Resolución Directoral N° 546-2020-JUS/DGTAIPD-DPDP

Lima, 14 febrero de 2020

Expediente N°
118-2018-JUS-DPDP-PS

VISTOS:

El Informe Nº 75-2019-JUS/DGTAIPD-DFI[1] del 28 de junio de 2019, emitido por la Dirección de Fiscalización e Instrucción de la Dirección General de Transparencia, Acceso a la Información Pública y Protección de Datos Personales (en adelante, DFI), y demás documentos que obran en el respectivo expediente, y;

CONSIDERANDO:

I. Antecedentes

1. El 02 de mayo de 2018, personal de la DFI tomó conocimiento de la página web de IBR PERÚ S.A. (www.ibrlatam.com)[2].

2. Mediante Orden de Visita de Fiscalización Nº 045-2018-JUS/DGTAIPD-DFI[3], del 3 de abril de 2018, la DFI dispuso la realización de una visita de fiscalización a IBR PERU S.A. (en adelante, la administrada).

3. Mediante Acta de Fiscalización N° 01-2018[4], se deja constancia de los hallazgos encontrados durante la visita de supervisión realizada a las instalaciones de la administrada el 7 de mayo de 2018, en su domicilio en calle las Orquídeas N° 103, piso 6, Surquillo, Lima.

4. Mediante Acta de Fiscalización N° 02-2018[5], se deja constancia de los hallazgos encontrados durante la visita de supervisión realizada a las instalaciones de la administrada el 21 de mayo de 2018, en su domicilio en calle las Orquídeas N° 103, piso 6, Surquillo, Lima.

5. Con documento ingresado con registro N° 35289[6] de fecha 01 de junio de 2018 la administrada presentó documentación sobre las medidas de seguridad.

M. GONZALEZ

[1] Folio 235 a 240
[2] Folio 2 al 18
[3] Folio 19
[4] Folio 20 al 29
[5] Folio 40 al 51
[6] Folio 112 al 122

6. Con documento ingresado con registro N° 37961[7] de fecha 14 de junio de 2019 la administrada señala que en Perú no cuentan con clave para accesos a la plataforma del sitio web, toda vez que dicha página fue creada por accionistas chilenos.

7. Mediante Informe Técnico N° 146-2018-DFI-ORQR[8] del 22 de junio de 2018, el Analista de Fiscalización en Seguridad de la Información informa sobre la evaluación del cumplimiento de las medidas de seguridad por parte de la administrada.

8. Mediante el correo electrónico del 24 de julio de 2018, el personal a cargo del Registro Nacional de Protección de Datos Personales informó que la administrada contaba con los bancos de "TRABAJADORES", "PROVEEDORES", "CLIENTES", "VIDEOVIGILANCIA", "POSTULANTES" y "VISITANTES", así como no tenía registrada ninguna comunicación de flujo transfronterizo, ni solicitud pendiente de atención[9].

9. Con Proveído del 13 de setiembre de 2018[10] la DFI resuelve ampliar el plazo de la fiscalización por 45 días hábiles adicionales.

10. Mediante Informe de Fiscalización N° 156-2018-JUS/DGTAIPD-DFI-AARM[11] del 31 de octubre del 2018, se remitió a la DFI el resultado de la fiscalización realizada, adjuntando las actas de fiscalización, así como los demás anexos y documentos que conforman el respectivo expediente.

11. Mediante Resolución Directoral N° 78-2019-JUS/DGTAIPD-DFI[12] del 21 de mayo del 2019, la DFI resolvió iniciar procedimiento administrativo sancionador a la administrada, por la siguiente infracción:

    - No haber implementado las medidas de seguridad para el tratamiento de los datos personales al: No documentar el procedimiento de verificación periódica de privilegios asignados, incumpliendo con lo dispuesto en el numeral 1 del artículo 39 del Reglamento de la LPDP respectivamente; configurándose 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 de la materia".*

12. Mediante Oficio N° 415-2019-JUS/DGTAIPD-DFI[13] recibido por la administrada el 28 de mayo de 2019, se notificó dicha resolución directoral.

13. Mediante escrito y anexos presentados el 18 de junio de 2019 con hoja de trámite 43151-2019MSC[14], la administrada presentó sus descargos.

---

[7] 125 al 126
[8] Folio 127 a 135
[9] Folio 136 a 137
[10] Folio 138
[11] Folio 149 a 154
[12] Folio 161 a 168
[13] Folio 169 a 170
[14] Folio 171 a 229

14. Mediante Informe Técnico N° 111-2019-DFI-ORQR[15] de 26 de junio de 2019 el Analista de Fiscalización en Seguridad de la Información informa sobre la evaluación de la implementación a las medidas de seguridad de la administrada.

15. Mediante Resolución Directoral N° 116-2019-JUS/DGTAIPD-DFI[16] de 28 de junio de 2019, la DFI dio por concluidas las actuaciones instructivas correspondientes al procedimiento sancionador.

16. Mediante Informe N° 75-2019-JUS/DGTAIPD-DFI[17] de 28 de junio de 2019, la DFI emitió el Informe Final de Instrucción, remitiendo a la Dirección de Protección de Datos Personales de la Dirección General de Transparencia, Acceso a la Información Pública y Protección de Datos Personales (en adelante, la DPDP) los actuados para que resuelva en primera instancia el procedimiento administrativo sancionador iniciado, recomendando lo siguiente:

    - Imponer sanción administrativa de multa ascendente a dos coma cinco (2,5) UIT por infracción leve tipificada en el literal a), numeral 1, del artículo 132 del Reglamento de la LPDP: *"Realizar tratamiento de datos personales incumpliendo las medidas de seguridad establecidas en la normativa de la materia".*

II. Competencia

17. Conforme con lo dispuesto en el artículo 74 del Reglamento de Organización y Funciones del Ministerio de Justicia y Derechos Humanos, aprobado por Decreto Supremo N° 013-2017-JUS, la DPDP es la unidad orgánica competente para resolver en primera instancia, los procedimientos administrativos sancionadores iniciados por la DFI.

18. En tal sentido, la autoridad que debe conocer el presente procedimiento sancionador, a fin de emitir resolución en primera instancia, es la directora de Protección de Datos Personales.

III. Normas concernientes a la responsabilidad de la administrada

19. Acerca de la responsabilidad de la administrada, se deberá tener en cuenta que el literal f) del numeral 1 del artículo 257 del Texto Único Ordenado de la Ley N° 27444, Ley del Procedimiento Administrativo General, aprobado por Decreto Supremo Nº 004-2019-JUS, en adelante LPAG, establece como una causal eximente de la responsabilidad por infracciones, la subsanación voluntaria del hecho imputado como infractor, si es realizada de forma previa a la notificación de imputación de cargos[18].

20. Asimismo, se debe atender a lo dispuesto en el artículo 126 del Reglamento de la LPDP, que considera como atenuantes la colaboración con las acciones de la autoridad y el reconocimiento espontáneo de las infracciones conjuntamente con la

---

[15] Folio 231
[16] Folio 232 a 233
[17] Folio 235 a 240
[18] **Texto Único Ordenado de la Ley N° 27444, Ley del Procedimiento Administrativo General, aprobado por Decreto Supremo Nº 004-2019-JUS**
"Artículo 257.- Eximentes y atenuantes de responsabilidad por infracciones
1.- Constituyen condiciones eximentes de la responsabilidad por infracciones las siguientes:
(...)
f) La subsanación voluntaria por parte del posible sancionado del acto u omisión imputado como constitutivo de infracción administrativa, con anterioridad a la notificación de la imputación de cargos a que se refiere el inciso 3) del artículo 255."

adopción de medidas de enmienda; dichas atenuantes, de acuerdo con la oportunidad del reconocimiento y las fórmulas de enmienda, pueden permitir la reducción motivada de la sanción por debajo del rango previsto en la LPDP[19].

21. Dicho artículo debe leerse conjuntamente con lo previsto en el numeral 2 del artículo 257 de la LPAG[20], 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

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

- Si la administrada no ha implementado las medidas de seguridad para el tratamiento de datos personales: al no documentar el procedimiento de verificación periódica de privilegios asignados Obligación establecida en el numeral 1 del artículo 39° del Reglamento, en consecuencia, 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 de la materia"*.

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

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

23. Se imputa a la administrada, a través de la Resolución Directoral N° 78-2019-JUS/DGTAIPD-DFI, la infracción leve tipificada en el literal a. del numeral 1, del artículo 132 del Reglamento de la LPDP, al presuntamente no haber implementado las medidas de seguridad para el tratamiento de datos personales, al no documentar el procedimiento de verificación periódica de privilegios asignados Obligación establecida en el numeral 1 del artículo 39° del Reglamento.

24. 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.

25. Al respecto, es preciso mencionar que el artículo 9° de la LPDP señala el principio de seguridad como uno de los principios rectores de la protección de datos personales:

---

[19] **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"

[20] **Texto Único Ordenado de la Ley N° 27444, Ley del Procedimiento Administrativo General, aprobado por Decreto Supremo N° 004-2019-JUS**
"Artículo 257.- Eximentes y atenuantes de responsabilidad por infracciones
(...)
2.- Constituyen condiciones atenuantes de la responsabilidad por infracciones las siguientes:
a) Si iniciado un procedimiento administrativo sancionador el infractor reconoce su responsabilidad de forma expresa y por escrito.
En los casos en que la sanción aplicable sea una multa esta se reduce hasta un monto no menor de la mitad de su importe.
b) Otros que se establezcan por norma especial."

> ***"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."*

26. 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."*

Sobre el incumplimiento del numeral 1 del artículo 39° del Reglamento de la LPDP

27. Se imputa a la administrada que no habría documentado el procedimiento de verificación periódica de privilegios asignados a los usuarios del sistema, de acuerdo al numeral 1 del artículo 39 del Reglamento de la LPDP.

28. 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."*

29. 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.

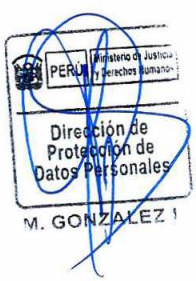
30. En el Acta de Fiscalización N° 02-2018[21] en la cual se deja constancia de la fiscalización de 21 de mayo de 2018, se indica lo siguiente:

[21] Folio 40 al 51

"(...) c) Se verificó que los agentes de cobranzas cuentan con usuarios de inicio de sesión del sistema operativo compartido, sin embargo, el acceso al sistema mitrol y al módulo de cobranza, el usuario es personal de acuerdo al privilegio asignado, d) Se verifico que los agentes de cobranzas no pueden realizar llamadas a los clientes de Avon, sin que el controlador le asigne una llamada de manera aleatoria. (...) Se verificó que la base de datos se alojan los registros de las cuentas del sistema Mitrol (inicio, cierre de sesión y acciones relevantes (...)".

31. Con Informe Técnico N° 146-2018-DFI-ORQR de 22 de junio de 2018[22], se informó sobre la visita de fiscalización a la administrada indicando lo siguiente:

"(...)
IV Evaluación del cumplimiento de las Medidas de Seguridad
(...)
2. Respecto a la obligación de tener documentos los procedimientos de gestión de accesos, gestión de privilegios y verificación periódica de privilegios asignados. Se verificó que IBR PERU S.A. cuenta con procedimientos documentados referentes a la gestión de accesos y gestión de privilegios los mismos que se encuentran incluidos en los documentos denominados "Procedimientos para acceso de la red corporativa por parte de los usuarios" (f. 118 a 120) y "Perfiles de acceso de usuarios" (f. 121); sin embargo no cuenta con procedimientos documentados respecto a la verificación periódica de privilegios asignados, Por lo que estaría incumpliendo con el numeral 1 del artículo 39° del Reglamento de la LPDP, el cual indica "Los sistemas informáticos que manejan bancos de datos personales incluyendo la gestión de los privilegios de dicho usuario, la identificación del usuario ante el sistema, la gestión de los privilegios de dicho usuario, la identificación del usuario ante el sistema, entre los que se encuentran usuario contraseña, uso de certificado digital, 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". En ese sentido, IBR PERU S.A. incumple con la disposición mencionada.
(...)
V. Conclusiones
2. IBR PERU S.A. no documenta el procedimiento de verificación periódica de privilegios asignados, incumpliendo con el numeral 1 del artículo 39° del Reglamento de la LPDP.
(...)"



32. Con fecha posterior, se emitió el Informe de Fiscalización N° 156-2018-JUS/DGTAIPD-DFI-AARM[23], que recoge las conclusiones sobre la fiscalización realizada, indicando lo siguiente:

"VI. Conclusiones
Cuarta: no contaría con las medidas de seguridad requeridas por el artículo 39° (numeral 1) del Reglamento de la LPDP al no documentar la verificación periódica de privilegios asignados. Hecho que constituiría una presunta infracción según lo dispuesto 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", dicha infracción es leve conforme al citado artículo".

[22] Folio 127 a 135
[23] Folio 149 a 154

33. De lo citado, se colige que la administrada no había implementado las medidas de seguridad establecidas en el numeral 1 del artículo 39° del Reglamento de la LPDP, consistentes en documentar los procedimientos de verificación periódica de privilegios, lo que motivo su inclusión en uno de los supuestos infractores imputados en la Resolución Directoral N° 78-2019-JUS/DGTAIPD-DFI.

34. Con escrito ingresado el 18 de junio de 2019 la administrada señalando que se atribuye una acción tipificada en el reglamento, lo cual no tiene rango de ley.

35. Sobres los argumentos de la administrada corresponde señalar que serán materia de análisis en el siguiente punto, no obstante, se evaluarán los medios probatorios presentados por la administrada.

36. Sobre la infracción materia de imputación con fecha 26 de junio de 2019 se emitió el Informe Técnico N° 111-2019-DFI-ORQR[24] de fecha 28 de mayo de 2019 indicando lo siguiente:

"(...)
3. Al respecto, luego de haber realizado la revisión y el análisis correspondiente a la documentación remitida por la administrada en sus descargos presentados el 18 de junio de 2019, se puede determinar que no ha evidenciado contar con procedimientos documentados referentes a la verificación periódica de privilegios asignados ya que no proporciona información que evidencie de manera específica la realización de una verificación periódica a los privilegios a los privilegios otorgados a todos los usuarios del sistema y/o servicios a través de los cuales realiza el tratamiento de datos personales. cabe precisar que la referida verificación debe estar contemplada dentro de un procedimiento documentado en el cual además se debe indicar la frecuencia y/o intervalo de tiempo en el cual se realiza. Por lo que estaría incumpliendo con el numeral 1 del artículo 39° del Reglamento de la LPDP.
III. CONCLUSIÓN
IBR PERÚ S.A., no ha evidenciado contar con procedimientos documentados respecto a la verificación periódica de privilegios asignados. Por lo tanto, no cumple con lo establecido en el numeral 1 del artículo 39° del Reglamento de la LPDP.
(...)"

Dirección de Protección de Datos Personales
M. GONZALEZ

37. Luego, con el escrito de descargos de fecha 12 de julio de 2019[25], la administrada señala lo siguiente:

- Al haber presentado el documento denominado **"IBR.PR1692. Como realizar revisión periódica de privilegios asignados en el sistema IBR"** de fecha 26 de diciembre de 2018 cumple con documentar los procedimientos respecto a la verificación periódica de privilegios asignados, ya que en dicho documento se establece expresamente que los procedimientos de verificación periódica de privilegios asignados se efectúan con periodicidad mensual y están a cargo del área de Tecnología de la Información.
- Por otro lado, señala que existe una infracción al principio de tipicidad, debido a que se atribuye la acción típica en un reglamento que no tiene rango de Ley, y que no se puede disponer el inicio del procedimiento imputando una infracción tipificada en un reglamento y no en una norma con rango de Ley.

[24] Folio 231
[25] Folio 241 a 277

- Asimismo, indica haber documentado los procedimientos de verificación periódica de privilegios asignados antes de la imputación de cargos.
- Es decir, la administrada manifiesta haber implementado las medidas de seguridad con fecha 26 de diciembre de 2018.

38. Con fecha 20 de diciembre de 2019 se emitió el Informe Técnico N° 284-2019-DFI-ORQR el cual señala lo siguiente:

> *V. Conclusiones*
> 1. *IBR PERU S.A. ha evidenciado contar con procedimientos respecto a la verificación periódica de privilegios asignados. Por lo tanto, cumple con lo establecido en el numeral 1 del artículo 39° del Reglamento de la LPDP.*
> *(...)"*

39. Entonces, se tiene que la administrada documentaba la verificación periódica de privilegios acreditando con el documento denominado "IBR.PR1692. Como realizar revisión periódica de privilegios asignados en sistemas IBR" luego del análisis a dichos documentos se determinó que ha evidenciado contar con procedimientos documentados referentes a la verificación periódica de privilegios asignados, toda vez que, la información proporcionada por la administrada evidencia de manera específica la realización de una verificación periódica a los privilegios a todos los usuarios de los sistemas y/o servicios a través de los cuales realiza el tratamiento de datos personales en cumplimento a lo dispuesto en el numeral 1 del artículo 39 del reglamento de la LPDP

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

40. Por lo que se tiene que la administrada habría realizada acciones de enmienda al subsanar dicha conducta lo cual, será tomada en cuenta al momento de graduar la sanción.

Sobre la supuesta ilegalidad de la norma bajo la cual se pretende sancionar a la administrada

41. La administrada, en su escrito de descargos presentado el día 18 de junio de 2019, señala que, la norma bajo la cual se pretende sancionar a la administrada es ilegal, dado que las infracciones y sanciones no se encuentran tipificadas en una norma con rango de ley, dado que es el Reglamento y no la Ley, quien tipifica las infracciones para este caso, citó como sustento de dicho argumento casos del Tribunal Constitucional y solicita que la imputación es su contra se declare nula.

42. Posteriormente en los descargos ingresados con fecha 12 de julio de 2019 y 09 de septiembre de 2019, la administrada en ambos escritos manifiesta que la imputación descrita por el Reglamento de la LPDP deviene en inconstitucional, toda vez que vulnera el principio de legalidad y tipicidad.

43. Al respecto, corresponde precisar las particularidades del principio de tipicidad en relación a los alcances del principio de legalidad. El principio de legalidad, refiere al instrumento normativo en el que debe preverse la potestad sancionadora, así como las infracciones y sanciones correspondientes. De otro lado, el principio de tipicidad alude al grado de predeterminación normativa de las conductas típicas proscribiendo supuestos de interpretación extensiva o analógica, es decir, corresponde sancionar un hecho cuando este se encuentre definido y tenga claramente definida su penalidad. Asimismo, el principio de tipicidad no se encuentra sujeto a una reserva de ley absoluta, pues en determinadas situaciones podría ser complementado a través de los reglamentos respectivos.

44. No obstante, la DPDP considera que, habiéndose determinado que la LPDP regula las infracciones y las sanciones respectivas, en sus artículos 38[26] y 39[27], corresponde indicar lo señalado en la Sentencia del Tribunal Constitucional de 10 de noviembre de 2015 (Pleno Jurisdiccional) recaída en los Expedientes N° 0014-2014-P1/TC, 0016-2014-PI/TC, 0019-2014-P1/TC y 0007-2015-PI/TC que indica los siguientes aspectos referidos al principio de legalidad y reserva de ley relativa: .

> *"(...) 180. En esta materia aplica entonces aquella reserva de ley relativa. Por ende, no resulta inconstitucional que se derive al reglamento la tipificación de las infracciones, en tanto se ha fijado en la ley las conductas sancionables y la escala y los tipos de sanción. 181. Por último, cabe añadir que si se regula una actividad con miras a garantizar la calidad del servicio público, resulta necesario dotar al organismo supervisor de las herramientas necesarias para corregir las infracciones que se adviertan en su ámbito específico. 182. De otro lado, y como es obvio, las resoluciones de sanción deberán estar debidamente motivadas, y la sanción que se imponga debe resultar proporcional a la naturaleza y gravedad de la infracción en que haya incurrido. (...)"*

45. Por el principio de tipicidad, las disposiciones reglamentarias de desarrollo solamente pueden "especificar o graduar" aquellas normas dirigidas a identificar las conductas (infracciones) o determinar sanciones, sin constituir nuevas conductas sancionables a las previstas legalmente, salvo los casos en que una ley o decreto legislativo permita tipificar infracciones por norma reglamentaria como se advierte de la normativa que regula la protección de datos personales, específicamente el artículo 38 de la LPDP.

Sobre la fecha cierta de la implementación de las medidas de seguridad por la administrada

1. En sus descargos del 12 de julio de 2020 (Folios 367 a 385), la administrada señala haber implementado las medidas de seguridad con fecha 26 de diciembre de 2018, es decir antes de la imputación de cargos, por tanto, se configura el eximente de responsabilidad.

2. En ese sentido, corresponde determinar la fecha desde la cual se habría tenido por subsanado el incumplimiento normativo.

3. Para determinar la fecha cierta de la implementación de las medidas de seguridad referida a documentar los procedimientos de verificación periódica de privilegios asignados, para ello, es necesario seguir los criterios establecidos en

---

[26] ***"Artículo 38.- Tipificación de infracciones***
Las infracciones se clasifican en leves, graves y muy graves, las cuales son tipificadas vía reglamentaria, de acuerdo a lo establecido en el numeral 4) del artículo 230 de la Ley N° 27444, Ley del Procedimiento Administrativo General, mediante Decreto Supremo con el voto aprobatorio del Consejo de Ministros. (...)".

[27] ***"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).
(...)
La Autoridad Nacional de Protección de Datos Personales determina la infracción cometida y el monto de la multa imponible mediante resolución debidamente motivada. Para la graduación del monto de las multas, se toman en cuenta los criterios establecidos en el artículo 230, numeral 3), de la Ley 27444, Ley del Procedimiento Administrativo General, o la que haga sus veces. (...)"

el artículo 245° del Código Procesal Civil respecto de la fecha cierta de los documentos presentados:

> ***Artículo 245.- Fecha cierta.***
> *Un documento privado adquiere fecha cierta y produce eficacia jurídica como tal en el proceso desde:*
> *1.- La muerte del otorgante.*
> *2.- La presentación del documento ante funcionario público.*
> *3.- La presentación del documento ante notario público, para que certifique la fecha o legalice las firmas.*
> *4.- La difusión a través de un medio público de fecha determinada o determinable.*
> *5.- Otros casos análogos.*
> *Excepcionalmente, el Juez puede considerar como fecha cierta la que haya sido determinada por medios técnicos que le produzcan convicción.*

4. Al carecer de certificación de fecha o legalización de firmas o de difusión en fecha determinable, la única fecha que puede considerarse como cierta para acreditar tal implementación del citado documento denominado "IBR.PR1692. Como realizar revisión periódica de privilegios asignados en sistemas IBR" es la de su presentación en mesa de partes, es decir el 12 de julio de 2019.

5. Asimismo, conviene señalar también que, para contar con el respaldo del principio de presunción de veracidad, es necesario que la información declarada cumpla el requisito establecido en el artículo 67° del TUO de la LPAG, en los siguientes términos:

> ***Artículo 67.- Deberes generales de los administrados en el procedimiento***
> *Los administrados respecto del procedimiento administrativo, así como quienes participen en él, tienen los siguientes deberes generales:*
> *(...)*
> *4. Comprobar previamente a su presentación ante la entidad, la autenticidad de la documentación sucedánea y de cualquier otra información que se ampare en la presunción de veracidad.*

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

6. Por consiguiente, corresponde considerar la implementación de las medidas de seguridad referidas a documentar los procedimientos de verificación periódica de privilegios asignados se realizó con fecha posterior a la imputación de cargos, toda vez que la resolución de inicio del procedimiento sancionador fue notificada el 28 de mayo de 2019, no obstante dado que, la administrada a la fecha ha cumplido con lo dispuesto en el numeral 1 del artículo 39° del Reglamento de la LPDP se debe considerar como un atenuante de responsabilidad.

7. En conclusión, a la fecha de emitir la presente resolución la conducta imputada a la administrada se encuentra debidamente subsanada, por lo tanto, dicha conducta debe ser tomada en cuenta al momento de imponer la sanción.

Sobre las sanciones a aplicar a los hechos analizados

46. La Tercera Disposición Complementaria Modificatoria del Reglamento del Decreto Legislativo N° 1353, aprobado mediante Decreto Supremo N° 019-2017-JUS[28], del

[28] **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 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

15 de septiembre del 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.

47. 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[29], sin perjuicio de las medidas correctivas que puedan determinarse de acuerdo con el artículo 118 del Reglamento de la LPDP[30].

48. En el presente caso se ha determinado la comisión de la siguiente infracción:

(i) No haber implementado las medidas de seguridad para el tratamiento de los datos personales al: No documentar el procedimiento de verificación periódica de privilegios asignados incumpliendo con los dispuesto en el numeral 1 del artículo 39 del Reglamento de la LPDP; configurándose la infracción leve tipificada en el literal a. del numeral 1 del artículo 132 de dicho reglamento: *"Realizar tratamiento de datos personales incumpliendo las medidas de seguridad establecidas en la normativa de la materia".*

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

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

50. 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 la infracción:</u>

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

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."

[29] **Ley N° 29733, Ley de Protección de Datos Personales**
"Artículo 39. Sanciones administrativas
En caso de violación de las normas de esta Ley o de su reglamento, la Autoridad Nacional de Protección de Datos Personales puede aplicar las siguientes multas:
1. Las infracciones leves son sancionadas con una multa mínima desde cero coma cinco de una unidad impositiva tributaria (UIT) hasta cinco unidades impositivas tributarias (UIT).
2. Las infracciones graves son sancionadas con multa desde más de cinco unidades impositivas tributarias (UIT) hasta cincuenta unidades impositivas tributarias (UIT).
3. Las infracciones muy graves son sancionadas con multa desde más de cincuenta unidades impositivas tributarias (UIT) hasta cien unidades impositivas tributarias (UIT)."

[30] **Reglamento de la Ley de Protección de Datos Personales, aprobado por Decreto Supremo Nº 003-2013-JUS**
"Artículo 118.- Medidas cautelares y correctivas.
Una vez iniciado el procedimiento sancionador, la Dirección de Sanciones podrá disponer, mediante acto motivado, la adopción de medidas de carácter provisional que aseguren la eficacia de la resolución final que pudiera recaer en el referido procedimiento, con observancia de las normas aplicables de la Ley Nº 27444, Ley del Procedimiento Administrativo General.
Asimismo, sin perjuicio de la sanción administrativa que corresponda por una infracción a las disposiciones contenidas en la Ley y el presente reglamento, se podrán dictar, cuando sea posible, medidas correctivas destinadas a eliminar, evitar o detener los efectos de las infracciones."

b) La probabilidad de detección de la infracción:

En lo concerniente al incumplimiento en la adopción de las medidas de seguridad previstas el numeral 1 del artículo 39° del Reglamento de la LPDP, referidas a no haber implementado los procedimientos de verificación periódica de los privilegios asignados, debe señalarse que dichos hechos se detectaron durante la visita de fiscalización realizada, al ser concerniente a operaciones internas de la administrada, con lo que se tiene que su probabilidad de detección es baja.

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

sobre la no aplicación de medidas de seguridad al tratamiento de los datos personales que maneja, implica que efectúa un tratamiento en el que no se tuvo el suficiente control de los procedimientos de verificación periódica de los privilegios asignados a cada usuario en particular, lo que incrementa el riesgo de afectación a la confidencialidad, disponibilidad e integridad de los datos personales.

d) El perjuicio económico causado:

No se ha evidenciado un perjuicio económico causado resultante de la comisión de la infracción.

e) La reincidencia en la comisión de la infracción:

La administrada no es reincidente, ya que no ha sido sancionada en alguna otra ocasión por la infracción analizada.

f) Las circunstancias de la comisión de la infracción:

En lo concerniente a la inobservancia de medidas de seguridad, debe precisarse que la administrada presentó documentación a fin de acreditar la subsanación de dicha conducta, lo cual es un hecho considerable como una enmienda que activa la atenuación de responsabilidad contemplada en el artículo 126 del Reglamento de la LPDP.

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

En el caso de la infracción, se evidenció acciones de la administrada tendientes a corregir su conducta, dado que, a la fecha al administrada ha cumplido con implementar las medidas de seguridad conforme a los dispuesto en el numeral 1 del artículo 39° del Reglamento de la LPDP.

51. Es pertinente indicar que para imponer la sanción se tendrá en cuenta la suma de todos los criterios que permiten graduar la sanción conforme a los argumentos desarrollados en el considerando 78 de la presente resolución directoral.

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

SE RESUELVE:

Artículo 1.- Sancionar a **IBR PERÚ S.A.** con la multa ascendente a uno coma cinco unidades impositivas tributarias **(1,5 UIT)** por la comisión de la infracción leve tipificada en literal a) numeral 1 del artículo 132 del Reglamento de la LDPD: *"Realizar tratamiento de datos personales incumpliendo las medidas de seguridad establecidas en la normativa de la materia".*

Articulo 3.- Notificar a **IBR PERÚ S.A.** que contra la presente resolución, de acuerdo a lo indicado en el artículo 218 de la LPAG, proceden los recursos de reconsideración o apelación dentro de los quince (15) días hábiles posteriores a su notificación[31].

Artículo 4.- Informar a **IBR PERÚ S.A.** 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 entenderá que cumplió con pagar la multa impuesta, si antes de que venza el plazo mencionado, cancela el 60% de la multa impuesta conforme a lo dispuesto en el artículo 128° del RLPDP[32].

Artículo 5.- Notificar a **IBR PERÚ S.A.** la presente resolución

Regístrese y comuníquese.

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

[31] **Texto Único Ordenado de la Ley N° 27444, Ley del Procedimiento Administrativo General, aprobado por Decreto Supremo Nº 004-2019-JUS**
"Artículo 218. Recursos administrativos
218.1 Los recursos administrativos son:
a) Recurso de reconsideración
b) Recurso de apelación
Solo en caso que por ley o decreto legislativo se establezca expresamente, cabe la interposición del recurso administrativo de revisión.
218.2 El término para la interposición de los recursos es de quince (15) días perentorios, y deberán resolverse en el plazo de treinta (30) días."

[32] **Reglamento de la Ley de Protección de Datos Personales, aprobado por Decreto Supremo Nº 003-2013-JUS**
"Artículo 128.- Incentivos para el pago de la sanción de multa.
Se considerará que el sancionado ha cumplido con pagar la sanción de multa si, antes de vencer el plazo otorgado para pagar la multa, deposita en la cuenta bancaria determinada por la Dirección General de Protección de Datos Personales el sesenta por ciento (60%) de su monto. Para que surta efecto dicho beneficio deberá comunicar tal hecho a la Dirección General de Protección de Datos Personales, adjuntando el comprobante del depósito bancario correspondiente. Luego de dicho plazo, el pago sólo será admitido por el íntegro de la multa impuesta."