarias para tener un control adecuado del tratamiento de los datos personales que realiza.
(…)" (Subrayado propio)

75. Mediante Informe Técnico N°271-2019-DFI-ORQR de 12 de diciembre de 2019 (Folios 205 a 206) el analista de fiscalización concluyó que la administrada no cumplía con las mediadas de seguridad técnicas requeridas en el artículo 39 del Reglamento de la LPDP por las consideraciones expuestas a continuación:

*"**IV. Evaluación del cumplimiento de las medidas de seguridad***
(...)

1. *Respecto a la obligación de tener documentados los procedimientos de gestión de accesos, gestión de privilegios y verificación periódica de privilegios asignados, a través del Acta de Fiscalización N°02-2019, se solicitó a la fiscalizada remitir documentación respecto a los procedimientos de gestión de accesos, gestión de privilegios y verificación periódica de privilegios asignados, para lo cual se le otorgó un plazo de 05 días hábiles (f 52). Cabe precisar que en la documentación remitida el 02 de octubre de 2019, mediante el Oficio N° 001670-2019-DG-OAJ-HEJCU, ingresado a través de la Hoja de Trámite N° 70041-2019MSC, la entidad fiscalizada remitió documentación, en la que adjunta el documento denominado "Proyecto de Directiva Administrativa N° 001-2019-HEJCU/OEI Lineamientos para regular el acceso, asignación de privilegios y uso adecuado de los sistemas y recursos informáticos en el Hospital de Emergencias José Casimiro Ulloa (Proyecto en Elaboración).*

> *Al respecto, luego de revisar y analizar el referido documento se puede determinar que la fiscalizada no cuenta con procedimientos documentados de gestión de accesos, gestión de privilegios y verificación periódica de privilegios asignados ya que la información remitida hace referencia a un proyecto en elaboración y no a procedimientos implementados y formalmente establecidos por la entidad. Es muy importante precisar que durante el proceso de fiscalización la entidad fiscalizada indicó, que la difusión de las imágenes de la tomografía del paciente (…), se realizaron desde el "Servicio de Medicina", ubicado en el quinto piso del Hospital. Asimismo, se constató que en dicho servicio cuentan con una computadora con usuario genérico con el cual acceden todos los médicos y residentes de turno, evidenciando que no cuenta con medidas de seguridad correspondientes al control de accesos y/o privilegios debidamente implementadas. Por lo tanto, se ha comprobado que la fiscalizada no cuenta con procedimientos documentados respecto a la gestión de accesos, gestión de privilegios y verificación periódica de privilegios asignados. Por lo que estaría incumpliendo con el numeral 1 del artículo 39° del Reglamento de la LPDP, el cual indica (…). En ese sentido, HOSPITAL DE EMERGENCIAS JOSÉ CASIMIRO ULLOA, no cumple con la disposición mencionada.*
>
> 2. *Respecto a generar y mantener registros de interacción lógica con el banco de datos personales de pacientes. Durante el proceso de fiscalización se verificó que los sistemas: "RIS" y "PACS", no generan ni mantienen registros de interacción lógica (referentes al inicio de sesión, cierre de sesión y acciones relevantes) (f. 49). Cabe precisar de que aún si los sistemas "RIS" y "PACS" tuvieran la facultad de generar los referidos registros de interacción, estos no serían de utilidad ya que el hacer uso de cuentas de usuario genéricas imposibilita tener registros certeros respecto a la trazabilidad de la actividad de las personas que hacen uso de los sistemas ya que todas estas comparten una misma cuenta de usuario. Al respecto, el numeral 2 del artículo 39° del Reglamento de la LPDP indica (…). En ese sentido, HOSPITAL DE EMERGENCIAS JOSÉ CASIMIRO ULLOA, no cumple con la disposición mencionada.*

(…) (Subrayado propio)

76. Revisados los alegatos presentados por la administrada, así como la documentación obrante en el expediente, este Despacho observa que la administrada no ha cumplido con evidenciar que los sistemas PACS y RIS cuenten con las medidas de seguridad debidamente implementadas en su funcionamiento. Por el contrario, de las propias declaraciones de la administrada se desprende que reconoce la falta de adecuación de sus sistemas a lo requerido por el Reglamento de la LPDP (al no contar con mecanismos efectivos para el control de los accesos y/o privilegios, así como la generación de registros de interacción lógica que permita identificar quién ingresó, en qué momento y qué acción respecto a los datos realizó en los sistemas)

77. Respecto a la documentación de los procedimientos de acceso y gestión de privilegios, la administrada presentó un proyecto en elaboración de la "*Directiva Administrativa N°001-2019-HEJCU/OEI Lineamientos para regular el acceso, asignación de privilegios y uso adecuado de los sistemas y recursos informáticos en el Hospital de Emergencias José Casimiro Ulloa"* (Folios 128 a 133), mas no ha acreditado la materialización de su implementación y aplicación efectiva, motivo por el cual este Despacho no puede considerarla como una acción de enmienda. Por el contrario, en el Informe Técnico N°159- 2019 - ET. INFORMATICA-OEI-HEJCU del 1 de octubre de 2019 (Folios 126 a 127) se informa que se está trabajando en un proyecto de directiva lo que demuestra que ni siquiera se trata de una versión final y apta para su difusión a los usuarios al estar pendiente de revisiones y aprobaciones: *"(…) Al respecto, informo a usted que esta área, como parte de sus procesos de*

mejora continua, viene trabajando en la elaboración del mencionado documento toda vez que a la fecha no se dispone de esta documentación. Es preciso informar que el documento que se viene elaborando es un proyecto de directiva de los sistemas y recursos informáticos implementados en el Hospital que debe ser revisado, corregido (de ser el caso) y visado por su jefatura, para la posterior aprobación por parte de la Dirección General y una vez aprobada difundirlo a todos los usuarios de la Institución. Se adjunta el proyecto de la directiva que se viene elaborando (…)" (Subrayado propio)

78. Respecto al extremo de generar y mantener registros de interacción lógica, la administrada refiere en sus descargos que existe un proyecto de actualización de los sistemas RIS y PACS en el cual se está considerando la interacción lógica; siendo que mediante Oficio 1359-2019 DGHEJCU de 13 de agosto de 2019 (Folio 125) se le solicitó a la Oficina General de Tecnología de la Información -OGTI del MINSA el apoyo para la evaluación de especificaciones técnicas sobre la adquisición de dichos sistemas.

Al respecto, este Despacho advierte que tampoco se ha acreditado la adecuación de los sistemas PACS y RIS, dado que solo consta la solicitud del apoyo en la evaluación de las especificaciones técnicas sobre la "Adquisición de Sistema Electrónico de Archivo y comunicación de imágenes médicas (PACS) con sistema de administración radiológico (RIS) y digitalización con impresión de imágenes" (Folios 137 a 174) y la respuesta a esta solicitud que obra en el Informe N°093-2019-OGTI-DT/MINSA del 13 de setiembre de 2019 (Folios 123 a 124), mas ello no evidencia que los sistemas PACS y RIS de la administrada puedan generar y mantener los registros de interacción lógica.

79. Mediante Informe Técnico N° 60-2020-DFI-ORQR de 27 de febrero de 2020 (Folios 312 a 313) el analista de fiscalización en seguridad de la información de la DFI emitió informe complementario de evaluación de la implementación de las medidas de seguridad por parte del administrado, en función a la información remitida por éste en sus descargos presentados el 17 de febrero de 2020, reafirmando sus conclusiones respecto al incumplimiento de los requerimientos del artículo 39 del Reglamento de la LPDP.

80. Por lo expuesto, este Despacho observa que sí se ha configurado la infracción imputada respecto al incumplimiento de las medidas de seguridad contenidas en el artículo 39 del Reglamento de la LPDP. No obstante ello, tal y como ha sido referido en el desarrollo de la Quinta Cuestión Previa, en aplicación del concurso de infracciones advertido, para el presente caso, la responsabilidad derivada de este incumplimiento de medidas de seguridad, respecto a los sistemas PACS y RIS, será subsumida en la sanción de multa correspondiente a la infracción de mayor gravedad por incumplimiento de la obligación de confidencialidad del artículo 17 de la LPDP.

Sobre el presunto incumplimiento del deber de confidencialidad

81. La LPDP establece como uno de sus principios rectores, el consentimiento en el artículo 5 que señala que *"Para el tratamiento de los datos personales debe mediar el consentimiento de su titular"*. Dicho consentimiento debe ser libre, expreso e informado de acuerdo a lo señalado en el numeral 5 de la LPDP.

82. El numeral 1 del artículo 13 de la LPDP establece que *"el tratamiento de datos personales debe realizarse con pleno respeto de los derechos fundamentales de sus titulares y de los derechos que esta Ley les confiere. (…)"*

83. Es en este contexto, que una de las formas de materializar el resguardo y respeto de los datos personales sobre los cuales una entidad realiza tratamiento para la ejecución de la prestación de los servicios que ofrece a sus usuarios, es a través del cumplimiento de la obligación de confidencialidad que se encuentra prevista en el artículo 17 de la LPDP:

> ***"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."* (El subrayado es nuestro)

84. Reviste mayor importancia cuando se involucra en el tratamiento a los datos personales de carácter sensible, como los relacionados al estado de salud de una persona; donde debe prevalecer la finalidad de protección de la esfera íntima del titular y donde el responsable de efectuar el tratamiento debe instaurar y supervisar con rigurosidad que sus dependientes -o personal del cual se valga para brindar sus servicios- cumplan con la prohibición de revelar o facilitar a terceros no autorizados el acceso y/o conocimiento de los mismos.

85. En la RD de Inicio se imputó como hecho infractor que la administrada habría realizado tratamiento de datos personales incumpliendo la obligación de confidencialidad, establecida en el artículo 17 de la LPDP, al haberse filtrado datos personales sensibles del padre de la denunciante sin consentimiento.

86. Conforme ha sido desarrollado en la Segunda Cuestión Previa de la presente Resolución, la configuración de la infracción al deber de confidencialidad se da por i) la ocurrencia de una difusión consciente y activa desde dentro de la organización que trata los datos hacia terceros no autorizados o, (ii) una omisión de seguridad relevante al interior de la organización que facilite y permita que datos que deben estar bajo reserva y resguardo de un titular de banco de datos personales sean conocibles por terceros no autorizados.

87. Al respecto, a criterio de esta Dirección, la administrada ha incurrido en ambos supuestos de incumplimiento al haberse evidenciado, principalmente, lo siguiente:

87.1. Fue el propio personal de la administrada (profesional médico, técnico y de enfermería) quien captó imágenes fotográficas, a través de sus dispositivos móviles, del estado físico del paciente mientras este se encontraba en la sala de trauma shock, así como de su información clínica respecto a su estado de salud (tomografía), quienes propiciaron finalmente que las mismas se filtren a través de diversos medios, como es de público conocimiento. Como establecimiento de salud, la administrada es responsable por todo tipo de daño o perjuicio causado a sus pacientes y/o usuarios de los servicios de salud, por la negligencia o imprudencia en el ejercicio de las funciones de los profesionales, técnicos, auxiliares y/o cualquier otro tercero que tenga cierto grado de dependencia con el nosocomio. Por consiguiente, el argumento de la administrada respecto a que las personas que filtraron los datos del paciente no actuaron en su representación y ni por intermedio de ella y que inclusive han sido sometidas procedimientos administrativos disciplinarios debe ser desestimado. En tal sentido el artículo 48 de la Ley General de Salud recoge la figura de la responsabilidad solidaria por cualquier actuación negativa del personal de salud en detrimento de sus pacientes, enfatizando inclusive la responsabilidad por omisión del establecimiento de salud:

> *"**Artículo 48 de la Ley General de Salud:***
> *El establecimiento de salud o servicio médico de apoyo es solidariamente responsable por los daños y perjuicios que se ocasionan al paciente, derivados del ejercicio negligente imprudente o imperito de las actividades de los profesionales, técnicos o auxiliares que se desempeñan en éste con relación de dependencia.*
> *Es exclusivamente responsable por los daños y perjuicios que se ocasionan al paciente por no haber dispuesto o brindado los medios que hubieren evitado que ellos se produjeran, siempre que la disposición de dichos medios sea exigible atendiendo a la naturaleza del servicio que ofrece."* (Subrayado propio)

87.2. Sobre lo mencionado en el numeral anterior, este Despacho advierte que la administrada no cumplió con remitir los contratos del personal médico que atendió la emergencia del padre de la denunciante y/o los documentos que aseguren la confidencialidad de la información a la que acceden en ejercicio de sus funciones (solicitud realizada en el Acta de Fiscalización 2-2019). Por tanto, la administrada no acreditó que cuente con acuerdos de confidencialidad con sus trabajadores y/o personal vinculado, sea de forma independiente o a través de una cláusula de confidencialidad en el contrato de trabajo y/o de prestación de servicios, para la protección de los datos personales de sus pacientes.

87.3. La administrada no contaba con un nivel suficiente y adecuado de protección de los datos personales, implementado de forma preventiva, sea en los sistemas automatizados que contienen datos de salud de sus usuarios (como el PACS y RIS) como en el área de "Servicio de Medicina de Hospitalización" del quinto piso del hospital al haberse constatado (conforme obra en el Acta de Fiscalización 2-2019) que en dicho ambiente cuenta con una computadora que está visible al público, permitiendo el acceso a través de un usuario genérico denominado "quinto piso" y una contraseña única utilizada por los médicos y residentes de turno. En tal sentido, debe desestimarse el argumento de la administrada (descrito en el

considerando 25.3 de esta Resolución) respecto a que habría demostrado propiciar un entorno seguro y confiable para el tratamiento de datos personales que le permita mitigar los riesgos de pérdida, alteración, tratamiento o acceso no autorizado de los datos, toda vez que del expediente materia de análisis y de los hechos se evidenció lo contrario.

87.4. Tal y como declaró la administrada, antes del 17 de abril de 2019 no contaba con ningún documento que regulara el uso de los teléfonos y/o dispositivos móviles, habiendo referido que a la fecha de la segunda visita de fiscalización (25 de setiembre de 2019) ya existía una directiva interna donde se restringe el uso de los teléfonos celulares (Folio 51). Sin embargo, la administrada no ha evidenciado que dicha directiva interna haya sido instaurada y difundida a todo el personal que presta servicios en el hospital.

88. Debe entenderse el deber de confidencialidad como un pilar clave que debe regir en toda forma de tratamiento de datos personales para garantizar una adecuada protección de los mismos, evitando que sean expuestos y/o tratados para fines distintos sin el consentimiento de sus titulares. Es en este sentido que este deber de confidencialidad está estrechamente vinculado, como ha sido expuesto en la Segunda Cuestión Previa de esta Resolución Directoral al Principio de Seguridad en tanto no puede garantizarse la primera sin la implementación de medidas técnicas, organizativas y legales preventivas a los riesgos conocidos e inherentes de toda actividad que involucre el uso de sistemas informáticos y/o automatizados, así como el tratamiento permanente y voluminoso de datos personales de carácter sensible que realiza una entidad hospitalaria.

89. En opinión de esta Dirección, el quebrantamiento del deber de confidencialidad se ha visto potenciado por la falta de actuación preventiva por parte del responsable del tratamiento -la administrada- no habiendo acreditado hasta el momento su adecuación y observancia de la normativa de protección de datos personales, a efectos de mitigar que situaciones como la denunciada se presenten nuevamente en perjuicio de sus pacientes.

90. Cabe mencionar que en el presente caso, los datos que fueron expuestos fueron datos sensibles relativos a la salud, que corresponden a la esfera más íntima de la persona, lo que agrava la conducta infractora, ya que atenta contra la dignidad humana. Al respecto, el artículo 1 de la Constitución Política del Perú establece que "La defensa de la persona humana y el respeto de su dignidad son el fin supremo de la sociedad y del Estado." En este caso se ha expuesto información de una persona vulnerando el derecho a la protección de sus datos, pero la calidad de los datos expuestos son sensibles al ser relativos a la salud, al tratarse de información médica, imágenes de ésta en la sala de Traumashock, así como información de carácter médico. Como puede observarse, dentro de los datos considerados relativos a la salud, los datos expuestos son extremadamente sensibles al exponer información médica relacionada con la intervención médica por parte de la administrada ante una situación de emergencia, que incluyen imágenes tomadas en un área que no es de acceso público.

91. Finalmente, la administrada hizo alusión a una incorrecta motivación de la RD de Inicio; sin embargo, al no haber identificado el extremo específico con claridad este Despacho no puede pronunciarse al respecto. Por el contrario, de la documentación y evidencia recabada se concluye que se han configurado los supuestos de hecho infractores.

92. Por lo expuesto en el presente acápite, este Despacho concluye que sí se ha configurado la infracción imputada respecto al incumplimiento de la obligación de confidencialidad contemplada en el artículo 17 de la LPDP.

Sobre las sanciones a aplicar a la infracción

93. 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.

94. 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[37], sin perjuicio de las medidas correctivas que puedan determinarse de acuerdo con el artículo 118 del Reglamento de la LPDP[38].

95. En el presente caso, se ha establecido la responsabilidad de la administrada por lo siguiente:

i) No haber cumplido con implementar las medidas de seguridad para el tratamiento de datos personales sensibles que realiza a través de los sistemas denominados “RIS” y “PACS” que utiliza para programar y visualizar tomografías, radiografías y otros diagnósticos por imágenes, al: i) No documentar los procedimientos de gestión de accesos, privilegios y verificación periódica de privilegios. Obligación establecida en el numeral 1 del artículo 39 del Reglamento de la LPDP; y ii) No generar ni mantener registros de interacción lógica con el banco de datos personales de pacientes. Obligación establecida en el numeral 2 del artículo 39 del Reglamento de la LPDP; con lo

[37] **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 tributarias (UIT).”

[38] **Reglamento de la Ley de Protección de Datos Personales, aprobado por Decreto Supremo Nº 003-2013-JUS**
“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 posible, medidas correctivas destinadas a eliminar, evitar o detener los efectos de las infracciones.”

cual se configurar la infracción grave tipificada en el literal c) del numeral 2 del artículo 132 del Reglamento de la LPDP, infracción sancionable con una multa mínima desde más de cinco unidades impositivas tributarias (5UIT) hasta cincuenta unidades impositivas tributarias (50UIT).

ii) Haber realizado tratamiento de datos personales incumpliendo la obligación de confidencialidad, establecida en el artículo 17 de la LPDP, al haberse filtrado datos sensibles del padre de la denunciante sin consentimiento; con lo cual se configura la infracción grave tipificada en el literal g) del numeral 2 del artículo 132 del Reglamento de la LPDP, infracción sancionable con una multa desde más de cinco unidades impositivas tributarias (5UIT) hasta cincuenta unidades impositivas tributarias (50UIT).

96. Por la existencia del concurso de infracciones detallado en la Quinta Cuestión Previa de la presente Resolución Directoral, debe reiterarse en este punto que la sanción por la responsabilidad derivada del primer hecho infractor será será subsumida en la sanción de multa correspondiente a la infracción de mayor gravedad por incumplimiento de la obligación de confidencialidad del artículo 17 de la LPDP. Al respecto, se debe de tener en cuenta que la media en amabas infracciones es de veinticinco (25) Unidades Impositivas Tributarias, lo que se tendrá en cuenta como punto de partida para evaluar el monto de la sanción.

97. Cabe señalar que esta Dirección determina el monto de la multa a ser impuesta tomando en cuenta para su graduación los criterios establecidos en el numeral 3 del artículo 248 de la LPAG. En tal sentido, debe prever que la comisión de la conducta sancionable no resulte más ventajosa para el infractor que cumplir las normas infringidas o asumir la sanción administrativa, por lo que la sanción deberá ser proporcional al incumplimiento calificado como infracción, observando para ello los criterios que dicha disposición señala para su graduación.

98. En el presente caso, se considera como criterios relevantes para graduar las sanciones, los siguientes:

Respecto al hecho infractor a sancionar:

a) <u>El beneficio ilícito resultante por la comisión de la infracción:</u>

La administrada es una entidad pública, sin ánimo de lucro, que se dedica al rubro de la salud, dedicada especialmente a la atención de emergencias y urgencias. Por lo tanto, la infracción cometida no les genera beneficio ilícito.

b) <u>La probabilidad de detección de las infracciones:</u>

La probabilidad de detección de la conducta infractora ha sido alta, en tanto los hechos denunciados fueron de conocimiento público, así como por las declaraciones de las autoridades de salud al anunciar que las personas que captaron las fotografías habían sido identificadas y estaban siendo investigadas.

c) La gravedad del daño al interés público y/o bien jurídico protegido:

En particular, se ha evidenciado que la administrada no ha cumplido con garantizar un nivel suficiente de protección de los datos personales sensibles de sus pacientes, al no contar con medidas de seguridad idóneas que busquen resguardar la confidencialidad de los mismos, orientando su actuar a prevenir el acceso y tratamiento por terceros no autorizados.

Asimismo, es necesario tener en cuenta que no se ha evidenciado una práctica sistemática de difusión de información médica. Pero al mismo tiempo, si bien se han difundido los datos de una sola persona, la calidad de datos expuesto ha sido sensible, al estar relacionados con la salud, y que además corresponden a una atención de emergencia.

d) El perjuicio económico causado:

No se evidencia un perjuicio económico resultante de la comisión de la infracción.

e) La reincidencia en la comisión de la infracción:

La administrada no fue sancionada anteriormente por la infracción.

f) Las circunstancias de la comisión de la infracción:

Este Despacho advierte que la administrada no ha llevado a cabo actuaciones de enmienda, en tanto no ha cumplido con evidenciar haber implementado medidas de seguridad necesarias para impedir que se genere la ocurrencia de una situación similar, específicamente respecto a la adecuación de sus sistemas informáticos PACS y RIS a lo requerido por el artículo 39 de la LPDP, lo cual debe ser replicado en cualquier sistema automatizado a través del cual efectúe tratamiento de datos su personal. Tampoco ha cumplido con acreditar que celebra acuerdos de confidencialidad con los profesionales médicos y, en general, con cualquier persona de la cual se valga para llevar a cabo la prestación de sus servicios (como personal administrativo, locadores, residentes médicos, enfermeras(os), técnicos de archivo) ni que restringe el uso de dispositivos móviles en situaciones de emergencia.

Asimismo, es preciso tener en cuenta que los datos expuestos, al ser el agraviado un ex presidente del Perú y figura pública, una consecuencia prevista era la difusión a través de diversos medios de los datos dada la curiosidad pública que generó la atención médica señalada, por lo tanto es clara la falta diligencia al momento que se trataron los datos de salud materia de la infracción cometida.

Así como también es preciso mencionar que en este caso, si bien las medidas correctivas van a tener como objetivo evitar que esta situación se repita con futuros pacientes, no será posible retrotraer la situación al estado anterior, puesto que no se tiene control respecto a quiénes accedieron y almacenaron las imágenes una vez difundidas.

La existencia o no de intencionalidad en la conducta del infractor:

En el presente caso, ha quedado probada la responsabilidad de la administrada en la comisión de las infracciones imputadas, no habiéndose advertido por este Despacho acción de enmienda efectiva y probada respecto a tales situaciones.

98. Es pertinente indicar que para imponer la sanción se tendrá en cuenta la suma de todos los criterios que permiten graduar la sanción conforme a los argumentos desarrollados a lo largo de la presente Resolución Directoral.

SE RESUELVE:

Artículo 1.- Sancionar a HOSPITAL DE EMERGENCIAS JOSE CASIMIRO ULLOA con una multa ascendente a veinticinco unidades impositivas tributarias (25 UIT) por la comisión de la infracción grave tipificada en el literal g), numeral 2, del artículo 132° de Reglamento de la LPDP: *"Incumplir la obligación de confidencialidad establecida en el artículo 17 de la Ley N° 29733".*

Artículo 2.- Imponer como medida correctiva a HOSPITAL DE EMERGENCIAS JOSE CASIMIRO ULLOA acreditar que:

i) celebra acuerdos de confidencialidad con su personal, sea de forma independiente o a través de una cláusula de confidencialidad en el contrato de trabajo y/o de locación de servicios,
ii) respecto a los sistemas PACS y RIS, a) cuenta con procedimientos documentados de gestión de accesos, gestión de privilegios y verificación periódica de privilegios asignados y b) generan y mantienen registros de interacción lógica (referentes al inicio de sesión, cierre de sesión y acciones relevantes), conforme lo requerido en los numerales 1 y 2 del artículo 39 del Reglamento de la LPDP, respectivamente.

Para el cumplimiento de tales medidas correctivas, se otorga el plazo de cuarenta y cinco (45) 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(s) medida(s) correctiva(s) es de treinta (30) días hábiles de notificada la resolución que resuelve el recurso y agota la vía administrativa.

Artículo 3.- Informar a HOSPITAL DE EMERGENCIAS JOSE CASIMIRO ULLOA, que el incumplimiento de las medidas correctivas constituye la comisión de la infracción tipificada como muy grave en el literal d) del numeral 3 del artículo 132 del Reglamento de la LPDP

Artículo 4- Informar a HOSPITAL DE EMERGENCIAS JOSE CASIMIRO ULLOA, 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[39].

[39] **Texto Único Ordenado de la Ley N° 27444, Ley del Procedimiento Administrativo General, aprobado por Decreto Supremo Nº 004-2019-JUS**

Artículo 5.- Informar a HOSPITAL DE EMERGENCIAS JOSE CASIMIRO ULLOA, que deberá realizar el pago de la multa en el plazo de veinticinco (25) días hábiles desde el día siguiente de notificada la presente Resolución.

Artículo 6.- Informar a HOSPITAL DE EMERGENCIAS JOSE CASIMIRO ULLOA que en caso 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 que pone fin la vía administrativa.

Artículo 7.- Informar a HOSPITAL DE EMERGENCIAS JOSE CASIMIRO ULLOA que 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[40]. Para el pago de la multa deberá considerar el valor de la UIT del año 2019.

Artículo 8.- Notificar a HOSPITAL DE EMERGENCIAS JOSE CASIMIRO ULLOA, la presente Resolución Directoral.

Regístrese y comuníquese.

PERÚ Ministerio de Justicia y Derechos Humanos
DIRECCIÓN DE PROTECCIÓN DE DATOS PERSONALES
M. GONZÁLEZ L.

Firmado digitalmente por GONZALEZ LUNA Maria Alejandra FAU 20131371617 soft
Fecha: 2020.12.02 13:59:02 -05'00'

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

"**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."

[40] **Reglamento de la Ley de Protección de Datos Personales, aprobado por Decreto Supremo Nº 003-2013-JUS**
"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."