Resolución Directoral

Resolución Directoral N° 1429-2018-JUS/DGTAIPD-DPDP

Expediente N°
015-2018-JUS/DPDP-PS

Resolución N° 1429-2018-JUS/DGTAIPD-DPDP

Lima, 26 de Junio de 2018

VISTOS:

El Informe Nº 051-2017-JUS/DGPDP-DSC de fecha 26 de mayo de 2016, que se sustenta en el Acta de Fiscalización Nº 01-2017 de fecha 26 de enero de 2017 (Expediente de Fiscalización N° 002-2017-DSC), emitido por la Dirección de Supervisión y Control de la Dirección General de Protección de Datos Personales; el escrito de descargo presentado el 08 de febrero de 2018; y demás documentos que obran en el respectivo expediente administrativo y;

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

CONSIDERANDO:

I. Antecedentes

1. Mediante Orden de Visita de Fiscalización Nº 002-2017-JUS/DGPDP-DSC[1], de fecha 24 de enero de 2017, 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 GRM GLOBAL RESEARCH MARKETING S.A.C. (en adelante, la administrada).

2. Mediante el Acta de Fiscalización N° 01-2017[2], se deja constancia de los hechos verificados en la visita realizada a las instalaciones de la administrada, sito en: Av. Alfredo Benavides N° 2818, Urb. El Rancho, distrito de Miraflores, provincia y departamento de Lima, el 26 de enero de 2017 a horas 12:12 pm.

3. Mediante Informe N° 017-2017-DSC-ORQR[3] de fecha 29 de marzo de 2017, se informó sobre la visita de fiscalización a la administrada.

[1] Folio 10
[2] Folio 17 a 22
[3] Folio 27 a 36

4. Mediante Informe N° 026-2017-DSC-VARS[4] de fecha 24 de abril de 2017, se emitió informe sobre la evaluación del cumplimiento de las medidas de seguridad de la administrada.

5. Mediante Informe N° 051-2017-JUS/DGPDP-DSC[5] recibido el 26 de mayo de 2017, la DSC remitió a la Dirección de Sanciones de la Dirección General de Protección de Datos Personales (en adelante, DS), los resultados de la supervisión realizada a la administrada, adjuntando las actas mencionadas en el considerando precedente y demás documentos que conforman el expediente administrativo; dicho informe fue notificado a la administrada con Oficio N° 210-2017-JUS/DGPDP-DSC[6] el 30 de mayo de 2017.

6. Mediante Resolución Directoral Nº 078-JUS/DGTAIPD-DFI[7] de fecha 29 de diciembre de 2017, notificada con Oficio N° 301-2017-JUS/DGTAIPD-DFI[8] el 18 de enero 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 la presunta comisión de la siguiente infracción:

   - La administrada no habría cumplido con implementar las medidas de seguridad para el tratamiento de datos personales, hecho que se habría configurado por:

     - No documentar los procedimientos de gestión de accesos, gestión de privilegios y verificación periódica de privilegios asignados (incumple lo establecido en el numeral 1 del artículo 39 del Reglamento de la Ley N° 29733, Ley de Protección de Datos Personales, aprobado mediante Decreto Supremo N° 003-2013-JUS).

     - No generar ni mantener registros de evidencias producto de la interacción lógica con su sistema (incumple lo establecido en el numeral 2 del artículo 39 del Reglamento de la Ley N° 29733, Ley de Protección de Datos Personales, aprobado mediante Decreto Supremo N° 003-2013-JUS).

     - Encontrarse el centro de datos en un área común, sin gabinetes para el servidor que se encuentra en el piso, el ambiente no cuenta con control de temperatura adecuado, UPS (sistema de alimentación ininterrumpida), extintor, tablero electrónico ni puerta con llave (incumple lo establecido en el artículo 40 del Reglamento de la Ley N° 29733, Ley de Protección de Datos Personales, aprobado mediante Decreto Supremo N° 003-2013-JUS).
     - No realizar copias de respaldo de la información contenida en el banco de datos de participantes (incumple con lo establecido en el artículo 40 del Reglamento de la Ley N° 29733, Ley de Protección de Datos Personales, aprobado mediante Decreto Supremo N° 003-2013-JUS).

     - Verificarse que los equipos cuentan con los puertos USB habilitados permitiendo la visualización y grabación de archivos, acceso a internet sin restricciones pudiendo acceder a cualquier tipo de páginas incluyendo las de correo personal, lo que genera riesgos de duplicidad de los datos personales (incumpliendo lo establecido en el artículo 43 del Reglamento de la Ley N° 29733, Ley de

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

[4] Folio 37 a 38
[5] Folio 42 a 45
[6] Folio 46
[7] Folio 47 a 51
[8] Folio 54

Protección de Datos Personales, aprobado mediante Decreto Supremo N° 003-2013-JUS).

7. Mediante Oficio N° 301-2017-JUS/DGTAIPD-DFI[9] de fecha 29 de diciembre de 2017, se notificó a la administrada la resolución que inicia el procedimiento administrativo sancionador.

8. Mediante escrito presentado con hoja de tramite 8904-2018MSC[10] y anexos[11] presentado el 08 de febrero de 2018, la administrada presentó su escrito de descargos.

9. Mediante Informe Técnico N° 42-2018-DFI-VARS[12] de fecha 19 de febrero de 2018, se emitió un informe técnico de la Dirección de Fiscalización e Instrucción.

10. Mediante Resolución Directoral Nº 29-2018-JUS/DGTAIPD-DFI[13], de fecha 20 de febrero de 2018, notificada a la administrada con Oficio N° 171-2018-JUS/DGTAIPD-DFI[14], el 09 de marzo de 2018, la Dirección de Fiscalización e Instrucción, en virtud a lo establecido en el artículo 122 del Reglamento de la LPDP, cerró la etapa instructiva del procedimiento administrativo sancionador.

11. Con Informe N° 15-2018-JUS/DGTAIPD-DFI[15] de fecha 20 de febrero de 2018, notificado a la administrada con Oficio N° 171-2018-JUS/DGTAIPD[16] el 13 de marzo de 2018, la DFI emitió el informe final de instrucción recomendando a la Dirección de Protección de Datos Personales imponer sanción administrativa de multa ascendente a una coma cuatro (1,4) U.I.T. a GRM GLOBAL RESEARCH MARKETING S.A.C., por el cargo acotado en el hecho imputado N° 01, por infracción tipificada en el literal a, numeral 1, del artículo 132 del RLPDP: "*Realizar tratamiento de datos personales incumpliendo las medidas de seguridad establecidas en el normativa sobre la materia*".

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

[9] Folio 54
[10] Folio 56 a 64
[11] Folio 65 a 130
[12] Folio 132 a 133
[13] Folio 134 a 135
[14] Folio 150
[15] Folio 137 a 141
[16] Folio 150

II. Competencia

12. 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 (ROF del MINJUS), derogando el Decreto Supremo N° 011-2012-JUS.

13. 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.

14. 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.

15. 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 Ley N° 29733, Ley de Protección de Datos Personales (LPDP) y a su reglamento, aprobado mediante Decreto Supremo N° 003-2013-JUS, (RLPDP).

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

III. Normativa sancionadora aplicable

16. 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).

17. 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.

18. Por su parte, el presente procedimiento sancionador se inició estando vigente el artículo 38 de la LPDP.

19. Entonces, el sistema jurídico ha permitido una excepción en torno al principio de irretroactividad[17] en materia penal y administrativo sancionador, conocido como la retroactividad benigna.

---

[17] **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. (El subrayado es nuestro)
(...)"

20. 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 destipificación 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.

21. 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.

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

22. 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.

23. Sobre la obligación de implementar las medidas de seguridad de la información de acuerdo a lo establecido en la LPDP y su Reglamento:

Norma	Regulación anterior	Regulación actual
Sustantiva	Obligación regulada en el artículo 39, 40 y 43 del Reglamento de la LPDP, aprobado mediante Decreto Supremo N° 003-2013-JUS, en	Obligación regulada en el artículo 39, 40 y 43 del Reglamento de la LPDP, aprobado mediante Decreto Supremo N° 003-2013-JUS, en

	concordancia con el artículo 9 de la LPDP.	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.

24. En atención a lo anterior, cabe señalar que el incumplimiento de implementar las medidas de seguridad de la información, 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 (26 de enero de 2017), toda vez que actualmente la sanción conforme a la tipificación resulta más beneficiosa al haber cambiado de grave a leve.

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

En ese sentido, en virtud de la excepción al principio de irretroactividad (retroactividad benigna) establecido en el artículo 246 del TUO de la LPAG[18], 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, 40 y 43 del Reglamento de la LPDP, al no haber implementados las medidas de seguridad de la información establecidas por tales normas.

[18] **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.
(...)"

25. 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[19] 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.

26. Asimismo, se debe atender a lo dispuesto en el artículo 126[20] 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

27. Dicho artículo debe leerse conjuntamente con lo previsto en el numeral 2 del artículo 255[21] de la LPAG, que establece como condición atenuante el reconocimiento de la responsabilidad por parte del infractor de forma expresa y por escrito, debiendo

---

[19] **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."

[20] **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"

[21] **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."

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

28. Para emitir pronunciamiento en el presente caso, se debe determinar si la administrada al momento de la fiscalización no habría cumplido con implementar las medidas de seguridad de la información consistentes en:

a. No documentar los procedimientos de gestión de accesos, gestión de privilegios y verificación periódica de privilegios asignados, incumpliendo lo establecido en el numeral 1 del artículo 39 del RLPDP.

b. No generar ni mantener registros de evidencias producto de la interacción lógica con su sistema, incumpliendo lo establecido en el numeral 2 del artículo 39 del RLPDP.

c. Encontrarse el centro de datos en un área común, sin gabinetes para el servidor que se encuentra en el piso, el ambiente no cuenta con control de temperatura adecuado, UPS (sistema de alimentación ininterrumpida), extintor, tablero electrónico ni puerta con llave, incumpliendo lo establecido en el artículo 40 del RLPDP.

d. No realizar copias de respaldo de la información contenida en el banco de datos de participantes, incumpliendo con lo establecido en el artículo 40 del RLPDP.

e. Los equipos cuentan con los puertos USB habilitados permitiendo la visualización y grabación de archivos, acceso a internet sin restricciones pudiendo acceder a cualquier tipo de páginas incluyendo las de correo personal, lo que genera riesgos de duplicidad de los datos personales, incumpliendo lo establecido en el artículo 43 del RLPDP.

Como consecuencia del análisis de los hechos antes acotados, corresponde determinar si 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*".

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

<u>Sobre el deber de cumplir con las medidas de seguridad</u>

29. Se imputa a la administrada que no habría implementado las medidas de seguridad de la información establecidas en los artículos 39, 40 y 43 del RLPDP, por haber incurrido presuntamente en los hechos descritos en el numeral 28 de la presente resolución; configurándose la infracción leve tipificada en el literal a. del numeral 1 del artículo 132 del Reglamento de la LPDP consistente 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.

30. Previo a ello, es preciso recordar que el artículo 9 de la LPDP señala el principio de seguridad como uno 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."*

31. Asimismo, 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."*

Sobre el incumplimiento del numeral 1 del artículo 39 del RLPDP

32. Se imputa a la administrada que no habría documentado los procedimientos de gestión de accesos, gestión de privilegios y verificación periódica de privilegios asignados a los usuarios del sistema, de acuerdo al numeral 1 del artículo 39 del RLPDP.

33. Respecto de las medidas de seguridad a adoptarse en el tratamiento de datos personales en soporte 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."

34. De lo anterior se desprende que es obligatorio definir procedimientos documentados de gestión de accesos y gestión de privilegios de los usuarios para el acceso al sistema, la identificación de usuarios en el sistema, así como el proceso de verificación periódica de dichos privilegios, esto es, se debe establecer el procedimiento para el alta, baja y modificación de datos, modificación de usuarios, así como sus privilegios en el sistema.

35. Del Acta de Fiscalización N° 01-2017[22] en la cual se deja constancia de la supervisión realizada a la administrada el día 26 de enero de 2017, se indica lo siguiente:

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

"(...) Se verificaron las medidas de seguridad en la computadora asignada al procurador (donde se realiza el tratamiento de datos personales), verificándose lo siguiente:
(...) La entidad supervisada manifestó que no realiza ni cuenta con documentación referente a la verificación periódica de privilegios asignados, asimismo, indicó que no cuenta con procedimientos documentados referentes a la gestión de accesos y la gestión de privilegios (...)."

36. Con Informe N° 017-2017-DSC-ORQR[23] de fecha 29 de marzo de 2017, se informó sobre la visita de fiscalización a la administrada indicando lo siguiente:

"IV. Conclusiones
(...)
2.GRM Global Research Marketing S.A.C. no ha documentado el procedimiento de verificación periódica de privilegios asignados.
3. GRM Global Research Marketing S.A.C. no ha documentado los procedimientos de gestión de accesos y gestión de los usuarios. (...)".

37. Mediante el Informe N° 026-2017-DSC-VARS[24] de fecha 24 de abril de 2017, se informó sobre el cumplimiento de las medidas de seguridad de la administrada, indicando lo siguiente:

"III. Conclusiones
1. GRM Global Research Marketing S.A.C. no ha documentado los procedimientos de gestión de accesos, gestión de privilegios y revisión periódica de privilegios (...)."

[22] Folio 17 a 22
[23] Folio 27 a 26
[24] Folio 37 a 38

38. Posteriormente, mediante Informe N° 051-2017-JUS/DGPDP-DSC[25] de fecha 26 de mayo de 2017, se emiten las conclusiones sobre el procedimiento de fiscalización a la administrada, indicando lo siguiente:

> *"(...) 21. GRM Global Research Marketing S.A.C. señaló no tener documentados los procedimientos de gestión de accesos, gestión de privilegios y revisión periódica de privilegios (...).*
> *IV.Conclusiones*
> *2. GRM Global Research Marketing S.A.C. no cuenta con las medidas de seguridad necesarias 'para la protección de datos personales, de acuerdo con las exigencias de la LPDP y su reglamento. (...)."*

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

39. De los informes descritos se desprende que al momento de la fiscalización el 26 de enero de 2017, la administrada no había implementado las medidas de seguridad consistentes en la documentación de gestión de accesos, gestión de privilegios y revisión periódica de privilegios de acuerdo a lo establecido en el numeral 1 del artículo 39 del RLPDP.

40. Posteriormente, la administrada presentó sus descargos el 08 de febrero de 2018[26], reconociendo haber cometido el hecho imputado, e indicando que implementó las medidas de seguridad a través del protocolo de seguridad de estudios cualitativos[27] que contienen la descripción de la gestión de accesos y privilegios, y la periodicidad de la verificación de los mismos, y el mecanismo de control de accesos y privilegios[28], documentos que adjunta al escrito; solicitó además que se considere tales acciones de enmienda como atenuantes al graduar la sanción de acuerdo al artículo 126 del RLPDP.

41. A fin de verificar la implementación de las medidas de seguridad declaradas en el escrito antes citado, la DFI emitió el Informe Técnico Complementario N° 42-2018-DFI-VARS[29] de fecha 19 de febrero de 2018, evaluando si las medidas descritas

[25] Folio 42 a 46
[26] Folio 56 a 64
[27] Folio 75 a 94
[28] Folio 96 a 109
[29] Folio 132 a 133

cumplían la normativa vulnerada, siendo que para el hecho imputado en este caso concluyo lo siguiente:

> *"(…) III. Conclusiones*
> *1. GRM Global Research Marketing S.A.C. ha cumplido con la obligación de documentar los procedimientos de gestión de accesos, gestión de privilegios y revisión periódica de privilegios asignados (…)."*

42. Tal como se aprecia de los descargos formulados sobre el incumplimiento de las medidas de seguridad consistentes en la documentación de procedimientos de gestión de accesos, gestión de privilegios y revisión periódica de privilegios; de la revisión de los documentos que se adjunta para acreditar el cumplimiento de dichas medidas, y del informe técnico antes descrito que evalúa las mismas; se observa que el incumplimiento imputado fue subsanado el 08 de febrero de 2018, con la implementación del protocolo de seguridad de estudios cualitativos[30]y el mecanismo de control de accesos y privilegios[31].

43. En tal sentido, habiéndose verificado que las acciones realizadas por la administrada para la implementación de las medidas de seguridad, se acreditaron a partir del 08 de febrero de 2018, esto es con fecha posterior al inicio del procedimiento sancionador, se configura el supuesto de acción de enmienda establecido en el artículo 126 del Reglamento de la LPDP, debiendo considerarse como atenuante al graduar la sanción a imponer.

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

Sobre el incumplimiento del numeral 2 del artículo 39 del RLPDP

44. Se imputa a la administrada que no habría generado ni mantenido registro de evidencias producto de la interacción lógica con su sistema, de acuerdo al numeral 2 del artículo 39 del RLPDP.

45. Respecto de las medidas de seguridad a adoptarse en el tratamiento de datos personales en soporte 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:*
>
> *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. (…)."*

46. De lo anterior se desprenden que es obligatorio generar y mantener registros que provean evidencia sobre las interacciones con el sistema, 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.

---

[30] Folio 75 a 94
[31] Folio 96 a 109

47. Del Acta de Fiscalización N° 01-2017[32] en la cual se deja constancia de la supervisión realizada a la administrada el día 26 de enero de 2017, se indica lo siguiente:

> *"(...) Se verificaron las medidas de seguridad en la computadora asignada al procurador (donde se realiza el tratamiento de datos personales), verificándose lo siguiente:*
> *(...) se verificó que no genera ni mantiene registro de interacción lógica con el banco de datos personales de participantes en estudios cualitativos."*

48. Con Informe N° 017-2017-DSC-ORQR[33] de 29 de marzo de 2017, se informó sobre la visita de fiscalización a la administrada indicando lo siguiente:

> *"IV. Conclusiones*
> *(...)*
> *4. GRM Global Research Marketing S.A.C. no genera registros de interacción lógica con el banco de datos automatizado de participantes en estudios cualitativos."*

49. Por Informe N° 026-2017-DSC-VARS[34] de 24 de abril de 2017, se emite informe sobre el cumplimiento de las medidas de seguridad de la administrada, indicando lo siguiente:

> *"III. Conclusiones*
> *2. GRM Global Research Marketing S.A.C. no genera ni mantiene registros de evidencias productos de la interacción lógica de las bases de datos automatizada (...)."*

50. Posteriormente, mediante Informe N° 051-2017-JUS/DGPDP-DSC[35] de fecha 26 de mayo de 2017, se emiten las conclusiones sobre el procedimiento de fiscalización a la administrada, indicando lo siguiente:

---

[32] Folio 17 a 22
[33] Folio 27 a 36
[34] Folio 37 a 38
[35] Folio 42 a 46

> *"(...) 22. Se verificó que GRM Global Research Marketing S.A.C. no genera ni mantiene registros de evidencias producto de la interacción lógica de las bases de datos automatizada (...)."*
> *IV.Conclusiones*
> *2. GRM Global Research Marketing S.A.C. no cuenta con las medidas de seguridad necesarias ´para la protección de datos personales, de acuerdo con las exigencias de la LPDP y su reglamento. (...)."*

51. De los informes descritos se desprende que al momento de la fiscalización el 26 de enero de 2017, la administrada no había implementado las medidas de seguridad consistentes en la generación de registros de evidencias de la interacción lógica que realiza con la base de datos automatizada, de acuerdo a lo establecido en el numeral 2 del artículo 39 del RLPDP.

52. Posteriormente, la administrada presentó sus descargos el 08 de febrero de 2018[36], reconociendo haber cometido el hecho imputado, e indicando que implementó las medidas de seguridad requeridas a través de un sistema informático que realiza la revisión de logs indicando fecha, usuario y acción realizada[37], documento que adjunta al escrito; solicitó además que se considere tal acción de enmienda como atenuante al graduar la sanción de acuerdo al artículo 126 del RLPDP.

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

53. A fin de verificar la implementación de las medidas de seguridad declaradas en el escrito antes citado, la DFI emitió el Informe Técnico Complementario N° 42-2018-DFI-VARS[38] de fecha 19 de febrero de 2018, evaluando si las medidas descritas cumplían la normativa vulnerada, siendo que para el hecho imputado en este caso concluyo lo siguiente:

> *"(...) III. Conclusiones*
> *2. GRM Global Research Marketing S.A.C. ha cumplido con generar y mantener registros de interacción lógica respecto su sistema que realiza tratamiento de datos personales (...)."*

54. Tal como se aprecia de los descargos formulados sobre el incumplimiento de las medidas de seguridad consistentes en generar y mantener registros de la interacción lógica que se realiza con las base de datos personales, de la revisión de los documentos que se adjunta para acreditar el cumplimiento de dichas medidas, y del informe técnico antes descrito que evalúa las mismas; se observa que el incumplimiento imputado fue subsanado el 08 de febrero de 2018, con la implementación del sistema informático que realiza la revisión de logs, indicando fecha, usuario y acción realizada[39].

55. En tal sentido, habiéndose verificado que las acciones realizadas por la administrada para la implementación de las medidas de seguridad, se acreditaron a partir del 08 de febrero de 2018, esto es con fecha posterior al inicio del procedimiento sancionador, se configura el supuesto de acción de enmienda establecido en el artículo 126 del Reglamento de la LPDP, debiendo considerarse como atenuante al graduar la sanción a imponer.

---

[36] Folio 56 a 64
[37] Folio 110 a 111
[38] Folio 132 a 133
[39] Folio 110 a 111

Sobre el incumplimiento del artículo 40 del RLPDP

56. Se imputa a la administrada que no habría implementado medidas de seguridad para su centro de datos, ya que este se encontraba en un área común, sin gabinetes para el servidor que estaba en el piso, el ambiente no cuenta con control de temperatura adecuado, UPS (sistema de alimentación ininterrumpida), extintor, tablero electrónico ni puerta con llave; de acuerdo al artículo 40 del RLPDP.

57. Respecto de las medidas de seguridad a adoptarse en el tratamiento de datos personales en soporte automatizado, el Reglamento de la LPDP señala lo siguiente:

> *"**Artículo 40.- Conservación, respaldo y recuperación de los datos personales.***
> *Los ambientes en los que se procese, almacene o transmita la información deberán ser implementados, con controles de seguridad apropiados, tomando como referencia las recomendaciones de seguridad física y ambiental recomendados en la "NTP ISO/IEC 17799 EDI. Tecnología de la Información. Código de Buenas Prácticas para la Gestión de Seguridad de la Información." en la edición que se encuentre vigente."*

58. De lo anterior se desprende que para el tratamiento de datos personales en soportes automatizados, entre ellos el almacenamiento, es necesario implementar ambientes que cuenten con controles de seguridad adecuados que cautelen la información de que se trate.

59. Del Acta de Fiscalización N° 01-2017[40] en la cual se deja constancia de la supervisión realizada a la administrada el día 26 de enero de 2017, se indica lo siguiente:

> *"(...) Se verificaron las medidas de seguridad del ambiente donde se encuentra el servidor de datos verificándose lo siguiente: 1) El servidor de datos se encuentra ubicado en un área común con la oficina de sistemas (no posee un ambiente aislado) y se encuentra ubicada en el piso de dicho ambiente, no posee base ups, extintor, tablero eléctrico, ni puerta con llave (...)."*

[40] Folio 17 a 22

60. Con Informe N° 017-2017-DSC-ORQR[41] de 29 de marzo de 2017, se informó sobre la visita de fiscalización a la administrada indicando lo siguiente:

> *"IV. Conclusiones*
> *(...)*
> *5. GRM Global Research Marketing S.A.C. dispone de ambiente (centro de datos), donde se almacena, procesa, transmite información de datos personales de participantes en estudios cualitativos sin los controles de seguridad apropiados.*

61. Por Informe N° 026-2017-DSC-VARS[42] de fecha 24 de abril de 2017, se emite informe sobre el cumplimiento de las medidas de seguridad de la administrada, indicando lo siguiente:

> *"III. Conclusiones*
> *3. GRM Global Research Marketing S.A.C. dispone de un ambiente donde se almacena, procesa, transmite información de datos personales, el centro de datos no cuenta con las medidas de seguridad adecuadas (...)".*

62. Posteriormente, mediante Informe N° 051-2017-JUS/DGPDP-DSC[43] de fecha 26 de mayo de 2017, se emiten las conclusiones sobre el procedimiento de fiscalización a la administrada, indicando lo siguiente:

> *"(...) 23. Respecto a controlar la seguridad de los ambientes en los que se almacena, procesa o transmita información de datos personales, se verificó que el centro de datos de GRM Global Research Marketing S.A.C. no cuenta con las medidas de seguridad necesarias (...)."*
> *IV.Conclusiones*
> *2. GRM Global Research Marketing S.A.C. no cuenta con las medidas de seguridad necesarias 'para la protección de datos personales, de acuerdo con las exigencias de la LPDP y su reglamento. (...)."*

63. De los informes descritos se desprende que al momento de la fiscalización el 26 de enero de 2017, la administrada no había implementado las medidas de seguridad consistentes en controles de seguridad para los ambientes en los que se procese, almacene o transmita información, de acuerdo a lo establecido en el artículo 40 del RLPDP.

64. Posteriormente, la administrada presentó sus descargos el 08 de febrero de 2018[44], reconociendo haber cometido el hecho imputado, e indicando que implementó las medidas de seguridad requeridas a través de la remodelación del dataroom de GRM[45], documento que adjunta al escrito; solicitó además que se considere tal acción de enmienda como atenuante al graduar la sanción de acuerdo al artículo 126 del RLPDP.

65. A fin de verificar la implementación de las medidas de seguridad declaradas en el escrito antes citado, la DFI emitió el Informe Técnico Complementario N° 42-2018-DFI-VARS[46] de 19 de febrero de 2018, evaluando si las medidas descritas cumplían

[41] Folio 27 a 36
[42] Folio 37 a 38
[43] Folio 42 a 46
[44] Folio 56 a 64
[45] Folio 112 a 121
[46] Folio 132 a 133

la normativa vulnerada, siendo que para el hecho imputado en este caso concluyo lo siguiente:

> *"(...) III. Conclusiones*
> *3. GRM Global Research Marketing S.A.C. ha cumplido con implementar las medidas de seguridad requerida en el primer párrafo del artículo 40 del Reglamento de la LPDP (...)."*

66. Tal como se aprecia de los descargos formulados sobre el incumplimiento de las medidas de seguridad consistentes en implementar ambientes que cuenten con controles de seguridad adecuados para cautelar la información que se procese, de la revisión de los documentos que se adjunta para acreditar el cumplimiento de dichas medidas, y del informe técnico antes descrito que evalúa las mismas; se observa que el incumplimiento imputado fue subsanado el 08 de febrero de 2018, con la remodelación del dataroom[47].

67. En tal sentido, habiéndose verificado que las acciones realizadas por la administrada para la implementación de las medidas de seguridad, se acreditaron a partir del 08 de febrero de 2018, esto es con fecha posterior al inicio del procedimiento sancionador, se configura el supuesto de acción de enmienda establecido en el artículo 126 del Reglamento de la LPDP, debiendo considerarse como atenuante al graduar la sanción a imponer.

Sobre el incumplimiento del artículo 40 del RLPDP

68. Se imputa a la administrada que no habría implementado las medidas de seguridad consistentes en realizar copias de respaldo de la información contenida en el banco de datos de participantes, de acuerdo al artículo 40 del RLPDP.

69. Respecto de las medidas de seguridad a adoptarse en el tratamiento de datos personales en soporte automatizado, el Reglamento de la LPDP señala lo siguiente:

[47] Folio 112 a 121

> *"**Artículo 40.- Conservación, respaldo y recuperación de los datos personales.***
> *(...)*
> *Adicionalmente, se deben contemplar los mecanismos de respaldo de seguridad de la información de la base de datos personales con un procedimiento que contemple la verificación de la integridad de los datos almacenados en el respaldo, incluyendo cuando sea pertinente, la recuperación completa ante una interrupción o daño, garantizando el retorno al estado en el que se encontraba al momento en que se produjo la interrupción o daño.*

70. De lo anterior se desprende que para el tratamiento de datos personales en soportes automatizados, es necesario implementar mecanismos de respaldo de seguridad de la información de la base de datos personales.

71. Del Acta de Fiscalización N° 01-2017[48] en la cual se deja constancia de la supervisión realizada a la administrada el día 26 de enero de 2017, se indica lo siguiente:

> *"(...) Se verificaron las medidas de seguridad del ambiente donde se encuentra el servidor de datos verificándose lo siguiente: (...) La Entidad supervisada manifestó que no realiza copias de respaldo del banco de datos personales de participantes en estudios cualitativos (...)."*

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

72. Con Informe N° 017-2017-DSC-ORQR[49] de fecha 29 de marzo de 2017, se informó sobre la visita de fiscalización a la administrada indicando lo siguiente:

> *"IV. Conclusiones*
> *(...)*
> *6.GRM Global Research Marketing S.A.C. no garantiza el respaldo de la información correspondiente al banco de datos personales de participantes en estudios cualitativos.*

73. Por Informe N° 026-2017-DSC-VARS[50] de fecha 24 de abril de 2017, se emite informe sobre el cumplimiento de las medidas de seguridad de la administrada, indicando lo siguiente:

> *"III. Conclusiones*
> *4. GRM Global Research Marketing S.A.C. no garantiza el respaldo de la información de datos personales de participantes en estudios cualitativos a través de la generación de copias seguras y continuas (...)."*

74. Posteriormente, mediante Informe N° 051-2017-JUS/DGPDP-DSC[51] de fecha 26 de mayo de 2017, se emiten las conclusiones sobre el procedimiento de fiscalización a la administrada, indicando lo siguiente:

> *"(...) 24. Se verificó que GRM Global Research Marketing S.A.C. no realiza copias de respaldo del banco de datos personales, no garantizando el respaldo de la información a través de la generación de copias seguras y continuas (...).*
> *IV.Conclusiones*

[48] Folio 17 a 22
[49] Folio 27 a 36
[50] Folio 37 a 38
[51] Folio 42 a 46

2. GRM Global Research Marketing S.A.C. no cuenta con las medidas de seguridad necesarias para la protección de datos personales, de acuerdo con las exigencias de la LPDP y su reglamento. (…).”

75. De los informes descritos se desprende que al momento de la fiscalización el 26 de enero de 2017, la administrada no había implementado las medidas de seguridad consistentes en implementar respaldos de seguridad de la información al no generar copias seguras, de acuerdo a lo establecido en el segundo párrafo del artículo 40 del RLPDP.

76. Posteriormente, la administrada presentó sus descargos el 08 de febrero de 2018[52], reconociendo haber cometido el hecho imputado, e indicando que implementó las medidas de seguridad requeridas a través del procedimiento de realización de copias de respaldo descrito en el protocolo de seguridad de estudios cualitativos[53], documentos que adjunta al escrito; solicitó además que se considere tal acción de enmienda como atenuante al graduar la sanción de acuerdo al artículo 126 del RLPDP.

77. A fin de verificar la implementación de las medidas de seguridad declaradas en el escrito antes citado, la DFI emitió el Informe Técnico Complementario N° 42-2018-DFI-VARS[54] de fecha 19 de febrero de 2018, evaluando si las medidas descritas cumplían la normativa vulnerada, siendo que para el hecho imputado en este caso concluyo lo siguiente:

“(…) III. Conclusiones
4. GRM Global Research Marketing S.A.C. ha evidenciado la realización de copias de respaldo referidas al cumplimiento con lo dispuesto en el segundo párrafo del artículo 40° del Reglamento de la LPDP (…).”

78. Tal como se aprecia de los descargos formulados sobre el incumplimiento de las medidas de seguridad consistentes en implementar respaldos de seguridad de la información a través de la generación de copias seguras y continuas, de la revisión de los documentos que se adjunta para acreditar el cumplimiento de dichas medidas,

[52] Folio 56 a 64
[53] Folio 123 a 125, 75 a 94
[54] Folio 132 a 133

y del informe técnico antes descrito que evalúa las mismas; se observa que el incumplimiento imputado fue subsanado el 08 de febrero de 2018, con el procedimiento de realización de copias de respaldo descrito en el protocolo de seguridad de estudios cualitativos[55].

79. En tal sentido, habiéndose verificado que las acciones realizadas por la administrada para la implementación de las medidas de seguridad, se acreditaron a partir del 08 de febrero de 2018, esto es con fecha posterior al inicio del procedimiento sancionador, se configura el supuesto de acción de enmienda establecido en el artículo 126 del Reglamento de la LPDP, debiendo considerarse como atenuante al graduar la sanción a imponer.

Sobre el incumplimiento del artículo 43 del RLPDP

80. Se imputa a la administrada que no habría implementado las medidas de seguridad consistentes en controles de seguridad para garantizar que las copias o reproducciones de documentos se realicen únicamente por personal autorizado, de acuerdo al artículo 43 del RLPDP.

81. Respecto de las medidas de seguridad a adoptarse en el tratamiento de datos personales en soporte automatizado, el Reglamento de la LPDP señala 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. (...)."*

82. De lo anterior se desprende que las copias generadas o la reproducción de documentos solo se podrán realizar bajo el control de personal autorizado, lo cual debe ser garantizado a través de la adopción de medidas de seguridad adecuadas para tal fin.

83. Del Acta de Fiscalización N° 01-2017[56] en la cual se deja constancia de la supervisión realizada a la administrada el día 26 de enero de 2017, se indica lo siguiente:

> *"(...) Se verificaron las medidas de seguridad en la computadora asignada al procurador donde se realiza el tratamiento de datos personales, verificándose lo siguiente: (...) 3) Cuenta con los puertos USB habilitados (permite la visualización y grabación de archivos).*

84. Con Informe N° 017-2017-DSC-ORQR[57] de fecha 29 de marzo de 2017, se informó sobre la visita de fiscalización a la administrada indicando lo siguiente:

> *"IV. Conclusiones*
> *(...)*
> *7. No tiene implementada una medida de seguridad que restrinja la generación de copias o reproducción de documentos (...)."*

[55] Folio 123 a 125, 75 a 94
[56] Folio 17 a 22
[57] Folio 27 a 36

85. Mediante Informe N° 026-2017-DSC-VARS[58] de fecha 24 de abril de 2017, se emite informe sobre el cumplimiento de las medidas de seguridad de la administrada, indicando lo siguiente:

> *"III. Conclusiones*
> *5. GRM Global Research Marketing S.A.C. no establece procedimientos que restrinjan la generación de copias o reproducción de documentos, incumpliendo el artículo 43 del Reglamento de la LPDP.*

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

86. Posteriormente, mediante Informe N° 051-2017-JUS/DGPDP-DSC[59] de fecha 26 de mayo de 2017, se emiten las conclusiones sobre el procedimiento de fiscalización a la administrada, indicando lo siguiente:

> *"(...) 25. Se verificó que GRM Global Research Marketing S.A.C. no establece procedimientos que restrinjan la generación de copias o reproducción de documentos, incumpliendo el artículo 43 del Reglamento de la LPDP (...).*
> *IV.Conclusiones*
> *2. GRM Global Research Marketing S.A.C. no cuenta con las medidas de seguridad necesarias para la protección de datos personales, de acuerdo con las exigencias de la LPDP y su reglamento. (...)."*

87. De los informes descritos se desprende que al momento de la fiscalización el 26 de enero de 2017, la administrada no había implementado las medidas de seguridad consistentes en controles de seguridad que garanticen la copia o reproducción de documentos únicamente por parte de personal autorizado, de acuerdo a lo establecido en el artículo 43 del RLPDP.

88. Posteriormente, la administrada presentó sus descargos el 08 de febrero de 2018[60], reconociendo haber cometido el hecho imputado, e indicando que implementó las medidas de seguridad requeridas a través de la instalación de una herramienta que permite inhabilitar los puertos USB y que se describe en el protocolo de seguridad de estudios cualitativos[61], documentos que adjunta al escrito; solicitó además que se

[58] Folio 37 a 38
[59] Folio 42 a 46
[60] Folio 56 a 64
[61] Folio 123 a 125, 75 a 94

considere tal acción de enmienda como atenuante al graduar la sanción de acuerdo al artículo 126 del RLPDP.

89. A fin de verificar la implementación de las medidas de seguridad declaradas en el escrito antes citado, la DFI emitió el Informe Técnico Complementario N° 42-2018-DFI-VARS[62] de fecha 19 de febrero de 2018, evaluando si las medidas descritas cumplían la normativa vulnerada, siendo que para el hecho imputado en este caso concluyó lo siguiente:

> *"(...) III. Conclusiones*
> *5. GRM Global Research Marketing S.A.C. ha evidenciado la implementación de medidas de seguridad referidas al cumplimiento con lo dispuesto en el artículo 43° del Reglamento de la LPDP."*

90. Tal como se aprecia de los descargos formulados sobre el incumplimiento de las medidas de seguridad consistentes en implementar mecanismos de control de reproducción de copias de documentos a fin de que sea realizado solo por parte del personal autorizado, de la revisión de los documentos que se adjunta para acreditar el cumplimiento de dichas medidas, y del informe técnico antes descrito que evalúa las mismas; se observa que el incumplimiento imputado fue subsanado el 08 de febrero de 2018, con la herramienta que permite inhabilitar los puertos USB y que se describe en el protocolo de seguridad de estudios cualitativos[63].

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

91. En tal sentido, habiéndose verificado que las acciones realizadas por la administrada para la implementación de las medidas de seguridad, se acreditaron a partir del 08 de febrero de 2018, esto es con fecha posterior al inicio del procedimiento sancionador, se configura el supuesto de acción de enmienda establecido en el artículo 126 del Reglamento de la LPDP, debiendo considerarse como atenuante al graduar la sanción a imponer.

92. En consecuencia, habiendo quedado acreditado que al momento de la fiscalización de 26 de enero de 2017, no se habían implementados las medidas de seguridad establecidas en los numerales 1 y 2 del artículo 39, el primer y segundo párrafo del artículo 40 y el artículo 43 del RLPDP, incumplimientos normativos que además han sido reconocidos por la administrada, se ha configurado la infracción leve tipificada en el literal a. del numeral 1 del artículo 132 del Reglamento de la LPDD consistente en: "*Realizar tratamiento de datos personales incumpliendo las medidas de seguridad establecidas en la normativa sobre la materia*".

93. No obstante lo anterior, también se verifica que se realizaron acciones de enmienda subsanando los incumplimientos normativos advertidos, con posterioridad al inicio del procedimiento sancionador, por lo que corresponde considerarlos como atenuantes al momento de imponer la sanción que corresponda.

Sobre las sanciones a aplicar a los hechos analizados

94. La Tercera Disposición Complementaria Modificatoria del Reglamento del Decreto Legislativo N° 1353, aprobado mediante Decreto Supremo N° 019-2017-JUS[64], de

[62] Folio 132 a 133

[63] Folio 123 a 125, 75 a 94

[64] **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

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.

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

95. 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[65], sin perjuicio de las medidas correctivas que puedan determinarse de acuerdo a lo establecido en el artículo 118 del Reglamento de la LPDP[66].

96. 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:

Incorpórese 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."

[65] **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)."

[66] **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 Nº 27444, Ley del Procedimiento Administrativo General.
Asimismo, sin perjuicio de la sanción administrativa que corresponda por una infracción a las disposiciones contenidas en la Ley y el presente reglamento, se podrán dictar, cuando sea posible, medidas correctivas destinadas a eliminar, evitar o detener los efectos de las infracciones."

(i) 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 la administrada no había implementado las medidas de seguridad consistentes en:

(a) Documentar los procedimientos de gestión de accesos, gestión de privilegios y verificación periódica de privilegios asignados, de acuerdo a lo establecido en el numeral 1 del artículo 39 del RLPDP.

(b) Generar y mantener registros de evidencias producto de la interacción lógica con su sistema, incumpliendo lo establecido en el numeral 2 del artículo 39 del RLPDP.

(c) Contar con áreas especiales y resguardadas para el almacenamiento de centros de datos, de acuerdo a lo establecido en el artículo 40 del RLPDP.

(d) Realizar copias de respaldo de la información contenida en el banco de datos de participantes, de acuerdo a lo establecido en el artículo 40 del RLPDP.

(e) Contar con mecanismos de control que garanticen que la copia o reproducción de documentos se realice solo por parte de personal autorizado, de acuerdo a lo establecido en el artículo 43 del RLPDP.

Infracción leve 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[67], sin perjuicio de las medidas correctivas a determinarse según el artículo 118 del Reglamento de la LPDP[68].

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

97. 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

---

[67] **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).
(...)".

[68] **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."

administrativa, por lo que la sanción deberá ser proporcional al incumplimiento calificado como infracción, observando para ello los criterios que dicha disposición señala para su graduación.

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

a) El beneficio ilícito resultante por la comisión de las infracciones:

No se ha evidenciado un beneficio ilícito resultante de la comisión de la infracción cometida.

b) La probabilidad de detección de la infracción:

Respecto a la comisión de la infracción imputada 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:

La infracción detectada afecta 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 la infracción imputada.

Tal infracción afecta el derecho de los ciudadanos a que se dé un tratamiento adecuado de sus datos personales.

d) El perjuicio económico causado:

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

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

e) La reincidencia en la comisión de la infracción:

GRM GLOBAL RESEARCH MARKETING S.A.C. 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:

Se encuentra acreditada la comisión de la infracción imputada, no obstante , también se han acreditado acciones de enmienda sobre la implementación de las medidas de seguridad establecidas en los artículos 39, 40 y 43 del RLPDP cuyo incumplimiento se imputa, las cuales constituyen atenuantes a ser consideradas al momento de graduar la sanción a imponer.

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.

99. 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 la infracción que a continuación se cita, correspondiéndole además la imposición de sanción en el rango que se describe de la siguiente forma:

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

No implementar las medidas de seguridad de la información de acuerdo a la normativa de protección de datos personales, consistentes en:

a. Documentar los procedimientos de gestión de accesos, gestión de privilegios y verificación periódica de privilegios asignados, de acuerdo a lo establecido en el numeral 1 del artículo 39 del RLPDP.

b. Generar y mantener registros de evidencias producto de la interacción lógica con su sistema, incumpliendo lo establecido en el numeral 2 del artículo 39 del RLPDP.

c. Contar con áreas especiales y resguardadas para el almacenamiento de centros de datos, de acuerdo a lo establecido en el artículo 40 del RLPDP.

d. Realizar copias de respaldo de la información contenida en el banco de datos de participantes, de acuerdo a lo establecido en el artículo 40 del RLPDP.

e. Contar con mecanismos de control que garanticen que la copia o reproducción de documentos se realice solo por parte de personal autorizado, de acuerdo a lo establecido en el artículo 43 del RLPDP.

Tales hechos constituyen 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.

100. 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 98 de la presente resolución directoral.

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

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:

Artículo 1.- Sancionar a **GRM GLOBAL RESEARCH MARKETING S.A.C.** con RUC 20511826421 con la multa ascendente a una coma cuatro unidades impositivas tributarias **(1,4 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 la administrada al momento de la fiscalización no había cumplido con implementar las siguientes medidas de seguridad: a) No documentar los procedimientos de gestión de accesos, gestión de privilegios y verificación periódica de privilegios asignados (incumple lo establecido en el numeral 1 del artículo 39 del RLPDP); b) No generar ni mantener registros de evidencias producto de la interacción lógica con su sistema (incumple lo establecido en el numeral 2 del artículo 39 del RLPDP); c) Encontrarse el centro de datos en un área común, sin gabinetes para el servidor que se encuentra en el piso, el ambiente no cuenta con control

de temperatura adecuado, UPS (sistema de alimentación ininterrumpida), extintor, tablero electrónico ni puerta con llave (incumple lo establecido en el artículo 40 del RLPDP); d) No realizar copias de respaldo de la información contenida en el banco de datos de participantes (incumple con lo establecido en el artículo 40 del RLPDP); e) Verificarse que los equipos cuentan con los puertos USB habilitados permitiendo la visualización y grabación de archivos, acceso a internet sin restricciones pudiendo acceder a cualquier tipo de páginas incluyendo las de correo personal, lo que genera riesgos de duplicidad de los datos personales (incumpliendo lo establecido en el artículo 43 del RLPDP).

Artículo 2.- Notificar a **GRM GLOBAL RESEARCH MARKETING S.A.C.** 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[69].

Artículo 3.- Informar a **GRM GLOBAL RESEARCH MARKETING S.A.C.** 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[70].

Artículo 4.- Notificar a **GRM GLOBAL RESEARCH MARKETING S.A.C** la presente resolución, en su domicilio sito en: Av. Pardo y Aliaga N° 699, Oficina N° 802, Distrito de San Isidro, Departamento de Lima.

Regístrese y comuníquese.

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

---

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

[70] **Decreto Supremo Nº 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 íntegro de la multa impuesta."