REPÚBLICA DEL PERÚ

Resolución Directoral

Resolución Directoral N° 999-2018-JUS/DGTAIPD-DPDP

Expediente N°
067-2017-JUS/DPDP-PS

Resolución N° 999-2018-JUS/DGTAIPD-DPDP

Lima, 22 de mayo de 2018

VISTOS:

El Informe Nº 092-2016-JUS/DGPDP-DSC[1] del 28 de diciembre de 2016 (Expediente de Fiscalización Nº 048-2015-DSC), emitido por la Dirección de Supervisión y Control de la Dirección General de Protección de Datos Personales, y demás documentos que obran en el respectivo expediente, y;

CONSIDERANDO:

PERÚ | Ministerio de Justicia y Derechos Humanos
Dirección de Protección de Datos Personales
M. GONZALEZ L.

I. Antecedentes

1. Mediante Orden de Visita de Fiscalización Nº 046-2016-JUS/DGPDP-DSC[2], de fecha 22 de agosto de 2016, la Dirección de Supervisión y Control de la Dirección General de Protección de Datos Personales (en adelante, DSC) dispuso la realización de una visita de fiscalización a COLEGIO PARTICULAR SAN VICENTE (en adelante, la administrada).

2. Mediante Acta de Fiscalización N° 01-2016[3], se deja constancia de los hallazgos encontrados durante la visita de supervisión realizada a las instalaciones de la administrada el día 24 de agosto de 2016, en su domicilio ubicado en Av. Los Maestros N° 250, Región Ica, Provincia de Ica, Distrito de Ica, fecha en la cual se adjuntó documentación[4] adicional a efectos de su evaluación por parte del personal supervisor.

[1] Folio 76 a 80
[2] Folio 07
[3] Folio 15 a 21
[4] Folio 22 a 50

3. Mediante Oficio N° 233-2016-JUS/DGPDP-DSC[5] de fecha 06 de setiembre de 2016, se requirió a la administrada la presentación de información complementaria para la realización de la supervisión.

4. Mediante escrito[6] presentado con hoja de trámite N° 55388-2016MSC el 19 de setiembre, la administrada presentó la documentación complementaria requerida.

5. Mediante Informe N° 044-2016-DSC-ORQR[7] de fecha 04 de noviembre de 2016, el personal técnico de la DSC emitió el informe de supervisión a la administrada.

6. Mediante Informe N° 092-2016-JUS/DGPDP-DSC[8] de fecha 28 de diciembre de 2016, se emitió el informe sobre el procedimiento de fiscalización a la administrada, remitiendo a la Dirección de Sanciones de la Dirección General de Protección de Datos Personales el resultado de la fiscalización realizada, adjuntando el acta de fiscalización así como los demás anexos y documentos que conforman el respectivo expediente administrativo; dicho informe fue notificado con Oficio N° 369-2016-JUS/DGPDP-DSC[9] el 03 de enero de 2017.

7. Mediante Resolución Directoral N° 028-2017-JUS/DGTAIPD-DFI[10] de fecha 20 de julio de 2017, la Dirección de Fiscalización e Instrucción de la Dirección General de Transparencia, Acceso a la Información Pública y Protección de Datos Personales, en adelante DFI, resolvió iniciar procedimiento administrativo sancionador a la administrada, por las siguientes infracciones:

   (i) Habría Incumplido el deber de información establecido en el artículo 18 de la Ley N° 29733, Ley de Protección de Datos Personales (en adelante, LPDP), ya que al recopilar datos de sus alumnos no habría informado que realiza flujo transfronterizo de datos; configurándose la Infracción grave tipificada en el literal a. del numeral 2 del artículo 38 de la consistente en: "*Dar tratamiento a los datos personales contraviniendo los principios establecidos en la presente Ley o incumpliendo sus demás disposiciones o las de su Reglamento*".

   (ii) Habría incumplido lo dispuesto por los artículos 26 y 77 del Reglamento del Decreto Supremo N° 003-2013-JUS, (en adelante, Reglamento de la LPDP), ya que no habría comunicado al Registro Nacional de Protección de Datos Personales, la realización de flujo transfronterizo; configurándose la Infracción grave tipificada en el literal a. del numeral 2 del artículo 38 de la consistente en: "*Dar tratamiento a los datos personales contraviniendo los principios establecidos en la presente Ley o incumpliendo sus demás disposiciones o las de su Reglamento*".

   (iii) Habría incumplido lo dispuesto por el artículo 9 de la LPDP, el numeral 1 del artículo 39 y por el artículo 43 del Reglamento de la LPDP, ya que no habría implementado las medidas de seguridad de documentar los procedimientos de gestión de accesos y gestión de privilegios de los usuarios del sistema, y no implementar controles de seguridad para la restricción de copias de datos, pues contaba con puertos USB y el grabador DVD habilitados, lo que permite la visualización y grabación de archivos; configurándose la Infracción grave tipificada

Ministerio de Justicia y Derechos Humanos PERÚ
Dirección de Protección de Datos Personales
GONZALEZ L.

[5] Folio 52
[6] Folio 53 a 62
[7] Folio 64 a 67
[8] Folio 76 a 80
[9] Folio 82
[10] Folio 83 a 88

en el literal a. del numeral 2 del artículo 38 de la LPDP consistente en: "*Dar tratamiento a los datos personales contraviniendo los principios establecidos en la presente Ley o incumpliendo sus demás disposiciones o las de su Reglamento*".

8. Mediante Oficio N° 105-2017-JUS/DGTAIPD-DFI[11] recibido por la administrada el 15 de setiembre de 2017, se le notificó la Resolución Directoral N° 028-2017-JUS/DGTAIPD-DFI que inicia el procedimiento administrativo sancionador.

9. Mediante escrito presentado con hoja de trámite 59733-2017MSC[12] el 04 de octubre de 2017, la administrada presentó sus descargos.

10. Mediante Informe N° 044-2017-DFI-VARS[13] de fecha 10 de noviembre de 2017, personal técnico de la Dirección de Fiscalización e Instrucción, emitió un informe de evaluación de implementación de las medidas de seguridad de la administrada.

PERÚ | Ministerio de Justicia y Derechos Humanos
Dirección de Protección de Datos Personales
M. GONZALEZ I

11. Mediante Proveído N° 019[14] (Expediente N° 051-2016-JUS/DGTAIPD-PS) de fecha 21 de noviembre de 2017, la DFI resolvió ampliar el plazo de la etapa instructiva por treinta (30) días hábiles adicionales; notificándose a la administrada con Oficio N° 178-2017-JUS/DGTAIPD-DFI[15], el 28 de noviembre de 2017.

12. Mediante Resolución Directoral N°085-2017-JUS/DGTAIPD-DFI[16] de fecha 29 de diciembre de 2017, la DFI dio por concluidas las actuaciones instructivas correspondientes al procedimiento sancionador. Dicha resolución fue notificada a la administrada el 15 de enero de 2018, a través del Oficio N° 308-2017-JUS/DGTAIPD-DFI[17].

13. Mediante Informe N° 056-2017-JUS/DGTAIPD-DFI[18] de fecha 29 de diciembre de 2017, la Dirección de Fiscalización e Instrucción emitió el Informe Final de Instrucción, remitiendo a la Dirección de Protección de Datos Personales los

[11] Folio 89
[12] Folio 90 a 107
[13] Folio 108
[14] Folio 109
[15] Folio 110 a 112
[16] Folio 113 a 114
[17] Folio 117
[18] Folio 118 a 126

actuados para que resuelva en primera instancia el procedimiento administrativo sancionador iniciado, recomendando lo siguiente:

1) Se recomienda imponer sanción administrativa de multa ascendente a una (1) UIT al Colegio Particular San Vicente, por el cargo acotado en el hecho imputado N° 01, por infracción tipificada en el literal f, numeral 1, artículo 132° del RLPDP: *"Dar tratamiento a los datos personales contraviniendo las disposiciones de la Ley y su Reglamento".*

2) Se recomienda imponer sanción administrativa de multa ascendente a una (1) UIT al Colegio Particular San Vicente, por el cargo acotado en el hecho imputado N° 02, por infracción tipificada en el literal f, numeral 1, artículo 132° del RLPDP: *"Dar tratamiento a los datos personales contraviniendo las disposiciones de la Ley y su Reglamento".*

3) Se recomienda imponer sanción administrativa de multa ascendente a dos (2) UIT al Colegio Particular San Vicente, por el cargo acotado en el hecho imputado N° 03, por infracción tipificada en el literal f, numeral 1, artículo 132° del RLPDP: *"Dar tratamiento a los datos personales contraviniendo las disposiciones de la Ley y su Reglamento".*

II. Competencia

14. Mediante Decreto Supremo N° 013-2017-JUS de fecha 21 de junio de 2017, se aprobó el Reglamento de Organización y Funciones del Ministerio de Justicia y Derechos Humanos (en adelante, ROF del MINJUS), derogando el Decreto Supremo N° 011-2012-JUS.

15. El artículo 70 del ROF del MINJUS crea la Dirección General de Transparencia, Acceso a la Información Pública y Protección de Datos Personales como órgano de línea encargado de ejercer la Autoridad Nacional de Protección de Datos Personales, para el cumplimiento de sus funciones fiscalizadoras y sancionadoras en materia de protección de datos personales.

PERÚ Ministerio de Justicia y Derechos Humanos
Dirección de Protección de Datos Personales
M. GONZALEZ L.

16. Conforme a lo dispuesto en el artículo 74 del ROF del MINJUS, la Dirección de Protección de Datos Personales es la unidad orgánica competente para resolver en primera instancia, los procedimientos administrativos sancionadores iniciados por la Dirección de Fiscalización e Instrucción.

17. Sin embargo, mediante Resolución Directoral N° 43-2017-JUS/DGTAIPD, se designó a la señora Anais Caridad Zavala Huaisara, Directora (e) de Transparencia y Acceso a la Información Pública, como autoridad administrativa que resolverá el procedimiento sancionador iniciado a COLEGIO PARTICULAR SAN VICENTE, debido a que se aceptó la abstención presentada por la Directora de Protección de Datos Personales.

18. Dado que la encargatura de la Dirección de Transparencia y Acceso a la Información Pública a la señora Anais Caridad Zavala Huaisara culminó el 03 de abril del presente; mediante Resolución Directoral N° 74-2018-JUS/DGTAIPD, se dejó sin efecto la abstención aceptada para resolver el procedimiento sancionador iniciado a COLEGIO PARTICULAR SAN VICENTE, señalando que la autoridad administrativa que resolverá el mencionado procedimiento sancionador será la Directora de Protección de Datos Personales.

19. En tal sentido, en ejercicio de sus facultades y conforme a sus competencias, corresponde a la Dirección de Protección de Datos Personales de la Dirección General de Transparencia, Acceso a la Información Pública y Protección de Datos Personales determinar si se ha cometido infracción a la LPDP y a su Reglamento.

III. Normativa sancionadora aplicable

20. En ejercicio de sus facultades, corresponde a la Dirección de Protección de Datos Personales de la Dirección General de Transparencia, Acceso a la Información Pública y Protección de Datos Personales determinar si se ha cometido infracción a la LPDP y a su reglamento.

21. Mediante el Decreto Supremo N° 019-2017-JUS de fecha 15 de setiembre de 2017, se aprobó el reglamento del Decreto Legislativo N° 1353 que crea la Autoridad Nacional de Transparencia y Acceso a la Información Pública, fortalece el Régimen de Protección de Datos Personales y la regulación de la gestión de intereses (en adelante, Decreto Legislativo N° 1353).

PERÚ Ministerio de Justicia y Derechos Humanos
Dirección de Protección de Datos Personales
M. GONZALEZ I

22. La Tercera Disposición Complementaria Modificatoria del mencionado reglamento incorpora el capítulo de infracciones al Título VI del Reglamento de la LPDP, agregando el artículo 132 que tipifica las infracciones.

23. Por su parte, el presente procedimiento sancionador se inició estando vigente el artículo 38 de la LPDP que en el numeral 2 literal a. estableció como infracción grave: "*Dar tratamiento a los datos personales contraviniendo los principios establecidos en la presente Ley o incumpliendo sus demás disposiciones o las de su Reglamento*".

24. Entonces, el sistema jurídico ha permitido una excepción en torno al principio de irretroactividad[19] en materia penal y administrativo sancionador, conocido como la retroactividad benigna.

[19] **Texto Único Ordenado de la Ley N° 27444, Ley del Procedimiento Administrativo General, aprobado por Decreto Supremo N° 006-2017-JUS.**
"Artículo 246.- Principios de la potestad sancionadora administrativa
La potestad sancionadora de todas las entidades está regida adicionalmente por los siguientes principios especiales:
(...)

25. La retroactividad benigna se hace efectiva si luego de la comisión de un ilícito administrativo, se produce una modificación normativa y dicha norma establece una consecuencia más beneficiosa para el infractor, ya sea la eliminación del tipo infractor o el establecimiento de una sanción menor, en comparación con la norma anterior (vigente al momento que se cometió la infracción), por lo que debe aplicarse retroactivamente la nueva norma. Cabe señalar que, la retroactividad debe ser el resultado de una evaluación integral por parte de la Administración y como tal debe verificarse los supuestos y requisitos que la norma exija de manera que produzca consecuencias jurídicas favorables para el administrado.

26. En este sentido, el artículo 2 del Decreto Legislativo N° 1272 modificó el principio de irretroactividad recogido en el TUO de la LPAG, en el cual se precisó los supuestos sobre los cuales se podría aplicar la excepción, siendo los siguientes:

    - Tipificación de la infracción más favorable
    - Previsión de la sanción más favorable, incluso de aquellas que se encuentran en etapa de ejecución.
    - Plazos de prescripción más favorables.

27. En la línea de lo expuesto, apreciándose que los supuestos de hechos (incumplimiento de la obligación) en los cuales habría incurrido la administrada ha variado de tipificación y de sanción (al momento en que se detectó la infracción); en atención a la excepción (retroactividad benigna) establecida en el principio de irretroactividad que rige la potestad sancionadora administrativa, se aplicará la disposición que resulte más favorable al administrado.

28. Sobre la obligación de informar el tratamiento de los datos personales a su titular, entre ellos la realización de flujo transfronterizo de datos personales:

PERÚ Ministerio de Justicia y Derechos Humanos
Dirección de Protección de Datos Personales
GONZALEZ I

Norma	Regulación anterior	Regulación actual
Sustantiva	Obligación regulada en el artículo 18 de la Ley de Protección de Datos Personales, Ley N° 29733 (LPDP).	Obligación regulada en el artículo 18 de la Ley de Protección de Datos Personales, Ley N° 29733 (LPDP).
Tipificadora	Literal a. del numeral 2 del artículo 38 de la LPDP, esto es: "*Dar tratamiento a los datos personales contraviniendo los principios establecidos en la presente Ley o incumpliendo sus demás disposiciones o las de su Reglamento*".	*Literal f. del numeral 1 del artículo 132 del Reglamento de la LPDP, esto es: "Dar tratamiento a los datos personales contraviniendo las disposiciones de la Ley y su Reglamento".*

5.- Irretroactividad.- *Son aplicables las disposiciones sancionadoras vigentes en el momento de incurrir el administrado en la conducta a sancionar, salvo que las posteriores le sean más favorables.*
Las disposiciones sancionadoras producen efecto retroactivo en cuanto favorecen al presunto infractor o al infractor, tanto en lo referido a la tipificación de la infracción como a la sanción y a sus plazos de prescripción, incluso respecto de las sanciones en ejecución al entrar en vigor la nueva disposición. (El subrayado es nuestro)
(...)"

Eventual sanción	Numeral 2 del artículo 39 de la LPDP que establece la infracción **grave** sancionada con más de 5 a 50 UIT.	Numeral 1 del artículo 39 de la LPDP que establece la infracción **leve** sancionada con más de 0,5 UIT hasta 5 UIT.

29. En atención a lo anterior, se evidencia que el marco normativo actual (norma que entró en vigencia el 16 de setiembre de 2017) es más favorable para la administrada en comparación con la norma anterior a la fecha en la que se cometió la infracción (24 de agosto de 2016), toda vez que actualmente la sanción conforme a la tipificación resulta más beneficiosa al haber cambiado de grave a leve.

    En ese sentido, en virtud de la excepción al principio de irretroactividad (retroactividad benigna) establecido en el artículo 246 del TUO de la LPAG[20], corresponde aplicar la tipificación más favorable a la administrada, esto es el literal f. del numeral 1 del artículo 132 del Reglamento de la LPDP: *"Dar tratamiento a los datos personales contraviniendo las disposiciones de la Ley y su Reglamento"*; al presunto incumplimiento de la disposición legal del artículo 18 de la LPDP, al no informar sobre el tratamiento que se realizará sobre los datos personales a su titular, entre ellos, no comunicar el flujo transfronterizo.

30. Sobre la obligación de comunicar la realización de flujo transfronterizo a la Autoridad de Protección de Datos Personales:

PERÚ Ministerio de Justicia y Derechos Humanos
Dirección de Protección de Datos Personales
GONZALEZ L

[20] **Texto Único Ordenado de la Ley N° 27444, Ley del Procedimiento Administrativo General, aprobado por Decreto Supremo N° 006-2017-JUS.**
"Artículo 246.- Principios de la potestad sancionadora administrativa
La potestad sancionadora de todas las entidades está regida adicionalmente por los siguientes principios especiales:
(...)
5.- Irretroactividad.-*Son aplicables las disposiciones sancionadoras vigentes en el momento de incurrir el administrado en la conducta a sancionar, salvo que las posteriores le sean más favorables.*
Las disposiciones sancionadoras producen efecto retroactivo en cuanto favorecen al presunto infractor o al infractor, tanto en lo referido a la tipificación de la infracción como a la sanción y a sus plazos de prescripción, incluso respecto de las sanciones en ejecución al entrar en vigor la nueva disposición.
(...)"

Norma	Regulación anterior	Regulación actual
Sustantiva	Obligación regulada en el artículo 26 y 77 del Reglamento de la LPDP.	Obligación regulada en el numeral 2 del artículo 34 de la LPDP, en concordancia con el artículo 26 y 77 del Reglamento de la LPDP.
Tipificadora	Literal a. del numeral 2 del artículo 38 de la LPDP, esto es: "*Dar tratamiento a los datos personales contraviniendo los principios establecidos en la presente Ley o incumpliendo sus demás disposiciones o las de su Reglamento*"	Literal e. del numeral 1 del artículo 132 del Reglamento de la LPDP, esto es: "*No inscribir o actualizar en el Registro Nacional los actos establecidos en el artículo 34 de la Ley*".
Eventual sanción	Numeral 2 del artículo 39 de la LPDP que establece la infracción **grave** sancionada con más de 5 a 50 UIT.	Numeral 1 del artículo 39 de la LPDP que establece la infracción **leve** sancionada con 0,5 UIT hasta 5 UIT.

31. En atención a lo anterior, cabe señalar que el incumplimiento de la obligación de implementar medidas de seguridad en la actual regulación de infracciones, se subsume en una tipificación específica que comprende dicho hecho infractor, por lo que corresponde aplicar dicha tipificación.

    Asimismo, en atención a lo anterior, se evidencia que el marco normativo actual (norma que entró en vigencia el 16 de setiembre de 2017) es más favorable para la administrada en comparación con la norma anterior a la fecha en la que se cometió la infracción (24 de agosto de 2016), toda vez que actualmente la sanción conforme a la tipificación resulta más beneficiosa al haber cambiado de grave a leve.

    En ese sentido, en virtud de la excepción al principio de irretroactividad (retroactividad benigna) establecido en el artículo 246 del TUO de la LPAG[21], corresponde aplicar la tipificación más favorable a la administrada, esto es el literal e. del numeral 1 del artículo 132 del Reglamento de la LPDP: *"No inscribir o actualizar en el Registro Nacional los actos establecidos en el artículo 34 de la Ley"*; al presunto incumplimiento de las disposiciones de los artículos 26 y 77 del Reglamento de la LPDP; al no haber presuntamente comunicado/inscrito la realización de flujo transfronterizo.

PERÚ Ministerio de Justicia y Derechos Humanos
Dirección de Protección de Datos Personales
M. GONZALEZ L

[21] **Texto Único Ordenado de la Ley N° 27444, Ley del Procedimiento Administrativo General, aprobado por Decreto Supremo N° 006-2017-JUS.**
"Artículo 246.- Principios de la potestad sancionadora administrativa
La potestad sancionadora de todas las entidades está regida adicionalmente por los siguientes principios especiales:
(...)
5.- Irretroactividad.-*Son aplicables las disposiciones sancionadoras vigentes en el momento de incurrir el administrado en la conducta a sancionar, salvo que las posteriores le sean más favorables.*
Las disposiciones sancionadoras producen efecto retroactivo en cuanto favorecen al presunto infractor o al infractor, tanto en lo referido a la tipificación de la infracción como a la sanción y a sus plazos de prescripción, incluso respecto de las sanciones en ejecución al entrar en vigor la nueva disposición.
(...)"

32. Sobre la obligación de implementar medidas de seguridad de la información, entre ellas, el deber de documentar sus procedimientos de gestión de accesos y gestión de privilegios y mantener controles en los puertos USB y reproductor de DVD, para evitar copias y reproducciones de la información por parte de personas no autorizadas:

Norma	Regulación anterior	Regulación actual
Sustantiva	Obligación regulada en el numeral 1 del artículo 39 y en el artículo 43 del Reglamento de la LPDP, aprobado mediante Decreto Supremo N° 003-2013-JUS, en concordancia con el artículo 9 de la LPDP.	Obligación regulada en el numeral 1 del artículo 39 y en el artículo 43 del Reglamento de la LPDP, aprobado mediante Decreto Supremo N° 003-2013-JUS, en concordancia con el artículo 9 de la LPDP.
Tipificadora	Literal a. del numeral 2 del artículo 38 de la LPDP, esto es: "*Dar tratamiento a los datos personales contraviniendo los principios establecidos en la presente Ley o incumpliendo sus demás disposiciones o las de su Reglamento*"	Literal a. del numeral 1 del artículo 132 del Reglamento de la LPDP, esto es: "*Realizar tratamiento de datos personales incumpliendo las medidas de seguridad establecidas en la normativa sobre la materia*".
Eventual sanción	Numeral 2 del artículo 39 de la LPDP que establece la infracción **grave** sancionada con más de 5 a 50 UIT.	Numeral 1 del artículo 39 de la LPDP que establece la infracción **leve** sancionada con 0,5 UIT hasta 5 UIT.

PERÚ Ministerio de Justicia y Derechos Humanos
Dirección de Protección de Datos Personales
M. GONZALEZ L

33. En atención a lo anterior, cabe señalar que el incumplimiento de la obligación de implementar medidas de seguridad en la actual regulación de infracciones, se subsume en una tipificación específica que comprende dicho hecho infractor, por lo que corresponde aplicar dicha tipificación.

Asimismo, se evidencia que el marco normativo actual (norma que entró en vigencia el 16 de setiembre de 2017) es más favorable para la administrada en comparación con la norma anterior a la fecha en la que se cometió la infracción (24 de agosto de 2016), toda vez que actualmente la sanción conforme a la tipificación resulta más beneficiosa al haber cambiado de grave a leve.

En ese sentido, en virtud de la excepción al principio de irretroactividad (retroactividad benigna) establecido en el artículo 246 del TUO de la LPAG[22], corresponde aplicar la tipificación más favorable a la administrada, esto es el literal a. del numeral 1 del artículo 132 del Reglamento de la LPDP: "*Realizar tratamiento de datos personales incumpliendo las medidas de seguridad establecidas en la normativa sobre la materia*"; al presunto incumplimiento de las disposiciones de los artículos 39 y 43 del Reglamento de la LPDP; al no haber documentado sus procedimientos de gestión de accesos y gestión de privilegios y no mantener controles en los puertos USB y reproductor de DVD, para evitar copias y reproducciones de la información por parte de personas no autorizadas.

34. De otro lado, acerca de la responsabilidad de la administrada, se debe tener en cuenta que el literal f) del numeral 1 del artículo 255[23] del Texto Único Ordenado de la Ley del Procedimiento Administrativo General, aprobado mediante Decreto Supremo N° 006-2017-JUS (en adelante, LPAG), establece como una causal eximente de la responsabilidad por infracciones, la subsanación voluntaria del acto imputado como infractor, si es realizada de forma previa a la notificación de imputación de cargos.

35. Asimismo, se debe atender a lo dispuesto en el artículo 126[24] 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 puede permitir la reducción motivada de la sanción por debajo del rango previsto en la LPDP.

PERÚ Ministerio de Justicia y Derechos Humanos
Dirección de Protección de Datos Personales
M. GONZALEZ L

[22] **Texto Único Ordenado de la Ley N° 27444, Ley del Procedimiento Administrativo General, aprobado por Decreto Supremo N° 006-2017-JUS.**
"Artículo 246.- Principios de la potestad sancionadora administrativa
La potestad sancionadora de todas las entidades está regida adicionalmente por los siguientes principios especiales:
(...)
5.- Irretroactividad.-*Son aplicables las disposiciones sancionadoras vigentes en el momento de incurrir el administrado en la conducta a sancionar, salvo que las posteriores le sean más favorables.*
Las disposiciones sancionadoras producen efecto retroactivo en cuanto favorecen al presunto infractor o al infractor, tanto en lo referido a la tipificación de la infracción como a la sanción y a sus plazos de prescripción, incluso respecto de las sanciones en ejecución al entrar en vigor la nueva disposición.
(...)"

[23] **Texto Único Ordenado de la Ley N° 27444, Ley del Procedimiento Administrativo General, aprobado por Decreto Supremo N° 006-2017-JUS.**
"Artículo 255.- 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 253."

[24] **Reglamento de la Ley de Protección de Datos Personales, aprobado por Decreto Supremo N° 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. Dicho artículo debe leerse conjuntamente con lo previsto en el numeral 2 del artículo 255[25] de la LPAG, 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. Análisis de la cuestión en discusión

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

(i) Si la administrada habría incumplido el deber de información establecido en el artículo 18 de la LPDP, al no informar a sus alumnos que realizaba flujo transfronterizo de los datos personales que recopilaba; y si en consecuencia, la administrada incurrió en la infracción leve tipificada en el literal f. del numeral 1 del artículo 132 del Reglamento de la LPDP: *"Dar tratamiento a los datos personales contraviniendo las disposiciones de la Ley y su Reglamento"*.

(ii) Si la administrada no habría comunicado e inscrito en la Autoridad de Protección de Datos Personales, la realización de flujo transfronterizo de datos personales, de acuerdo a lo dispuesto por los artículos 26 y 77 del Reglamento de la LPDP y el artículo 34 de la LPDP; y si en consecuencia, la administrada incurrió en la infracción leve tipificada en el literal e. del numeral 1 del artículo 132 del Reglamento de la LPDP: *"No inscribir o actualizar en el Registro Nacional los actos establecidos en el artículo 34 de la Ley"*.

(iii) Si la administrada no habría implementado las medidas de seguridad consistentes en documentar los procedimientos de gestión de accesos y gestión de privilegios

PERÚ Ministerio de Justicia y Derechos Humanos
Dirección de Protección de Datos Personales
GONZALEZ L.

[25] **Texto Único Ordenado de la Ley N° 27444, Ley del Procedimiento Administrativo General, aprobado por Decreto Supremo N° 006-2017-JUS.**
*"**Artículo 255.- 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."

de los usuarios del sistema, y no implementar controles de seguridad para la restricción de copias de datos, pues contaba con puertos USB y el grabador DVD habilitados, lo que permitiría la visualización y grabación de archivos, incumpliendo lo dispuesto por los artículos 39 y 43 del Reglamento de la LPDP; y si en consecuencia, la administrada incurrió en la infracción leve tipificada en el literal a. del numeral 1 del artículo 132 del Reglamento de la LPDP: "*Realizar tratamiento de datos personales incumpliendo las medidas de seguridad establecidas en la normativa sobre la materia*".

(i) <u>Sobre el deber de informar la realización de flujo transfronterizo de datos personales a sus titulares</u>

38. Se imputa a la administrada que habría efectuado tratamiento de datos personales incumpliendo las disposiciones de la Ley y su Reglamento, dado que habría incumplido la disposición legal del artículo 18 de la LPDP, en tanto que no habría informado que realizaba flujo transfronterizo de datos personales a sus titulares (alumnos); por lo que habría incurrido en la infracción leve tipificada en el literal f. del numeral 1 del artículo 132 del Reglamento de la LPDP, esto es: *"Dar tratamiento a los datos personales contraviniendo las disposiciones de la Ley y su Reglamento"*.

En tal sentido corresponde analizar la normativa vigente y aplicable sobre la materia, los medios probatorios que dejan constancia de los hallazgos encontrados en el procedimiento, y los descargos presentados por la administrada para desvirtuar el hecho imputado.

39. Así, se tiene que el artículo 2 de la LPDP modificado por la Tercera Disposición Complementaria Modificatoria del Decreto Legislativo N° 1353, establece las definiciones de los términos que coadyuvan a la comprensión de la LPDP y su Reglamento y la protección que otorgan; entre aquellas definiciones, para este caso, importa resaltar lo que se entiende por datos personales, titular de datos personales, titular del banco de datos personales y tratamiento de datos personales; los que se detallan a continuación:

*"**Artículo 2. Definiciones***
Para todos los efectos de la presente Ley, se entiende por:
(...)
*4. **Datos personales.** Toda información sobre una persona natural que la identifica o la hace identificable a través de medios que pueden ser razonablemente utilizados."*
(...)
*16. **Titular de datos personales.** Persona natural a quien corresponde 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.*
(...)
*19. **Tratamiento de datos personales.** Cualquier operación o procedimiento técnico, automatizado o no, que permite la recopilación, registro, organización, almacenamiento, conservación, elaboración, modificación, extracción, consulta, utilización, bloqueo, supresión, comunicación por transferencia o por difusión o cualquier otra forma de procesamiento que facilite el acceso, correlación o interconexión de los datos personales."*

40. Por su parte, el numeral 4 del artículo 2 del Reglamento de la LPDP define los datos personales en los siguientes términos:

> *"4.**Datos personales:** Es aquella información numérica, alfabética, gráfica, fotográfica, acústica, sobre hábitos personales, o de cualquier otro tipo concerniente a las personas naturales que las identifica o las hace identificables a través de medios que puedan ser razonablemente utilizados."*

41. De las normas acotadas se desprende que los datos personales consisten en toda información, incluida la información fotográfica, que sirve para identificar o hacer identificables a las personas naturales; estos datos son susceptibles de conformar bancos de datos personales diferenciados a cargo de personas naturales o jurídicas encargadas de administrarlos, determinando su finalidad y contenido, así como el tratamiento que se dará a dicha información, a través de las operaciones o procedimientos técnicos, que entre otros, permitan la recopilación, registro, almacenamiento, conservación, utilización de los datos personales.

PERÚ Ministerio de Justicia y Derechos Humanos
Dirección de Protección de Datos Personales
GONZALEZ L

42. De otro lado, el artículo 18 de la LPDP establece el derecho de los titulares de los datos personales sobre el tratamiento que se realizará sobre aquellos, indicando lo siguiente:

> *"**Artículo 18. Derecho de información del titular de datos personales***
> *El titular de datos personales tiene derecho a ser informado en forma detallada, sencilla, expresa, inequívoca y de manera previa a su recopilación, sobre la finalidad para la que sus datos personales serán tratados; quiénes son o pueden ser sus destinatarios, la existencia del banco de datos en que se almacenarán, así como la identidad y domicilio de su titular y, de ser el caso, del o de los encargados del tratamiento de sus datos personales; el carácter obligatorio o facultativo de sus respuestas al cuestionario que se le proponga, en especial en cuanto a los datos sensibles; la transferencia de los datos personales; las consecuencias de proporcionar sus datos personales y de su negativa a hacerlo; el tiempo durante el cual se conserven sus datos personales; y la posibilidad de ejercer los derechos que la ley le concede y los medios previstos para ello."*

43. Así, de la normas acotadas se desprende que los titulares de los datos personales deben ser informados sobre el tratamiento que se realizará respecto de los mismos,

se trate de información gráfica, fotográfica, sonora o conductual, indicándoles la finalidad de dicho tratamiento, como por ejemplo el fin de la recopilación y almacenamiento de los datos, informando además si existe una base de datos que conservará la información (sea nacional o internacional) y el tiempo de la conservación, qué personas se encargarán de administrar la información y los terceros destinarios de aquella si los hubiera.

44. Ahora bien, en el Acta de Fiscalización N° 01-2016, se dejó constancia de la visita de supervisión realizada a la administrada el 24 de agosto de 2016, indicando lo siguiente:

> *"(...) cuentan con un sistema denominado "Control de Información Personal del Alumno" (sistema web) al cual se accede desde la página web de la fiscalizada (www.sanvicenteica.edu.pe) (...).*
> *(...) Cuenta con el servicio de internet, intranet, y página web (www.sanvicenteica.edu.pe), desde la cual se accede al sistema "Control de Información Personal del Alumno" y en el cual, el asesor de informática registra los datos de los alumnos y a la vez, otorga un usuario y contraseña de acceso a cada tutor de aula. (...)."*

45. En el Informe N° 044-2016-DSC-ORQR[26] de 04 de noviembre de 2016, emitido por el personal técnico de la DSC mediante el cual se informa sobre la supervisión realizada a la administrada, se indica que:

> *"(...) 4. El tratamiento de datos personales de alumnos en versión automatizada, se realiza a través del sistema web "Control de Información Personal del Alumno", al cual se accede desde la página web www.sanvicenteica.edu.pe y recopila información (...)."*

> *"(...) 24. La página web www.sanvicenteica.edu.pe se encuentra localizada en la ciudad de Dallas en los Estados Unidos de Norteamérica."*

46. De otro lado, el Informe N° 092-2016-JUS/DGPDP-DSC[27] de 28 de diciembre de 2016, mediante el cual se emiten las conclusiones sobre el procedimiento de fiscalización realizado, indica:

> *"(...) 17. Según se aprecia en las impresiones del sistema web "Control de la Información Personal del Alumno", Colegio de Particular San Vicente, recopila datos personales de los alumnos que son matriculados por sus padres, para lo cual se accede desde la página web www.sanvicenteica.edu.pe;*
>
> *18. Cabe indicar que de acuerdo con lo señalado en el Informe N° 044-2016-DSC-ORQR, la dirección IP de dicha página web se encuentra en la ciudad de Dallas, Estados Unidos de Norteamérica, lo cual implica la realización de flujo transfronterizo de los datos recopilados.*
>
> *19. No obstante, en las interfaces de dicho sistema web no se presenta ningún dispositivo o medio informativo por el cual se indique a sus usuarios, que se efectuará el mencionado flujo transfronterizo. (...);*

PERÚ Ministerio de Justicia y Derechos Humanos
Dirección de Protección de Datos Personales
M. GONZALEZ L

[26] Folio 64 a 67
[27] Folio 76 a 80

IV. Conclusiones
(...)2. Colegio Particular San Vicente no informa a los usuarios del sistema web "Control de la Información Personal del Alumno", acerca del flujo transfronterizo que realizará con la información a registrar (...)."

47. De los documentos antes descritos, se observa que el servidor de la web www.sanvicenteica.edu.pe se ubica en Estados Unidos de América[28], específicamente en la ciudad de Dallas, y que a través del sistema denominado "Control de Información Personal del Alumno"de dicha página web, recopila datos personales de sus alumnos. En tal sentido, verificándose que la administrada recopila datos personales de sus alumnos a través de una página web cuyo servidor (donde se almacenan los datos) se ubica en Estados Unidos, se colige que la administrada realiza flujo transfronterizo de tales datos.

48. Asimismo, de la revisión de la página web en mención, así como de los documentos ya citados, se observa que no se ha consignado dispositivo alguno en el sistema "Control de la Información Personal del Alumno" de www.sanvicenteica.edu.pe, que indique a los usuarios sobre la realización de flujo transfronterizo de datos personales, lo cual permite concluir que la administrada realizaba flujo transfronterizo de datos personales sin informarlo a los usuarios de su página web, incumpliendo así el deber de información establecido en el artículo 18 de la LPDP.

49. Por su parte, el 04 de octubre de 2017, la administrada presentó sus descargos señalando que el sistema "Control de la Información Personal del Alumno" tenía por finalidad mantener actualizados los datos de los alumnos, pero no llegó a ser utilizado por la totalidad de usuarios a los que estaba dirigido; por esa razón indica que dio de baja a dicho sistema así como a los datos registrados en el mismo, lo cual sustenta en la copia del Oficio N° 090-2016-I.E.E.P./DIRECCION y el Acta de Eliminación de Datos.

50. De la evaluación de los documentos antes citados se observa que con el Oficio N° 090-2016-I.E.E.P./DIRECCION, el área de informática de la administrada tramitó la solicitud de baja del sistema "Control de Información Personal del Alumno", y con el Acta de Eliminación de Datos[29], se dejó constancia que se eliminó el pedido de

[28] Folio 70
[29] Folio 101

usuario y contraseña para el acceso al sistema (http://sanvicenteica.edu.pe/portal/sistemabd2016.html), se eliminaron los programas y carpetas que conformaban el sistema y se eliminaron los registros de las tablas de la base de datos MySQL que almacenaba la data de alumnos, lo cual a su vez fue comunicado a la dirección de la administrada con Informe N° 001[30], firmado por el asesor informático de la administrada..

51. En tal sentido, se aprecia que si bien al momento de la fiscalización, esto es el 24 de agosto de 2016, se observó que la administrada recopilaba datos personales a través de su sistema "Control de Información Personal del Alumno" de la página web www.sanvicenteica.edu.pe ubicada en la ciudad de Dallas – Estados Unidos, lo que implicaba la realización de flujo transfronterizo de datos sin informarlo a sus usuarios; es de advertir que con la documentación evaluada, en aplicación del principio de presunción de veracidad según el cual las declaraciones de los administrados se presumen ciertas, se tiene por acreditada la baja del sistema aludido, entendiéndose que ya no recopila datos a través de la misma, y por ende insubsistente la obligación de informar a los usuarios sobre la realización de flujo transfronterizo.

52. Cabe agregar que los documentos citados describen acciones de enmienda respecto de la imputación efectuada, lo que será considerado como atenuante al momento de graduar la sanción en aplicación del artículo 126 del Reglamento de la LPDP, ya que tales documentos fueron presentados el 04 de octubre de 2017 sin consignar fecha cierta, por lo tanto de forma posterior al inicio del procedimiento sancionador el 15 de setiembre de 2017.

(ii) <u>Sobre el deber de comunicar la realización de flujo transfronterizo a la Autoridad Nacional de Protección de Datos Personales</u>

53. Se imputa a la administrada que no habría comunicado a la Autoridad Nacional de Protección de Datos Personales la realización de flujo transfronterizo de datos personales; por lo que habría incurrido en la infracción tipificada en el literal e. del numeral 1 del artículo 132 del Reglamento de la LPDP consistente en: "*No inscribir o actualizar en el Registro Nacional los actos establecidos en el artículo 34 de la Ley*";

    En tal sentido, corresponde analizar la normativa vigente y aplicable sobre la materia, los medios probatorios que dejan constancia de los hallazgos encontrados en el procedimiento, y los descargos presentados por la administrada para desvirtuar el hecho imputado.

54. Sobre la obligación de la comunicación de la realización de flujo transfronterizo, la LPDP establece lo siguiente:

    > "***Artículo 2. Definiciones***
    > *Para todos los efectos de la presente Ley, se entiende por:*
    > *(...)*
    > ***10. Flujo transfronterizo de datos personales.*** *Transferencia internacional de datos personales a un destinatario situado en un país distinto al país de origen de los datos personales, sin importar el soporte en que estos se encuentren, los medios por los cuales se efectuó la transferencia, ni el tratamiento que reciban."*

PERÚ Ministerio de Justicia y Derechos Humanos
Dirección de Protección de Datos Personales
M. GONZALEZ L

[30] Folio 102

*"**Artículo 34. Registro Nacional de Protección de Datos Personales***
Créase el Registro Nacional de Protección de Datos Personal como registro de carácter administrativo a cargo de la Autoridad Nacional de Protección de Datos Personales, con la finalidad de inscribir en forma diferenciada, a nivel nacional, lo siguiente:
(...)
2. Las comunicaciones de flujo transfronterizo de datos personales."

55. Por su parte, el Reglamento de la LPDP respecto de la obligación de comunicación de flujo transfronterizo señala lo siguiente:

*"**Artículo 26.- Participación de la Dirección General de Protección de Datos Personales respecto del flujo transfronterizo de datos personales.***
Los titulares del banco de datos personales o responsables del tratamiento, podrán solicitar la opinión de la Dirección General de Protección de Datos Personales respecto a si el flujo transfronterizo de datos personales que realiza o realizará cumple con lo dispuesto por la Ley y el presente reglamento."
En cualquier caso, el flujo transfronterizo de datos personales se pondrá en conocimiento de la Dirección General de Protección de Datos Personales, incluyendo la información que se requiere para la transferencia de datos personales y el registro de banco de datos."

PERÚ Ministerio de Justicia y Derechos Humanos
Dirección de Protección de Datos Personales
GONZALEZ I

*"**Artículo 77.- Actos y documentos inscribibles en el Registro.***
Serán objeto de inscripción en el Registro Nacional de Protección de Datos Personales con arreglo a lo dispuesto en la Ley y en este título:
(...)
5. Las comunicaciones referidas al flujo transfronterizo de datos personales. (...)"

56. De las normas legales antes citadas se desprende que el flujo transfronterizo de datos personales es la transferencia internacional de datos personales a un destinatario situado en un país distinto al país de origen de los datos, transferencia que debe ser comunicada a la Dirección de Protección de Datos Personales, con la finalidad que aquella pueda llevar a cabo la supervisión del cumplimiento de las exigencias legales para la realización del flujo transfronterizo.

57. Ahora bien, en la visita de fiscalización realizada a la administrada el 30 de mayo de 2016 se levantó el Acta de Fiscalización N° 01-2016[31], en la cual se dejó constancia de lo siguiente:

> *"(...) cuentan con un sistema denominado "Control de Información Personal del Alumno" (sistema web) al cual se accede desde la página web de la fiscalizada (www.sanvicenteica.edu.pe) (...).*
>
> *(...) Cuenta con el servicio de internet, intranet, y página web (www.sanvicenteica.edu.pe), desde la cual se accede al sistema "Control de Información Personal del Alumno" y en el cual, el asesor de informática registra los datos de los alumnos y a la vez, otorga un usuario y contraseña de acceso a cada tutor de aula. (...)."*

58. En el Informe N° 044-2016-DSC-ORQR[32] de fecha 04 de noviembre de 2016, emitido por el personal técnico de la DSC mediante el cual se informa sobre la supervisión realizada a la administrada, se indica que:

> *"(...) 4. El tratamiento de datos personales de alumnos en versión automatizada, se realiza a través del sistema web "Control de Información Personal del Alumno", al cual se accede desde la página web www.sanvicenteica.edu.pe y recopila información (...)."*
>
> *"(...) 24. La página web www.sanvicenteica.edu.pe se encuentra localizada en la ciudad de Dallas en los Estados Unidos de Norteamérica."*

59. Asimismo, en la comunicación de correo electrónico de fecha 13 de diciembre de 2016[33], la DSC solicitó a la Dirección de Registro Nacional de Protección de Datos Personales (DRNPDP) informar si la administrada había comunicado la realización de flujo transfronterizo a la Autoridad de Protección de Datos Personales, observándose que mediante correo electrónico de fecha 16 de diciembre de 2016[34], la DRNPDP informó que la administrada a dicha fecha no había inscrito comunicación de flujo transfronterizo.

60. De otro lado, el Informe N° 092-2016-JUS/DGPDP-DSC[35] de 28 de diciembre de 2016, mediante el cual se emiten las conclusiones sobre el procedimiento de fiscalización realizado, indica:

> *"(...) IV. Conclusiones*
> *4. Colegio Particular San Vicente no ha comunicado la realización de flujo transfronterizo de los datos personales recopilados a través del sistema web "Control de la Información Personal del Alumno"*

61. Por su parte, el 04 de octubre de 2017, la administrada presentó sus descargos señalando que el sistema "Control de la Información Personal del Alumno" fue dado de baja, así como los datos registrados en el mismo, siendo que al ya no existir dicho sistema en la web ya no recopila datos personales, y por ende ya no realiza flujo transfronterizo de datos, por lo que alega, ya no tiene la obligación de comunicar la

PERÚ Ministerio de Justicia y Derechos Humanos
Dirección de Protección de Datos Personales
M. GONZALEZ L

[31] Folio 15 a 21
[32] Folio 64 a 67
[33] Folio 71
[34] Folio 73
[35] Folio 76 a 80

realización de flujo transfronterizo a la Autoridad de Protección de Datos Personales, en tanto que ya no realiza dicho flujo.

62. Al respecto, cabe señalar que de la revisión de los documentos con los cuales sustenta sus alegatos, esto es, la copia del Oficio N° 090-2016-I.E.E.P./DIRECCION[36], el Acta de Eliminación de Datos[37], y el Informe N° 001[38], se observa que la administrada ha dado de baja al sistema "Control de la Información Personal del Alumno", por lo que en aplicación del principio de presunción de veracidad, según el cual los documentos y declaraciones de los administrados se presumen ciertos, se tiene que por acreditada la baja del sistema, entendiéndose que al ya no existir, ya no recopila datos y por ende ya no realiza flujo transfronterizo, con lo cual a la actualidad desaparece la obligación de comunicarlo a la Autoridad de Protección de Datos Personales.

63. Cabe agregar que los documentos citados describen acciones de enmienda respecto de la imputación efectuada, lo que será considerado como atenuante al momento de graduar la sanción en aplicación del artículo 126 del Reglamento de la LPDP, ya que tales documentos fueron presentados el 04 de octubre de 2017 sin consignar fecha cierta, por lo tanto de forma posterior al inicio del procedimiento sancionador el 15 de setiembre de 2017.

PERÚ Ministerio de Justicia y Derechos Humanos
Dirección de Protección de Datos Personales
GONZALEZ L

(iii) <u>Sobre el presunto incumplimiento de las medidas de seguridad</u>

64. Se imputa a la administrada que no habría implementado las medidas de seguridad de la información dado que no habría documentados los procedimientos de gestión de accesos y gestión de privilegios de acuerdo a lo establecido en el numeral 1 del artículo 39 del Reglamento de la LPDP, y porque no habría generado restricciones para la generación de copias o reproducción de documentos ya que los puertos USB y grabador de DVD de la computadora del área de informática habrían estado habilitados, permitiendo la visualización y grabación de archivos, incumpliendo lo dispuesto por el artículo 43 de la LPDP; configurándose la infracción leve tipificada en el literal a. del numeral 1 del artículo 132 del Reglamento de la LPDD consistente

[36] Folio 100
[37] Folio 101
[38] Folio 102

en: "*Realizar tratamiento de datos personales incumpliendo las medidas de seguridad establecidas en la normativa sobre la materia*".

En tal sentido corresponde analizar la normativa vigente y aplicable sobre la materia, los medios probatorios que dejan constancia de los hallazgos encontrados en el procedimiento, y los descargos presentados por la administrada para desvirtuar el hecho imputado.

65. Al respecto, es preciso mencionar que el artículo 9 de la LPDP señala el principio de seguridad como no de los principios rectores de la protección de datos personales:

> ***"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."*

66. En ese marco, el artículo 16 de la LPDP establece la obligación de adoptar medidas de seguridad para el tratamiento de datos personales:

> ***"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.*
> *(...)*
> *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."*

67. Por su parte, sobre las medidas de seguridad a adoptarse en el tratamiento de datos personales ya sea en soporte automatizado o no automatizado, el Reglamento de la LPDP señala 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:*
>
> *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."*
>
> *"**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."*

68. De las disposiciones legales antes citadas, se colige que en cuanto al tratamiento de datos personales en soportes automatizados, es obligatorio definir los procesos de gestión de accesos y privilegios, la identificación de usuarios en el sistema, así como el proceso de verificación periódica de dichos privilegios; mediante procedimientos documentados a fin de garantizar su idoneidad.

    Asimismo, en cuanto al control de accesos a información la norma señala que la generación de copias o la reproducción de los documentos únicamente podrán ser realizadas bajo el control del personal autorizado.

69. Ahora bien, del Acta de Fiscalización N° 01-2016[39] en la cual se deja constancia de la supervisión realizada a la administrada el día 24 de agosto de 2016, se indica lo siguiente:

    "(...) Referente a las medidas de seguridad, se verificó que la computadora asignadas al Asesor de Informática (...) tiene los puertos USB habilitados (permite visualizar y grabar archivos), cuenta con grabador de DVD habilitado (...);

    (...) No cuenta con procedimientos documentados referidos a la gestión de accesos y gestión de privilegios (...)".

70. Luego, con Informe N° 044-2016-DSC-ORQR[40] de fecha 04 de noviembre de 2016, la DSC emite un informe sobre la visita y evaluación del cumplimiento de las medidas de seguridad de la administrada, indicando lo siguiente:

    "(...) Tratamiento automatizado
    (...)
    8. Se verificaron las medidas de seguridad en la computadora asignada al Asesor de Informática, constatándose:
    (...)
    c) Cuenta con los puertos USB habilitados permite la visualización y grabación de archivos. Asimismo, cuenta con grabador de DVD habilitado.

[39] Folio 15 a 21
[40] Folio 64 a 67

(...)
10. La entidad supervisada indicó que no cuenta con procedimientos documentados referentes a la gestión de accesos y gestión de privilegios de los usuarios.
(...)
V. Conclusiones
(...)
2. El colegio Particular San Vicente no documenta los procedimientos de gestión de accesos y gestión de privilegios (...);
(...)
6. El colegio Particular San Vicente no establece procedimientos que restrinjan la generación de copias o reproducción de documentos (....)."

71. Posteriormente, con Informe N° 092-2016-JUS/DGPDP-DSC[41] de 28 de diciembre de 2016, la DSC emitió el informe que recoge las conclusiones del procedimiento sancionador indicando lo siguiente:

Sobre las medidas de seguridad necesarias para el tratamiento de datos personales
"(...) 32. (...) Se constató que dicha entidad no tiene documentados los procedimientos de gestión de accesos y gestión de privilegios del sistema "Control de Información Personal del Alumno" (....).";
33. (...) Se verificó que la entidad fiscalizada no tiene implementados controles o restricciones de copias en la computadora donde se realiza el tratamiento de datos personales de sus alumnos (asignada al Asesor de Informática), la cual contaba con los puertos USB y el grabador de DVD habilitado para visualizar y copiar archivos. (...)."

72. Del acta de fiscalización y de los informes antes descritos se observa que al momento de la fiscalización y posteriormente en la verificación de la implementación de medidas de seguridad, se constató que la administrada no documentaba los procedimientos de gestión de accesos y gestión de privilegios de los usuarios de sus sistemas, con lo cual se incumplía lo dispuesto por el numeral 1 del artículo 39 del Reglamento de la LPDP; asimismo, se evidenció que no realizaba controles de los puertos USB y lectora de DVD ya que se encontraban habilitados, lo que permitía que se copie y/o reproduzca información sin controles por parte de personal no autorizado, con lo cual se incumplía lo dispuesto por el artículo 43 del Reglamento de la LPDP.

73. Por su parte, la administrada presentó sus descargos mediante escrito de 04 de octubre de 2017, señalando que ha implementado una serie de medidas para cumplir con las normas sobre protección de datos personales, entre ellas, aprobó la "Directiva de Seguridad de Datos Personales", lo cual sustenta con la presentación de la copia de la Resolución Directoral N° 014-2017-I.E.P.P. "SV"-I[42].

74. Sobre el particular, mediante Informe N° 044-2017-DFI-VARS de 10 de noviembre de 2017, personal técnico de la DFI emite informe de evaluación de implementación de las medidas de seguridad de la administrada, señalando lo siguiente:

"(...) Respecto a la obligación de tener documentado la gestión de accesos, gestión de privilegios (...), se verificó que a la fecha la institución fiscalizada

[41] Folio 76 a 80
[42] Folio 104 a 107

mantiene un banco de datos denominado "alumnos" (Código RNPDP N° 10985), (...) en el cual detalla que realiza tratamiento de datos personales de alumnos en soporte automatizado. Por lo cual mantiene la obligación de contar con la referida documentación;

En cuanto a la falta de restricciones de copias de datos personales colegio particular San Vicente ha señalado políticas para los equipos que realicen tratamiento de datos personales tales como inhabilitación de puertos USB y grabadores de CD/DVD (...)."

75. De acuerdo con lo concluido en el informe técnico antes descrito, de la "Directiva de Seguridad de Datos Personales", se observa que se han establecido lineamientos para la restricción de copias y reproducciones de información a través del acceso vía puertos de USD/DVD indicando que ello solo será realizado por personal autorizado y que adoptará las medidas para inhabilitar dichos accesos, en ese sentido, en aplicación del principio de presunción de veracidad, se tendrán por ciertos los alegatos de la administrada como acciones de enmienda de la imputación efectuada, sin perjuicio de que a través de la imposición de una medida correctiva se requiera la exhibición del cumplimiento de tales medidas.

PERU Ministerio de Justicia y Derechos Humanos
Dirección de Protección de Datos Personales
GONZALEZ L

76. De otro lado, en cuanto a la documentación de procedimientos de gestión de accesos y gestión de privilegios, se advierte que si bien ha eliminado de su página web el sistema "Control de Información Personal del Alumno" con el cual realizaba el tratamiento automatizado de datos personales, también lo es que de acuerdo a lo verificado por el área técnica de la DFI, al 10 de noviembre de 2017, aún subsistía la existencia del banco de datos personales automatizado "alumnos", según lo indicado en el Informe N° 044-2017-DFI-VARS, por lo que subsiste la obligación de documentar los procedimientos de gestión de accesos y gestión de privilegios sobre dicha información, no habiéndose por ende desvirtuado ni acreditado acciones de enmienda respecto de esta imputación.

77. Así pues, de la fiscalización de las acciones realizadas por la administrada para la implementación de las medidas de seguridad exigibles, a partir del 04 de octubre de 2017, esto es con fecha posterior al inicio del procedimiento sancionador el 15 de setiembre de 2017, se evidencia que ha realizado acciones de enmienda para implementar las medidas de seguridad requeridas con el establecimiento de lineamientos para la implementación de restricciones de copias a través de la

inhabilitación de los puertos USB/DVD, lo que en aplicación del artículo 126 del Reglamento de la LPDP, será considerado como acción de enmienda a efectos de atenuar la sanción a imponer.

Sobre las sanciones a aplicar a los hechos analizados

78. La Tercera Disposición Complementaria Modificatoria del Reglamento del Decreto Legislativo N° 1353, aprobado mediante Decreto Supremo N° 019-2017-JUS[43], de fecha 15 de setiembre de 2017, 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 al Reglamento de la LPDP, que en adelante tipifica las infracciones.

79. 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 0,5 de una unidad impositiva tributaria hasta una multa de 100 unidades impositivas tributarias[44], sin perjuicio de las medidas correctivas que puedan determinarse de acuerdo a lo establecido en el artículo 118 del Reglamento de la LPDP[45].

80. En el presente caso, en aplicación de la excepción establecida en el principio de irretroactividad (retroactividad benigna) se ha determinado la comisión de las siguientes infracciones:

    (i) Infracción leve tipificada en el literal f. del numeral 1 del artículo 132 del Reglamento de la LPDP: *"Dar tratamiento a los datos personales contraviniendo las disposiciones de la Ley y su Reglamento"*; ya que al momento de la fiscalización se detectó que la administrada no informaba a sus alumnos que realizaba flujo transfronterizo sobre los datos personales que recopilaba, incumpliendo con ello lo dispuesto en el artículo 18 de la LPDP. Infracción leve

PERÚ | Ministerio de Justicia y Derechos Humanos
Dirección de Protección de Datos Personales
M. GONZALEZ L

---

[43] **Decreto Supremo N° 019-2017-JUS, que aprueba el Reglamento del Decreto Legislativo N° 1153**
"Tercera.- Incorporación del Capítulo IV de Infracciones al Título VI de Infracciones y Sanciones al Reglamento de la Ley N° 29733, Ley de Protección de Datos Personales
Incorpórese el Capítulo IV de Infracciones al Título VI al Reglamento de la de la Ley N° 29733, Ley de Protección de Datos Personales, aprobado por el Decreto Supremo N° 003-2013-JUS, en los siguientes términos:
TÍTULO VI INFRACCIONES Y SANCIONES
CAPÍTULO IV
INFRACCIONES
Artículo 132.- Infracciones
Las infracciones a la Ley N° 29733, Ley de Protección de Datos Personales, o su Reglamento se califican como leves, graves y muy graves y se sancionan con multa de acuerdo al artículo 39 de la citada Ley."

[44] **Ley N° 29733, Ley de Proteccion 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)."

[45] **Decreto Supremo N° 003-2013-JUS, que aprueba el Reglamento de la Ley de Protección de Datos Personales**
"Artículo 118.- Medidas cautelares y correctivas.
Una vez iniciado el procedimiento sancionador, la Dirección de Sanciones podrá disponer, mediante acto motivado, la adopción de medidas de carácter provisional que aseguren la eficacia de la resolución final que pudiera recaer en el referido procedimiento, con observancia de las normas aplicables de la Ley N° 27444, Ley del Procedimiento Administrativo General.
Asimismo, sin perjuicio de la sanción administrativa que corresponda por una infracción a las disposiciones contenidas en la Ley y el presente reglamento, se podrán dictar, cuando sea posible, medidas correctivas destinadas a eliminar, evitar o detener los efectos de las infracciones."

que de acuerdo con el artículo 39 de la LPDP, es sancionable con una multa desde cero coma cinco (0,5) UIT hasta cinco (5) UIT[46], sin perjuicio de las medidas correctivas a determinarse según el artículo 118 del Reglamento de la LPDP[47].

(ii) Infracción leve tipificada en el literal e. del numeral 1 del artículo 132 del Reglamento de la LPDP: *"No inscribir o actualizar en el Registro Nacional los actos establecidos en el artículo 34 de la Ley"*; ya que al momento de la fiscalización se detectó que la administrada no había comunicado e inscrito en la Autoridad de Protección de Datos Personales, la realización de flujo transfronterizo de datos personales, de acuerdo a lo dispuesto por los artículos 26 y 77 del Reglamento de la LPDP y el artículo 34 de la LPDP. Infracción leve que de acuerdo con el artículo 39 de la LPDP, es sancionable con una multa desde cero coma cinco (0,5) UIT

PERÚ Ministerio de Justicia y Derechos Humanos
Dirección de Protección de Datos Personales
M. GONZÁLEZ L.

[46] **Ley N° 29733, Ley de Protección de Datos Personales:**
"Artículo 38. Infracciones
Constituye infracción sancionable toda acción u omisión que contravenga o incumpla alguna de las disposiciones contenidas en esta Ley o en su reglamento.
Las infracciones se califican como leves, graves y muy graves.
(...)".
"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).
(...)".

[47] **Reglamento de la Ley de Protección de Datos Personales, aprobado por Decreto Supremo N° 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 N° 27444, Ley del Procedimiento Administrativo General.
Asimismo, sin perjuicio de la sanción administrativa que corresponda por una infracción a las disposiciones contenidas en la Ley y el presente reglamento, se podrán dictar, cuando sea posible, medidas correctivas destinadas a eliminar, evitar o detener los efectos de las infracciones."

hasta cinco (5) UIT[48], sin perjuicio de las medidas correctivas a determinarse según el artículo 118 del Reglamento de la LPDP[49].

(iii) Infracción leve tipificada en el literal a. del numeral 1 del artículo 132 del Reglamento de la LPDP: "*Realizar tratamiento de datos personales incumpliendo las medidas de seguridad establecidas en la normativa sobre la materia*"; ya que al momento de la fiscalización se detectó que la administrada no había implementado las medidas de seguridad consistentes en documentar los procedimientos de gestión de accesos y gestión de privilegios de los usuarios del sistema, y no implementar controles de seguridad para la restricción de copias de datos, pues contaba con puertos USB y el grabador DVD habilitados, lo que permitiría la visualización y grabación de archivos, incumpliendo lo dispuesto por los artículos 39 y 43 del Reglamento de la LPDP.

81. Cabe señalar que la Dirección de Protección de Datos Personales determina el monto de las multas a ser impuestas tomando en cuenta para su graduación los criterios establecidos en el numeral 3 del artículo 246 del TUO de la LPAG. En tal sentido, debe prever que la comisión de las conductas sancionables no resulten más ventajosas 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.

82. En el presente caso, se considera como criterios relevantes para graduar las infracciones evidenciadas los siguientes:

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

No se ha evidenciado un beneficio ilícito resultante de la comisión de las infracciones cometidas.

PERÚ Ministerio de Justicia y Derechos Humanos
Dirección de Protección de Datos Personales
M. GONZALEZ L.

[48] **Ley N° 29733, Ley de Protección de Datos Personales:**
"Artículo 38. Infracciones
Constituye infracción sancionable toda acción u omisión que contravenga o incumpla alguna de las disposiciones contenidas en esta Ley o en su reglamento.
Las infracciones se califican como leves, graves y muy graves.
(...)".
"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).
(...)".

[49] **Reglamento de la Ley de Protección de Datos Personales, aprobado por Decreto Supremo N° 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 N° 27444, Ley del Procedimiento Administrativo General.
Asimismo, sin perjuicio de la sanción administrativa que corresponda por una infracción a las disposiciones contenidas en la Ley y el presente reglamento, se podrán dictar, cuando sea posible, medidas correctivas destinadas a eliminar, evitar o detener los efectos de las infracciones."

b) La probabilidad de detección de la infracción:

Respecto a la comisión de las infracciones imputadas se tiene que la probabilidad de detección de las conductas infractoras descritas es baja puesto que ha sido necesario realizar una fiscalización para la detección de las mismas, así como para analizar las medidas adoptadas por la administrada.

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

Las infracciones detectadas afectan el derecho fundamental a la protección de datos personales, el cual se encuentra reconocido en el numeral 6 del artículo 2 de la Constitución Política del Perú, siendo desarrollado por la LPDP y su reglamento.

En el presente caso, ha quedado acreditada la responsabilidad de la administrada por las infracciones imputadas.

Tales infracciones afectan el derecho de los ciudadanos a que se dé un tratamiento adecuado de sus datos personales.

PERU Ministerio de Justicia y Derechos Humanos
Dirección de Protección de Datos Personales
GONZALEZ L

d) El perjuicio económico causado:

No se ha evidenciado un perjuicio económico causado resultante de la comisión de las infracciones imputadas.

e) La reincidencia en la comisión de la infracción:

COLEGIO PARTICULAR SAN VICENTE no es reincidente, ya que no ha sido sancionada en alguna otra ocasión por la infracción imputada en el presente procedimiento sancionador.

f) Las circunstancias de la comisión de la infracción:

(i) Respecto de la comisión de la infracción imputada consistente en realizar tratamiento de datos personales contraviniendo las disposiciones de la ley, en este caso incumpliendo lo dispuesto por el artículo 18 de la LPDP; se advierte que al momento de la fiscalización la administrada no informaba a los alumnos

(usuarios del sistema) sobre la realización de flujo transfronterizo respecto los datos personales que recopilaba a través de su sistema "Control de Información Personal del Alumno" de la página web www.sanvicenteica.edu.pe.

No obstante ello, se advierte que la administrada ha realizado acciones de enmienda para cumplir con la disposición del artículo 18 de la LPDP, dando de baja al sistema aludido, con lo cual se entiende que ya no recopila datos a través de dicho sistema, resultando a la actualidad insubsistente la obligación de informar a los usuarios sobre la realización de flujo transfronterizo respecto de datos que ya no recopila, lo cual conforme a lo dispuesto por el artículo 126 del Reglamento de la LPDP y el artículo 255 del TUO de la LPAG será considerado como atenuante al momento de graduar la sanción a imponer.

(ii) Respecto de la comisión de la infracción imputada consistente en no inscribir o actualizar los actos establecidos en el artículo 34 de la LPDP; se advierte que al momento de la fiscalización se detectó que la administrada no había comunicado e inscrito en el Registro Nacional de Protección de Datos Personales, la realización de flujo transfronterizo de datos personales respecto los datos que recopilaba a través de su sistema "Control de Información Personal del Alumno" de la página web www.sanvicenteica.edu.pe.

No obstante ello, se advierte que la administrada ha realizado acciones de enmienda para cumplir con la disposición del artículo 34 de la LPDP, dando de baja al sistema aludido, con lo cual se entiende que ya no recopila datos a través de dicho sistema, resultando a la actualidad insubsistente la obligación de comunicar e inscribir en el Registro Nacional de Protección de Datos Personales, la realización de flujo transfronterizo respecto de datos que ya no recopila, lo cual conforme a lo dispuesto por el artículo 126 del Reglamento de la LPDP y el artículo 255 del TUO de la LPAG será considerado como atenuante al momento de graduar la sanción a imponer.

(iii) Respecto de la comisión de la infracción imputada consistente en no implementar las medidas de seguridad de acuerdo a la LPDP; se advierte que al momento de la fiscalización se detectó que la administrada no había documentado los procedimientos de gestión de accesos y gestión de privilegios de los usuarios del sistema, y no había implementado controles de seguridad para la restricción de copias de datos, pues contaba con puertos USB y el grabador DVD habilitados, incumpliendo lo dispuesto por los artículos 39 y 43 del Reglamento de la LPDP.

No obstante ello, se advierte que la administrada ha realizado acciones de enmienda para cumplir con las disposiciones acotadas, señalado que implementará políticas para restringir las copias e inhabilitar los puertos USB/DVD, lo cual conforme a lo dispuesto por el artículo 126 del Reglamento de la LPDP y el artículo 255 del TUO de la LPAG será considerado como atenuante al momento de graduar la sanción a imponer.

Sin embargo, a fin de dar cumplimiento a la normativa sobre protección de datos personales, resulta necesario que la administrada acredite haber documentado los procedimientos de gestión de accesos y gestión de privilegios para el banco de datos automatizado "alumnos"; lo cual será requerido a través de la imposición de una medida correctiva.

Perú Ministerio de Justicia y Derechos Humanos
Dirección de Protección de Datos Personales
M. GONZALEZ L

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

No se ha evidenciado que haya elementos que acrediten la no intencionalidad de las infracciones cometidas.

83. En consecuencia, habiéndose realizado el análisis de las conductas infractoras aplicando el principio de irretroactividad de la potestad sancionadora administrativa establecido en el numeral 5 del artículo 246 del Texto Único Ordenado de la Ley N° 27444, Ley del Procedimiento Administrativo General, aprobado por Decreto Supremo Nº 006-2017-JUS; se ha determinado que los hechos infractores en los cuales incurrió la administrada se subsumen en las infracciones que a continuación se citan, correspondiéndoles además la imposición de sanciones en el rango que se describe de la siguiente forma:

(i)Realizar tratamiento de datos personales contraviniendo las disposiciones de la Ley, específicamente el artículo 18 de la LPDP, al no informar a sus alumnos que realizaba flujo transfronterizo sobre los datos personales que recopilaba; hecho que constituye la infracción leve tipificada en el literal f. del numeral 1 del artículo 132 del Reglamento de la LPDP: *"Dar tratamiento a los datos personales contraviniendo las disposiciones de la Ley y su Reglamento"*; siendo que conforme al numeral 1 del artículo 39 de la LPDP, para infracciones leves, corresponde la imposición de una sanción de multa entre 0,5 UIT hasta 5 UIT, debiendo considerarse la acción de enmienda realizada como atenuante.

(ii) No inscribir y comunicar en el Registro Nacional de Protección de Datos Personales, la realización de flujo transfronterizo de datos personales, hecho que constituye la infracción leve tipificada en el literal e. del numeral 1 del artículo 132 del Reglamento de la LPDP: *"No inscribir o actualizar en el Registro Nacional los actos establecidos en el artículo 34 de la Ley"*; siendo que conforme al numeral 1 del artículo 39 de la LPDP, para infracciones leves, corresponde la imposición de una sanción de multa entre 0,5 UIT hasta 5 UIT, debiendo considerarse la acción de enmienda realizada como atenuante.

(iii) No implementar las medidas de seguridad de la información de acuerdo a la normativa de protección de datos personales, consistentes en documentar los procedimientos de gestión de accesos y gestión de privilegios de los usuarios del sistema, y no implementar controles de seguridad para la restricción de copias de

PERÚ Ministerio de Justicia y Derechos Humanos
Dirección de Protección de Datos Personales
GONZALEZ L

datos, ya que mantenía los puertos USB y el grabador DVD habilitados; hecho que constituye la infracción leve tipificada en el literal a. del numeral 1 del artículo 132 del Reglamento de la LPDP: "*Realizar tratamiento de datos personales incumpliendo las medidas de seguridad establecidas en la normativa sobre la materia*"; siendo que conforme al numeral 1 del artículo 39 de la LPDP, para infracciones leves, corresponde la imposición de una sanción de multa entre 0,5 UIT hasta 5 UIT, debiendo considerarse la acción de enmienda realizada como atenuante.

84. Es pertinente indicar que el rango medio de la sanción a imponer para la infracciones cometidas es de dos punto setenta y cinco (2.75) unidades impositivas tributarias por cada infracción; por lo que es razonable que a partir de allí se apliquen los atenuantes, para cada caso, para ello se tendrá en cuenta la suma de todos los criterios que permiten graduar la sanción conforme a los argumentos desarrollados en el considerando 81 de la presente resolución directoral.

Por las consideraciones expuestas y de conformidad con lo dispuesto por la Ley N° 29733, Ley de Protección de Datos Personales, su reglamento aprobado por el Decreto Supremo N° 003-2013-JUS, el Texto Único Ordenado de la Ley N° 27444, Ley del Procedimiento Administrativo General, aprobado por Decreto Supremo Nº 006-2017-JUS, y el Reglamento del Decreto Legislativo N° 1353 que crea la Autoridad Nacional de Transparencia y Acceso a la Información Pública, fortalece el Régimen de Protección de Datos Personales y la regulación de la gestión de intereses, aprobado por Decreto Supremo N° 019-2017-JUS;

SE RESUELVE:

PERÚ | Ministerio de Justicia y Derechos Humanos
Dirección de Protección de Datos Personales
M. GONZALEZ L.

Artículo 1.- Sancionar a **COLEGIO PARTICULAR SAN VICENTE** con RUC 20104311076 con la multa ascendente a cero como cinco unidad impositiva tributaria **(0,5 UIT)** por la comisión de la infracción leve tipificada en el literal f. del numeral 1 del artículo 132 del Reglamento de la LPDP: *"Dar tratamiento a los datos personales contraviniendo las disposiciones de la Ley y su Reglamento"*; al haberse acreditado al momento de la fiscalización el incumplimiento del artículo 18 de la LPDP, ya que no informaba a sus alumnos que realizaba flujo transfronterizo sobre los datos personales que recopilaba.

Artículo 2.- Sancionar a **COLEGIO PARTICULAR SAN VICENTE** con RUC 20104311076 con la multa ascendente a cero como cinco unidad impositiva tributaria **(0,5 UIT)** por la comisión de la infracción leve tipificada en el literal e. del numeral 1 del artículo 132 del Reglamento de la LPDP: *"No inscribir o actualizar en el Registro Nacional los actos establecidos en el artículo 34 de la Ley"*; al haberse acreditado que al momento de la fiscalización, no había comunicado ni inscrito en el Registro de Protección de Datos Personales, la realización de flujo transfronterizo de datos personales.

Artículo 3.- Sancionar a **COLEGIO PARTICULAR SAN VICENTE** con RUC 20104311076 con la multa ascendente a una unidad impositiva tributaria **(1 UIT)** por la comisión de la infracción leve tipificada en el literal a. del numeral 1 del artículo 132 del Reglamento de la LPDP: "*Realizar tratamiento de datos personales incumpliendo las medidas de seguridad establecidas en la normativa sobre la materia*"; al haberse acreditado que al momento de la fiscalización, no había implementado las medidas de seguridad consistentes en documentar los procedimientos de gestión de accesos y

gestión de privilegios de los usuarios del sistema, y no implementar controles de seguridad para la restricción de copias de datos, ya que mantenía los puertos USB y el grabador DVD habilitados.

Artículo 4.- Imponer Medida Correctiva a **COLEGIO PARTICULAR SAN VICENTE** con RUC 20104311076, consistente en la exhibición de la documentación de procedimientos de gestión de accesos y gestión de privilegios para el banco de datos automatizado "alumnos"; medida que deberá cumplirse en un plazo de 30 días hábiles, debiendo informar además que su incumplimiento puede acarrear responsabilidades de acuerdo a los dispuesto en el literal d) del numeral 3 del artículo 132 del Reglamento de la LPDP[50].

Articulo 5.- Notificar a **COLEGIO PARTICULAR SAN VICENTE** que contra la presente resolución, de acuerdo a lo indicado en el artículo 216 del Texto Único Ordenado de la Ley N° 27444, Ley del Procedimiento Administrativo General, aprobado por Decreto Supremo Nº 006-2017-JUS, proceden los recursos de reconsideración o apelación dentro de los quince (15) días hábiles posteriores a su notificación[51].

PERÚ Ministerio de Justicia y Derechos Humanos
Dirección de Protección de Datos Personales
M. GONZALEZ

[50] **Reglamento del Decreto Legislativo Nº 1353, Decreto Legislativo que crea la Autoridad Nacional de Transparencia y Acceso a la Información Pública, fortalece el Régimen de Protección de Datos Personales y la regulación de la gestión de intereses DECRETO SUPREMO Nº 019-2017-JUS**
Tercera.- Incorporación del Capítulo IV de Infracciones al Título VI de Infracciones y Sanciones al Reglamento de la Ley Nº 29733, Ley de Protección de Datos Personales
Incorpórase el Capítulo IV de Infracciones al Título VI al Reglamento de la de la Ley Nº 29733, Ley de Protección de Datos Personales, aprobado por el Decreto Supremo Nº 003-2013-JUS, en los siguientes términos:
TÍTULO VI INFRACCIONES Y SANCIONES
CAPÍTULO IV
INFRACCIONES
Artículo 132.- Infracciones
Las infracciones a la Ley Nº 29733, Ley de Protección de Datos Personales, o su Reglamento se califican como leves, graves y muy graves y se sancionan con multa de acuerdo al artículo 39 de la citada Ley.
3.Son infracciones muy graves:
d) No cesar en el indebido tratamiento de datos personales cuando existiese un previo requerimiento de la Autoridad como resultado de un procedimiento sancionador o de un procedimiento trilateral de tutela.

[51] **Texto Único Ordenado de la Ley N° 27444, Ley del Procedimiento Administrativo General, aprobado por Decreto Supremo N° 006-2017-JUS**
*"**Artículo 216. Recursos administrativos***
216.1 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.
216.2 El término para la interposición de los recursos es de quince (15) días perentorios, y deberán resolverse en el plazo de treinta (30) días."

Artículo 6.- Informar que el pago de la multa será requerido una vez que la resolución que impone la sanción quede firme. En el requerimiento de pago se le otorgará diez (10) días hábiles para realizarlo y se entiende que cumplió con pagar la multa impuesta, si antes de que venza el plazo establecido en el requerimiento de pago, cancela el 60% de la multa impuesta conforme a lo dispuesto en el artículo 128 del reglamento de la LPDP[52].

Artículo 7.- Notificar a **COLEGIO PARTICULAR SAN VICENTE** la presente resolución, en su domicilio sito en: Av. Los Maestros N° 250 (Ovalo del estadio) Provincia y Departamento de Ica.

Regístrese y comuníquese.

MARÍA ALEJANDRA GONZÁLEZ LUNA
Directora (e) de la Dirección de Protección de Datos Personales
Ministerio de Justicia y Derechos Humanos

[52] **Decreto Supremo N° 003-2013-JUS, aprobado por Reglamento de la Ley de Protección de Datos Personales, aprobado por**
"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 integro de la multa impuesta."