



Resolución Directoral N° 2243-2022-JUS/DGTAIPD-PPDP

Expediente N°
111-2021-JUS/DGTAIPD-PAS

16 de junio de 2022

VISTOS:

El Informe N° 150-2021-JUS/DGTAIPD-DFI del 23 de noviembre de 2021¹, emitido por la Dirección de Fiscalización e Instrucción de la Dirección General de Transparencia, Acceso a la Información Pública y Protección de Datos Personales (en adelante, la DFI), y demás documentos que obran en el respectivo expediente, y;

CONSIDERANDO:

I. Antecedentes

1. Mediante la Orden de Fiscalización N° 157-2019-JUS/DGTAIPD-DFI del 26 de noviembre de 2019², se dispuso efectuar una visita a fin de iniciar la fiscalización a Colegio Parroquial Cristo Rey, identificado con RUC N° 20119880328 (en adelante, la administrada), con la finalidad de verificar si cumple con las disposiciones de la Ley N° 29733, Ley de Protección de Datos Personales (en adelante, LPDP) y su reglamento, aprobado por el Decreto Supremo N° 003-2013-JUS (en adelante, Reglamento de la LPDP).
2. En el acta de fiscalización respectiva³, se dejó constancia de los siguiente:
 - Se realiza el tratamiento no automatizado de datos personales de los alumnos, los cuales son recopilados directamente del padre de familia mediante el formulario que llena en el proceso de admisión, "Documentos para la inscripción al proceso de admisión".
 - Se realiza tratamiento automatizado de los datos personales de los alumnos, los cuales son registrados mediante un formulario por la secretaria general en el "módulo del postulante" del sistema "SieWeb".
 - Se verificó que al realizar la matrícula, el padre de familia ingresa información adicional al mencionado sistema.

¹ Folios 380 al 396

² Folio 21

³ Folios 22 al 72

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

Resolución Directoral N° 2243-2022-JUS/DGTAIPD-DPDP

- En relación a lo establecido en el artículo 39, numeral 2, del Reglamento de la LPDP, se verificó la generación de registros de interacción lógica únicamente del inicio y cierre de sesión por medio del sistema “SieWeb”.
 - Respecto a lo dispuesto en el artículo 43° del Reglamento de la LPDP, se verificó que la administrada cuenta con equipos de generación de reproducción de documentos, sin embargo, estos equipos no cuentan con contraseña para su acceso, asimismo la asignación de equipos es realizada por área. Por otro lado, se verificó que el encargado del soporte del sistema es quien asigna los privilegios a los demás usuarios y que estos privilegios son solicitados de manera verbal.
3. En la misma acta de fiscalización, se solicitó a la administrada remitir los documentos de gestión de accesos, de privilegios y lo relativo a la verificación periódica de los privilegios, así como el sustento de las medidas de seguridad implementadas en el centro de datos, donde se encuentra ubicado el servidor de datos que almacena el banco de datos personales y que se evidencie la realización de copias de respaldo del banco de datos personales.
 4. Por medio del escrito ingresado con la Hoja de Trámite N° 86737-2019MSC del 09 de diciembre de 2019, la administrada se apersona y solicita una prórroga para presentar la documentación requerida⁴.
 5. Mediante la Hoja de Trámite N° 90295-2019MSC del 23 de diciembre de 2019, la administrada presenta la información requerida en el Acta de Fiscalización N° 01-2019; señalando como domicilio procesal Calle Bernardo Monteagudo N° 201, distrito de San Isidro, Lima⁵.
 6. Con el Oficio N° 002-2020-JUS/DGTAIPD-DFI del 02 de enero de 2020, el cual fue notificado el 10 de enero de 2020, se solicitó a la administrada presentar documentación que permita evidenciar la información específica sobre medidas de seguridad requerida en la mencionada Acta de Fiscalización N° 01-2019.
 7. El 17 de enero de 2020, la administrada presenta la información requerida por medio de la Hoja de Trámite N° 3450-2020MSC, respecto a lo señalado en el Oficio N° 002-2020⁶.
 8. Asimismo, el 19 de febrero de 2020, la administrada, por medio del documento con Hoja de Trámite N° 11366-2020MSC, presenta información en relación al Acta de Fiscalización N° 01-2019, adjuntando el documento “Contrato de licencia de uso de SieWeb”⁷, firmado con H&O System S.A.C. (en adelante, la encargada).
 9. El 27 de febrero de 2020, el Analista de Fiscalización en Seguridad de la Información de la DFI emite el Informe Técnico N° 59-2020-DFI-ORQR y sus anexos, sobre las medidas de seguridad implementadas por la administrada⁸.

⁴ Folios 73 al 78

⁵ Folios 79 al 278

⁶ Folios 290

⁷ Folios 288 al 293

⁸ Folios 294 al 305

Resolución Directoral N° 2243-2022-JUS/DGTAIPD-DPDP

10. Mediante el proveído del 31 de marzo de 2020, se dispuso ampliar el plazo de fiscalización al Colegio Parroquial Cristo Rey por 45 días hábiles adicionales, contados a partir del 02 de abril de 2020.
11. A través del Informe de Fiscalización N° 121-2020-JUS/DGTAIPD-DFI-PCFC del 23 de junio de 2020⁹, el Analista Legal de Fiscalización de la DFI, luego de evaluar los documentos presentados y las consideraciones expuestas, concluyó que se han determinado con carácter preliminar las circunstancias que justifican la instauración de un procedimiento administrativo sancionador, relativas al supuesto incumplimiento de las medias de seguridad requeridas por los artículos 39°, 42° y 43° del reglamento de la LPDP. Dicho informe fue notificado a la administrada mediante Oficio N.° 530-2020-JUS/DGTAIPD-DFI el 05 de agosto de 2020.
12. Con la Hoja de Trámite N° 2020USC-422658 del 02 de octubre de 2020¹⁰, la administrada presenta información en relación a lo reseñado en el informe de fiscalización.
13. Mediante el proveído del 16 de julio de 2021, se solicita al Analista de Fiscalización en Seguridad de la Información emitir un informe técnico respecto a las medidas de seguridad implementadas por la administrada, sobre la base de la documentación presentada.
14. A través del Informe Técnico N° 132-2021-DFI-ORQR del 26 de julio de 2021¹¹, el Analista de Fiscalización en Seguridad de la Información de la DFI, se pronuncia sobre las medidas de seguridad implementadas por la administrada:
 - Ha evidenciado contar con procedimientos documentados referentes a la verificación periódica de privilegios asignados. Por lo tanto, cumple con lo establecido en el numeral 1 del artículo 39° del Reglamento de la LPDP.
 - No ha evidenciado generar ni mantener registros de evidencias producto de la interacción lógica correspondientes a las acciones realizadas por los usuarios en su sistema "SieWeb", incumpliendo con lo establecido en el numeral 2 del artículo 39° del Reglamento de la LPDP.
 - Ha evidenciado de manera específica almacenar la documentación que conforma el banco de datos personales no automatizado de alumnos en ambientes que se encuentran debidamente protegidos y cuyos mecanismos de acceso se encuentran debidamente asignados a un personal responsable, cumpliendo con lo establecido en el artículo 42° del Reglamento de la LPDP.
 - No ha evidenciado implementar medidas de seguridad respecto al cumplimiento de lo dispuesto en el artículo 43° del Reglamento de la LPDP.
15. Por medio de la Resolución Directoral N° 186-2021-JUS/DGTAIPD-DFI del 7 de septiembre de 2021¹², la DFI resolvió iniciar procedimiento administrativo

⁹ Folios 307 al 316

¹⁰ Folios 307 al 316

¹¹ Folios 329 al 332

¹² Folios 333 al 344

Resolución Directoral N° 2243-2022-JUS/DGTAIPD-DPDP

sancionador a la administrada, debido a que no habría implementado las medidas de seguridad para el tratamiento de datos personales, al:

- No generar ni mantener registros de interacción lógica, según requiere el numeral 2 del artículo 39 del Reglamento de la LPDP.
- No restringir la generación de copias o reproducción de documentos que contienen datos personales. Obligación establecida en el artículo 43° del Reglamento de la LPDP.

Dichas situaciones configurarían la infracción leve tipificada en el literal a) del numeral 1 del artículo 132 de dicho reglamento: *“Realizar tratamiento de datos personales incumpliendo las medidas de seguridad establecidas en la norma sobre la materia.”*

16. A través de la Cédula de Notificación N° 707-2021-JUS/DGTAIPD-DFI se notificó a la administrada dicha resolución directoral, el 17 de septiembre de 2021¹³.
17. Por medio del escrito ingresado con la Hoja de Trámite N° 258416 del 12 de octubre de 2021¹⁴, la administrada presentó sus descargos, adjuntando documentación sustentatoria de sus argumentos.
18. A través del Informe Técnico N° 256-2021-DFI-ORQR del 2 de noviembre de 2021¹⁵, el Analista de Fiscalización en Seguridad de la Información de la DFI concluyó, acerca de los documentos sustentatorios de las medidas de seguridad de la administrada, lo siguiente:
 - No ha evidenciado generar ni mantener registros de evidencias producto de la interacción lógica correspondientes a las acciones relevantes realizadas por los usuarios en su sistema “SieWeb”, incumpliendo con lo dispuesto en el numeral 2 del artículo 39 del Reglamento de la LPDP.
 - No ha evidenciado implementar medidas de seguridad respecto al cumplimiento de lo dispuesto en el artículo 43° del Reglamento de la LPDP.
19. Mediante el Informe N° 150-2021-JUS/DGTAIPD-DFI, la DFI remitió a la Dirección de Protección de Datos Personales de la Dirección General de Transparencia, Acceso a la Información Pública y Protección de Datos Personales (en adelante, la DPDP) los actuados para que resuelva en primera instancia el procedimiento administrativo sancionador iniciado, recomendando a la administrada la multa ascendente a dos coma diecisiete unidades impositivas tributarias (2,17 UIT) por la comisión de la infracción grave tipificada en el literal a) del numeral 1 del artículo 132 del Reglamento de la LPDP.
20. Con la Resolución Directoral N° 258-2021-JUS/DGTAIPD-DFI del 23 de noviembre de 2021¹⁶, la DFI dio por concluidas las actuaciones instructivas correspondientes al procedimiento sancionador.

¹³ Folios 346 al 347

¹⁴ Folios 348 al 376

¹⁵ Folios 377 al 379

¹⁶ Folios 397 al 401

Resolución Directoral N° 2243-2022-JUS/DGTAIPD-DPDP

21. Dichos documentos fueron notificados a la administrada a través de la Cédula de Notificación N° 914-2021-JUS/DGTAIPD-DFI, el 29 de noviembre de 2021¹⁷.
22. Por medio del escrito ingresado el 09 de diciembre de 2021, con la Hoja de Trámite N° 2021USC-001814912¹⁸, la administrada presentó sus descargos respecto al Informe Final de Instrucción, solicitando el uso de la palabra en un informe oral, el cual se efectuó el 16 de febrero de 2022.
23. Mediante la Carta N° 323-2022-JUS/DGTAIPD-DPDP, notificada el 1 de febrero de 2022, se solicitó a la administrada remitir la documentación probatoria (video, captura de pantalla) respecto a la obtención de los registros de interacción lógica del sistema "SieWeb", generados respecto a las acciones relevantes efectuadas por los usuarios con perfil "Lectura y Escritura" con relación a lo señalado en el Informe Técnico N° 256-2021-DFI-ORQR.
24. Por medio del escrito ingresado con la Hoja de Trámite N° 48063-2022MSC, la administrada presenta información requerida en la Carta N° 323-2022-JUS/DGTAIPD-DPDP¹⁹.
25. A través del Informe Técnico N° 037-2022-DFI-ORQR del 31 de marzo de 2022²⁰, el Analista de Fiscalización en Seguridad de la Información de la DFI concluyó, acerca de la implementación de medidas de seguridad por parte de la administrada, que se evidencia de manera específica la generación de registros de interacción lógica correspondientes a las acciones relevantes realizadas por los usuarios del sistema "SieWeb", cumpliendo con la obligación establecida en el numeral 2 del artículo 39° del Reglamento de la LPDP.

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. Para la determinación de la responsabilidad de la administrada respecto de una infracción, se deberá tomar en cuenta lo establecido en el artículo 257 de la Ley N° 27444, Ley del Procedimiento Administrativo General, aprobado por Decreto Supremo N° 004-2019-JUS (en adelante, la LPAG), en su calidad de norma común

¹⁷ Folios 402 al 404

¹⁸ Folios 405 al 420

¹⁹ Folios 425 al 431

²⁰ Folios 436 al 438

Resolución Directoral N° 2243-2022-JUS/DGTAIPD-DPDP

para los procedimientos administrativos, conjuntamente con lo establecido en el Reglamento de la LPDP.

29. En tal sentido, se atiende al hecho de que el literal f) del numeral 1 de dicho artículo de la LPAG, establece como una causal eximente de la responsabilidad por infracciones, la subsanación del hecho imputado como infractor, si es realizada de forma previa a la notificación de imputación de cargos y a iniciativa voluntaria por parte de la administrada²¹, sin provenir del mandato de la autoridad a través de algún documento mediante el cual se solicite subsanar el acto calificable como infracción, como señala adecuadamente Morón²².
30. Por su parte, en lo que atañe a las atenuantes de la responsabilidad administrativa, se debe prestar atención a lo dispuesto en el numeral 2 del mismo artículo de la LPAG²³, en virtud del cual la aplicación de aquellas dependerá del reconocimiento expreso de la infracción, conjuntamente con los factores establecidos en la norma especial, el artículo 126 del Reglamento de la LPDP: El reconocimiento espontáneo, acompañado de acciones para su enmienda y colaboración con las acciones de la autoridad, factores que, de acuerdo con lo oportuno del reconocimiento y la efectividad de la enmienda, pueden conllevar la reducción motivada de la sanción hasta por debajo del rango previsto en la LPDP²⁴.
31. Por supuesto, la efectividad de los actos de enmienda mencionados, de acuerdo con el objetivo de las normas de protección de datos personales y del procedimiento administrativo, dependerá de su capacidad de diluir la trascendencia y los efectos antijurídicos de la conducta infractora, reparando la situación al punto de acercarla lo más posible al estado anterior al hecho infractor.

IV. Primera cuestión previa: Sobre la vinculación entre el Informe de Instrucción y el pronunciamiento de esta dirección

32. 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:

²¹ **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.

²² MORÓN URBINA, Juan Carlos: "Comentarios a la Ley del Procedimiento Administrativo General". Décimo quinta edición. Lima, Gaceta Jurídica, 2020, tomo II, p. 522.

²³ **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.

²⁴ **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.

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

Resolución Directoral N° 2243-2022-JUS/DGTAIPD-DPDP

“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.

(...)”

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

“Artículo 255.- Procedimiento sancionador

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

(...)

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

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

34. De los artículos transcritos, se desprende que la separación de las dos autoridades, así como la previsión de ejercicio de actuaciones por parte de la autoridad sancionadora o resolutora, situaciones que implican la autonomía de criterio de cada una de ellas.
35. En tal sentido, la autoridad sancionadora o resolutora puede hacer suyos todos los argumentos, conclusiones y recomendaciones expuestos por la autoridad instructora, así como puede efectuar una distinta evaluación de los hechos comprobados o inclusive, cuestionar estos hechos o evaluar situaciones que si bien fueron tomadas en cuenta al momento de efectuar la imputación, no se evaluaron de la misma manera al finalizar la instrucción.
36. Por tal motivo, la resolución que emita una autoridad sancionadora o resolutora, puede apartarse de las recomendaciones del informe final de instrucción o incluso cuestionar los hechos expuestos y su valoración, haciendo una evaluación diferente, teniendo en cuenta la su naturaleza no vinculante de dicho informe, y sin que ello conlleve una vulneración de la predictibilidad o de la expectativa legítima del administrado, la cual no encuentra asidero en la normativa referida al procedimiento administrativo.
37. Por supuesto, la divergencia de criterios mencionada, no puede implicar vulneraciones al debido procedimiento, como el impedir el derecho de defensa de

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

Resolución Directoral N° 2243-2022-JUS/DGTAIPD-DPDP

los administrados, ni ampliar o variar los hechos imputados y su valoración como presuntas infracciones.

V. Segunda cuestión previa: Acerca del interés que define la responsabilidad sobre el tratamiento de datos personales objeto de encargo y la exigencia de ejercer diligentemente el control sobre la encargada

38. Entre los partícipes en los procesos que involucran tratamiento de datos personales, se encuentra no solo el titular del banco de datos personales y/o el responsable de dicho tratamiento; se desarrollan actividades de tratamiento de datos personales que son parte de dichos procesos, a través de otras empresas o personas, o se emplean los datos personales que estas entidades ponen a su disposición, circunstancias que constituyen el encargo de tratamiento.

39. El artículo 2 de la LPDP contiene sus definiciones, transcritas a continuación:

“Artículo 2. Definiciones

Para todos los efectos de la presente Ley, se entiende por:

(...)

7. Encargado de tratamiento de datos personales. *Toda persona natural, persona jurídica de derecho privado o entidad pública que sola o actuando conjuntamente con otra realiza el tratamiento de los datos personales por encargo del titular del banco de datos personales en virtud de una relación jurídica que le vincula con el mismo y delimita el ámbito de su actuación. Incluye a quien realice el tratamiento sin la existencia de un banco de datos personales.*

8. Encargo de tratamiento. *Entrega por parte del titular del banco de datos personales a un encargado de tratamiento de datos personales en virtud de una relación jurídica que los vincula. Dicha relación jurídica delimita el ámbito de actuación del encargado de tratamiento de los datos personales.*

(...)

17. Titular del banco de datos personales. *Persona natural, persona jurídica de derecho privado o entidad pública que determina la finalidad y contenido del banco de datos personales, el tratamiento de estos y las medidas de seguridad.”*

40. Por su parte, el Reglamento de la LPDP, de forma complementaria, contiene las siguientes definiciones:

“Artículo 1.- Objeto.

El presente reglamento tiene por objeto desarrollar la Ley N° 29733, Ley de Protección de Datos Personales, en adelante la Ley, a fin de garantizar el derecho fundamental a la protección de datos personales, regulando un adecuado tratamiento, tanto por las entidades públicas, como por las instituciones pertenecientes al sector privado. Sus disposiciones constituyen normas de orden público y de cumplimiento obligatorio.

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

Resolución Directoral N° 2243-2022-JUS/DGTAIPD-PPDP

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:

(...)

10. Encargado del tratamiento: *Es quien realiza el tratamiento de los datos personales, pudiendo ser el propio titular del banco de datos personales o el encargado del banco de datos personales u otra persona por encargo del titular del banco de datos personales en virtud de una relación jurídica que le vincula con el mismo y delimita el ámbito de su actuación. Incluye a quien realice el tratamiento de datos personales por orden del responsable del tratamiento cuando este se realice sin la existencia de un banco de datos personales.*

(...)

14. Responsable del tratamiento: *Es aquél que decide sobre el tratamiento de datos personales, aun cuando no se encuentren en un banco de datos personales.*

15. Tercero: *Es toda persona natural, persona jurídica de derecho privado o entidad pública, distinta del titular de datos personales, del titular o encargado del banco de datos personales y del responsable del tratamiento, incluyendo a quienes tratan los datos bajo autoridad directa de aquellos.”*

41. De las normas citadas, se desprende que existe una pluralidad de niveles de participación en el tratamiento; teniendo como el concepto más amplio el del responsable del tratamiento, definido llanamente como quien “decide sobre el tratamiento de datos personales”, lo que a su vez incorpora el concepto de titular de los bancos de datos personales, que es una persona o entidad que decide sobre las actividades de tratamiento y la estructura, finalidad y preservación de la seguridad de los datos personales incorporados en un conjunto estructurado.
42. En ambos casos, está presente el poder de decisión que tienen sobre los datos personales, estructurados o no en un banco de datos personales, que se ejerce a través de la elección de los datos personales que serán objeto de tratamiento (en el caso de los bancos de datos personales, en su contenido y estructura), de las actividades de tratamiento de datos personales a realizar, de quiénes intervienen en tales actividades y, principalmente, de la finalidad a alcanzar, relacionada con el interés del responsable que se busca atender con dicho tratamiento.
43. En tal sentido, debe entenderse que dicho interés se satisface a través de medios (acciones, servicios, actividades de tratamiento, bienes empleados, entre otros), provistos o desarrollados por otras empresas, cuya contratación le resulta más provechosa que realizar la actividad encargada por su propia cuenta.
44. Sobre la finalidad y el correcto empleo de estos medios contratados, a fin de que sean compatibles con dicha finalidad, el responsable decide y ejerce el control supremo, y a la vez que goza de los beneficios que surta la actividad que conlleva el tratamiento de datos personales.

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

Resolución Directoral N° 2243-2022-JUS/DGTAIPD-DPDP

45. Al estar orientados hacia la satisfacción del responsable del tratamiento, tales medios se emplean en favor de este y su interés, siendo estos cualesquiera con los que desarrollen alguna actividad de tratamiento de datos personales, que pueden ser proporcionados por el mismo responsable al encargado para realizar la actividad del tratamiento, sin perjuicio de que este último realice otra actividad de tratamiento, como por ejemplo la recopilación de datos personales para la validación de identidad de los titulares.
46. Al atenderse en este proceso comercial el interés del responsable del tratamiento, surge la obligación a cargo de este, de garantizar un lícito y adecuado tratamiento de datos personales a lo largo de todo ese proceso, a fin de que la satisfacción de tal interés mantenga compatibilidad con el ordenamiento jurídico y con los derechos de las personas, los titulares de los datos personales.
47. Ello, aunado a su posición contractual, obliga al encargado a ceñir su desempeño a lo que establezca el responsable y a los resultados que este requiera, situación que conlleva dos labores que debe desarrollar el responsable:
 - Llevar a cabo con diligencia, las acciones de control necesarias para que el encargo se cumpla de acuerdo con lo pactado, en protección de sus intereses, sin efectos ilícitos en la prestación.
 - En lo relativo a evitar efectos ilícitos, la obligación de controlar y supervisar el cumplimiento de disposiciones legales y reglamentarias y/o evitar que algún daño ilícito se produzca como consecuencia de un desarrollo negligente de las actividades que satisfacen su interés, por parte del encargado.
48. El control ejercido sobre la actuación del encargado se traduce en la instrucción sobre los objetivos y modalidades de tratamiento, provisión de medios e información necesarios (como puede ser las modalidades de validación de identidad de clientes), así como en la implementación de medios para el ejercicio de los derechos de los titulares de los datos personales, para el contacto permanente entre el responsable y el encargado, y de otro lado, el requerimiento información u ordenar acciones específicas, sin que estas necesariamente se deriven de estipulaciones contractuales, sino del deber de control del responsable.
49. Asimismo, al estar obligado a ejercer dicho control, el responsable debe ser capaz de demostrar en cualquier momento que lo efectúa de manera efectiva; sea durante la vigencia del contrato de encargo, durante el período en el que se ejecutan las prestaciones respectivas, así como después de dicha vigencia y de haberse completado la mencionada ejecución, cuando haya efectos remanentes del tratamiento de datos personales objeto de encargo.
50. Entonces, cuando en un encargo de tratamiento se configure la comisión de una infracción y/o de cualquier hecho que implique un daño efectivo o potencial, debe tomarse en cuenta respecto de la responsabilidad, lo siguiente:
 - El principal obligado para preservar la licitud del tratamiento de los datos personales es el responsable de este, al ser necesario dicho tratamiento para

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

Resolución Directoral N° 2243-2022-JUS/DGTAIPD-DPDP

satisfacer su interés, por lo que debe ejercer diligentemente el control del mismo y demostrar haber ejercido dicho control en todo momento.

- En caso de que el responsable no haya ejercido diligentemente el control sobre el encargo de dicho tratamiento y/o no demuestre tal actuación, deberá responder por la infracción.
- Sin perjuicio de lo anterior, la responsabilidad del encargado por el incumplimiento o el tratamiento ilícito, coexistirá respecto de aquellas acciones que implican una conducta distinta a la que se estipuló para el encargo y a las instruidas por el responsable durante la prestación del servicio.
- En caso de que el responsable haya ejercido de forma diligente el control de las acciones de tratamiento de datos personales objeto de encargo y sustente adecuadamente el haber ejercitado dicho control, no le serán imputables los hechos ilícitos o dañosos.
- En ese mismo caso, al detectarse un hecho infractor que haya sobrepasado el diligente control del responsable, el encargado será responsable.

51. Ahora bien, la capacidad de ejercicio del control por parte del responsable del tratamiento de los datos personales, así como su demostración, no puede evaluarse de la misma manera para todas las empresas ni para todos los rubros o actividades del mercado; debiendo obedecerse a las particularidades que se presentan en cada caso concreto.
52. Así, la exigencia de control y demostración de su ejercicio, será alta cuando el encargo se vincule con una actividad de gran extensión en el mercado o en un numeroso público objetivo, como los casos de productos de consumo masivo o la prestación de servicios de salud, educación, telecomunicaciones o financieros, debiendo ser menor en los casos de actividades más reducidas.
53. Para determinar tal exigencia, también se evaluará tal factor en función a la mayor o menor especialización, la cercanía geográfica existente entre el encargado y el responsable, mayores o menores capacidades para aplicar la normativa de protección de datos personales, así como el posicionamiento y presencia del responsable en su mercado relevante.
54. De lo expuesto, se desprende que quien determina y controla las finalidades y modalidades de las actividades de tratamiento de datos personales, dirigidas a la satisfacción de su interés, es responsable por dicho tratamiento, debiendo ejercer el control sobre tales actividades encargadas de formar diligente y poder demostrar siempre tal ejercicio, asumiendo un rol proactivo para preservar los derechos de los titulares de los datos personales.
55. Por ello, conjuntamente con lo concerniente a la existencia de infracción, es necesario examinar factores como el interés de la administrada, así como el ejercicio del control sobre las actividades dirigidas a satisfacerlo, por parte de quien cumpla el rol de encargado.

VI. Cuestiones en discusión

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

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

Resolución Directoral N° 2243-2022-JUS/DGTAIPD-DPDP

- 56.1 Si la administrada es responsable por no haber implementado las medidas de seguridad para el tratamiento de datos personales, al:
- No generar ni mantener registros de interacción lógica.
 - No restringir la generación de copias o reproducción de documentos que contienen datos personales.
- 56.2 En el supuesto de resultar responsable, si debe aplicarse la exención de responsabilidad por la subsanación de la infracción, según lo previsto en el numeral 1 del artículo 257 de la LPAG, o las atenuantes, de acuerdo con lo dispuesto en el artículo 126 del reglamento de la LPDP, en consonancia con el numeral 2 del artículo 257 de la LPAG.
- 56.3 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.

VII. Análisis de las cuestiones en discusión

Sobre el presunto tratamiento de datos personales, sin aplicar las medidas de seguridad correspondientes

57. 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.”

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

“Artículo 16. Seguridad del tratamiento de datos personales

Para fines del tratamiento de datos personales, el titular del banco de datos personales debe adoptar medidas técnicas, organizativas y legales que garanticen su seguridad y eviten su alteración, pérdida, tratamiento o acceso no autorizado.

Los requisitos y condiciones que deben reunir los bancos de datos personales en materia de seguridad son establecidos por la Autoridad Nacional de Protección de Datos Personales, salvo la existencia de disposiciones especiales contenidas en otras leyes.

Queda prohibido el tratamiento de datos personales en bancos de datos que no reúnan los requisitos y las condiciones de seguridad a que se refiere este artículo.”

59. Este artículo, que desarrolla las principales acciones a realizar a fin de cumplir con el principio de Seguridad, establece dos tipos de objetivos de la adopción de

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

Resolución Directoral N° 2243-2022-JUS/DGTAIPD-DPDP

medidas técnicas, organizativas y legales de seguridad: El objetivo general, que es la garantía de la seguridad de los datos personales, y el objetivo específico, que es la adopción de medidas a través de las cuales se concreta tal garantía, dirigidas a evitar la alteración, pérdida, tratamiento o acceso no autorizado a la información custodiada.

60. El artículo 39 del Reglamento de la LPDP, en su numeral 2, establece lo siguiente:

“Artículo 39.- Seguridad para el tratamiento de la información digital.

Los sistemas informáticos que manejen bancos de datos personales deberán incluir en su funcionamiento:

(...)

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.”

61. El numeral 2 de dicho artículo establece la obligación a cargo de los responsables de tener registro de los pormenores de cada operación relevante de tratamiento de los datos personales, como la identidad de quién la efectuó, el momento en que se realizó y en qué consistió.
62. Durante la fiscalización, se verificó que la administrada contaba con el sistema “SlieWeb” para efectuar el tratamiento automatizado de los datos personales de sus alumnos, sobre los cuales, se señaló en el Informe Técnico N° 059-2020-DFI-ORQR que no generaban registros de interacción lógica con sus usuarios.
63. Dicha circunstancia se tomó como base el Informe de Fiscalización N° 121-2020-JUS/DGTAIPD-DFI-PCFC, así como para el primer extremo de esta imputación, efectuada por medio de la Resolución Directoral N° 186-2021-JUS/DGTAIPD-DFI.
64. Mediante la Hoja de Tramite N° 000258416 ingresada el 12 de octubre de 2021, la administrada presenta sus descargos en relación a lo resuelto por medio de la Resolución Directoral N° 186-2021-JUS/DGTAIPD-DFI, señalando que ha facilitado a la DFI los niveles de acceso por perfil en el sistema “SieWeb”, evidenciando así que la interacción lógica de los datos está determinada por los niveles de acceso por perfil de manera que estarían demostrando tener debidamente monitoreado y documentado lo ya mencionado, cuestión que la DFI no ha valorado adecuadamente.

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

Resolución Directoral N° 2243-2022-JUS/DGTAIPD-DPDP

65. Asimismo, la administrada en su escrito adjuntó una carta remitida por la encargada²⁵, para dejar constancia en relación a sus sistemas de seguridad lo siguiente:

(...)

- El acceso a Los Servidores donde se aloja la base de datos solo es permitido a 2 personas dentro de la organización;*
- Todo respaldo (backup) de información este encriptado con clave solo conocida por las H & O SYSTEM que tienen acceso a los servidores. Si bien el Cliente debe mantener Backup ellos están encriptados y con clave.*
- **SieWeb mantiene una auditoría de todas las altas, bajas y cambios que se realiza en la base de datos.***
- SieWeb mantiene una auditoría de todos los accesos que se sistema.*

(...)

66. La aclaración realizada guarda concordancia con la cláusula décimo cuarta del contrato firmado por la administrada y la encargada, en la que se especificó que esta última es responsable de la aplicación de medidas técnicas, organizativas y legales para preservar la integridad, confidencialidad y disponibilidad de los datos personales que reciba de la administrada²⁶.
67. Dicha circunstancia aclara las características del servicio que brinda la encargada, que al ser titular del sistema "SieWeb" se encuentra en mejor posición para controlar los registros de interacciones con los datos lógicos que se dan en el marco de tal sistema; situación que se configuró durante todo el tiempo de vigencia del vínculo contractual.
68. Posteriormente, la administrada presenta un video explicativo acerca de la generación de tales registros de interacción lógica, el cual se encuentra dividido en 3 partes.
69. A través del Informe Técnico N° 037-2022-DFI-ORQR del 31 de marzo de 2022²⁷, el Analista de Fiscalización en Seguridad de la Información de la DFI, se pronuncia sobre tales videos concluyendo que se ha evidenciado de manera específica que genera y mantiene registros de evidencias producto de la interacción lógica correspondientes a las acciones relevantes realizadas por los usuarios del sistema "SieWeb", por lo cual la administrada cumple con la obligación establecida en el numeral 2 del artículo 39° del Reglamento de la LPDP.
70. Entonces, se logra corroborar que la administrada habría cumplido con la obligación establecida en el numeral 2 del artículo 39° del Reglamento de la LPDP antes de la imputación de cargos, al verificarse cuan concernida estaba la administrada respecto del control de los registros de interacción llevados sobre el mencionado sistema, cuyo encargo y límites está contractualmente previsto.

²⁵ Folio 373

²⁶ Folio 52

²⁷ Folios 329 al 332

Resolución Directoral N° 2243-2022-JUS/DGTAIPD-DPDP

71. Por tal motivo, la presente imputación debe declararse infundada, conforme a lo expuesto en los considerandos anteriores.
72. Por su parte, el artículo 43 del Reglamento de la LPDP, establece lo siguiente:

“Artículo 43.- Copia o reproducción.
La generación de copias o la reproducción de los documentos únicamente podrán ser realizadas bajo el control del personal autorizado. Deberá procederse a la destrucción de las copias o reproducciones desechadas de forma que se evite el acceso a la información contenida en las mismas o su recuperación posterior.”
73. El párrafo reglamentario transcrito establece la obligación a cargo de los responsables de controlar la generación de copias o la reproducción de documentos, a fin de evitar acceso no autorizado y preservar la confidencialidad de la información que pueda contenerse.
74. Durante la fiscalización, se verificó que la administrada contaba con equipos de reproducción de documentos (multifuncionales) y que para acceder a dichos equipos no se requería contraseña, ni se encontraban debidamente asignados al personal.
75. Por otro lado, se revisó las medidas de seguridad de la computadora asignada al encargado de soporte del sistema, en la que se realiza el tratamiento de datos personales de los alumnos, constatando que contaba con los puestos USB y grabador de disco habilitados, con acceso a cuentas de correo personal y servicio de internet sin restricciones, lo cual generaría un riesgo de fuga de la información, sobre lo cual, se señaló en el Informe Técnico N° 059-2020-DFI-ORQR que no cumplía con la obligación señalada en el artículo 43° del Reglamento de la LPDP.
76. Dicha circunstancia se tomó como base en el Informe de Fiscalización N° 121-2020-JUS/DGTAIPD-DFI-PCFC, sirviendo de fundamento para este extremo de la imputación, efectuada por medio de la Resolución Directoral N° 186-2021-JUS/DGTAIPD-DFI.
77. En sus descargos, la administrada presentó el documento “Declaración de compromiso de confidencialidad”, el cual señala la obligación de confidencialidad con sus trabajadores, precisando la prohibición de obtención de copias, ya sean físicas, electrónicas, graficas, fotográficas, en video o en cualquier formato, sin previa autorización expresa y por escrito.
78. Si bien en el presente caso, la DFI opinó que para evidenciar el cumplimiento de la obligación la administrada debió adjuntar fotografías, capturas de pantalla y/o videos en los que pueda constatar la implementación de medidas de seguridad y/o controles adoptados para restringir la copia o reproducción de documentos, es necesario considerar que al contar con el documento mencionado, en el que de forma expresa se establece la prohibición de la obtención de copias de documentos sin previa autorización expresa y por escrito, este Despacho considera que tal situación no se enmarca en el supuesto establecido por el citado artículo 43 del Reglamento de la LPDP.

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

Resolución Directoral N° 2243-2022-JUS/DGTAIPD-DPDP

79. Cabe mencionar que, si bien no se ha evidenciado por medio de capturas de pantallas y/o videos la implementación de tales medidas restrictivas, tampoco se tienen elementos probatorios de que se hayan realizado efectivamente copias sin autorización, siendo esta última conducta la que regula el artículo 43 del Reglamento de la LPDP.
80. En efecto, de lo recopilado durante la visita de fiscalización, solo se desprende que el equipo del responsable del soporte de sistema tiene habilitados los dispositivos de escritura de archivos y de envío de mensajes a través de internet, mas (lo cual es consignado en el acta de fiscalización), no se tienen pruebas de la concreta obtención de tales copias.
81. En consecuencia, este Despacho considera que este extremo de la imputación debe ser desestimado, correspondiendo que se declare infundada la misma.

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

SE RESUELVE:

Artículo 1.- Declarar Infundada la imputación a Colegio Parroquial Cristo Rey respecto no haber cumplido con implementar las medidas de seguridad para el tratamiento de datos personales, respecto a la obligación en el numeral 2 del artículo 39 del Reglamento de la LPDP; infracción leve contemplada en el literal a) del inciso 1 del artículo 132 del Reglamento de la LPDP: *"Realizar tratamiento de datos personales incumpliendo las medidas de seguridad establecidas en la normatividad sobre la materia"*.

Artículo 2.- Declarar Infundada la imputación a Colegio Parroquial Cristo Rey respecto no haber cumplido con implementar las medidas de seguridad para el tratamiento de datos personales, respecto a la obligación establecida en el artículo 43 del Reglamento de la LPDP; infracción leve contemplada en el literal a) del inciso 1 del artículo 132 del Reglamento de la LPDP: *"Realizar tratamiento de datos personales incumpliendo las medidas de seguridad establecidas en la normatividad sobre la materia"*.

Artículo 3.- Informar a Colegio Parroquial Cristo Rey 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 notificación²⁸.

²⁸ **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.

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

Resolución Directoral N° 2243-2022-JUS/DGTAIPD-DPDP

Artículo 4.- Notificar a Colegio Parroquial Cristo Rey la presente resolución directoral, a su domicilio procesal electrónico, correo electrónico datospersonales.esola@esola.com.pe

Regístrese y comuníquese.

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

MAGL/rvr/ggg

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