Resolución Directoral Nro. 49-2020-JUS/DGTAIPD

Lima, 10 de noviembre de 2020

EXPEDIENTE Nro.	:	130-2019-JUS/DGTAIPD-PS.
ADMINISTRADA	:	BANCO DE CRÉDITO DEL PERÚ S.A.
MATERIAS	:	IMPUGNACIÓN DE MEDIDA CORRECTIVA

VISTOS:

El documento de fecha 25 de agosto de 2020, que contiene el recurso de apelación contra la Resolución Directoral Nro. 1169-2020- JUS/DGTAIPD – DPDP de 30 de junio de 2020; y, los demás actuados en el Expediente Nro. 130-2019- JUS/DGTAIPD-PAS.

CONSIDERANDO:

I. ANTECEDENTES

1. Mediante escrito ingresado con Hoja de Trámite Nro. 47126- 2018MSC, la administrada informa a la Autoridad Nacional de Protección de Datos Personales (en adelante, ANPD), la existencia de una brecha de seguridad, en los siguientes términos:

   «El 7 de julio de 2018 identificó un comportamiento inusual en uno de sus aplicativos, hecho que generó sospecha de una intrusión informática. El día 10 de julio de 2018 se confirmó que terceros habían empleado el mecanismo de inyección de código malicioso en el referido aplicativo, permitiendo que, desde una dirección anonimizada, se pueda realizar consultas automatizadas de números de DNI, determinando que el número de consultas realizadas corresponden a treinta

y cuatro mil doscientos cuarenta y dos (34,242), obteniendo a raíz de lo descrito los siguientes datos personales:

- Nombre completo.
- Dirección.
- Correo electrónico.
- Número de tarjetas de crédito, así como número de las cuentas de ahorro, CTS y cuentas corrientes asociadas a las tarjetas de débito.
- Adicionalmente, lograron obtener información sobre los saldos de 21,129 cuentas pertenecientes a 18,305 clientes. BCP señaló que, a pesar de ello, no se efectuaron operaciones fraudulentas en dichas cuentas».

2. Determinada la intrusión informática la administrada procedió a realizar acciones y activar el protocolo frente a la situación producida para evitar se produzcan perjuicios, entre ellos, la comunicación a los clientes y bloqueos temporales o definitivos de las tarjetas de débito.

3. Mediante Oficios Nro. 500-2018-JUS/DGTAIPD-DFI, de 8 de agosto de 2018 y 674-2018-JUS/DGTAIPD-DFI, de 19 de octubre de 2018, la Dirección de Fiscalización e Instrucción (en adelante, DFI) solicitó la siguiente información a la administrada, la misma que fue remitida con documentos ingresados con Hojas de Trámite Nro. 55666-2018MSC de 28 de agosto de 2018 y 70361-2018MSC de 8 de noviembre de 2018.

4. Con fecha 23 de noviembre de 2018, la administrada comunicó a la Dirección de Protección de Datos Personales, mediante escrito ingresado con Hoja de Trámite Nro. 74313-2018MSC, otra brecha de seguridad, en la que informó lo siguiente:

   (i) El 12 de noviembre de 2018 identificó que se estaba produciendo la sustracción de información (datos personales) de sus clientes a través de uno de sus aplicativos por parte de terceras personas.
   (ii) De la revisión realizada, se encontró que desde una IP externa, a través de un BOT (robot) que contaba con un «APIKEY» (llave), se estaba permitiendo el ingreso a la infraestructura del BCP a fin de capturar datos personales de clientes, las consultas identificadas corresponden a un millón ciento dieciséis mil doscientos cuarenta y dos (1'116,242), de los cuales se obtuvo, principalmente, la siguiente información:

   - Nombre completo.
   - Fecha de nacimiento.
   - Dirección.
   - Correo electrónico.
   - Número de tarjetas de débito, así como número de las cuentas de ahorro, CTS y cuentas corrientes asociadas a las tarjetas de débito.

- Número de tarjetas de crédito.
- Segmento de banca.
- Fecha de apertura de las tarjetas.
- Fecha de renovación de las tarjetas.
- Fecha de vencimiento de las tarjetas.
- *Status* de las tarjetas (bloqueo, confirmada, por asignar, etc.).
- Usuario de token.
- Fecha, hora, tipo y código de la última operación realizada por la tarjeta (apertura, bloqueo, cambio, etc.).
- Código de sucursal o agencia de la última operación realizada por la tarjeta.
- Código del promotor de servicios de la última operación realizada por la tarjeta, entre otros datos.

5. Además, mencionó que los terceros no obtuvieron información sobre saldos, movimientos y/o líneas de crédito de los clientes y que no se efectuaron operaciones fraudulentas en dichas cuentas. Asimismo, indicó que una vez determinada la existencia de la intrusión informática, procedió a aplicar el protocolo establecido por el banco para casos de intrusiones informáticas, entre las cuales realizó comunicaciones a los clientes, ya sea por llamadas telefónicas, correos o SMS, informándoles que terceros accedieron a la información personal y de sus cuentas y/o tarjetas.

6. Con Proveído de 7 de febrero de 2019, la DFI dispuso iniciar actuaciones de fiscalización a la administrada, a fin de verificar las medidas técnicas y organizativas implementadas respecto a las brechas de seguridad comunicadas a la ANPD. Para tal efecto, mediante la Orden de Visita de Fiscalización Nro. 014-2019-JUS/DGTAIPD-DFI, la DFI dispuso la realización de visitas de fiscalización, a fin de verificar si dicha entidad, en el desarrollo de sus actividades, cumplía con la Ley Nro. 29733, Ley de Protección de Datos Personales (en adelante, la LPDP) y su reglamento, aprobado por Decreto Supremo Nro. 003-2013-JUS (en adelante, el reglamento de la LPDP).

7. Las visitas de fiscalización se realizaron los días 8, 14 y 25 de febrero, así como el 5 de marzo de 2019, dejando constancia de estas en las Actas de Fiscalización Nros. 01, 02, 03 y 04-2019.

8. Mediante Informe Técnico Nro. 52-2019-DFI-VARS de 26 de marzo de 2019, referente a la evaluación de la implementación de medidas de seguridad respecto a las intrusiones informáticas comunicadas por la administrada, el analista de fiscalización en seguridad de la información concluyó que después de las brechas de seguridad notificadas por el BCP (intrusiones informáticas notificadas el 26 de julio de 2018 y 23 de noviembre de 2018), se verificó que, si bien la entidad había implementado un proceso de respuesta de incidentes, este no había sido

totalmente satisfactorio, al evidenciarse que no se habría implementado la medida de seguridad referente a los registros de interacción lógica para el tratamiento de datos personales, obligación establecida en el numeral 2 del artículo 39 del Reglamento de la LPDP.

9. Con Hoja de Trámite Nro. 53295-2019MSC, de fecha 25 de julio de 2019, la administrada remitió información adicional respecto a las comunicaciones realizadas a la Autoridad:

   (i) Informó que tomó conocimiento de que terceros no autorizados disponían de información personal y de saldos de las cuentas de mil ciento setenta y seis (1,176), siendo que el noventa y ocho por ciento (98%) de los mismos coincide con los clientes cuya información fue comprometida en la intrusión informática del 12 de noviembre de 2018.
   (ii) Indicó que no fueron comprometidas las claves de las tarjetas y que hasta la fecha no se produjeron operaciones fraudulentas en perjuicio de dichas cuentas.
   (iii) Informó que comunicó a los clientes afectados lo sucedido, indicándoles que en el eventual caso que se diera alguna operación no autorizada en sus cuentas con motivo de este incidente, el BCP respondería y reconocería las pérdidas asociadas a dicha operación.
   (iv) Informó que puso a disposición de sus clientes la activación de un sistema que permitía recibir informes en su correo electrónico de todas las transacciones asociadas a las cuentas y productos que tienen en el BCP.

10. Por medio del Informe de Fiscalización Nro. 131-2019-JUS/DGTAIPD-DFI-AARM de 21 de agosto de 2019, se concluye que se han determinado con carácter preliminar las circunstancias que justifican la instauración de un procedimiento administrativo sancionador, el mismo que fue notificado a la administrada mediante Oficio Nº 759-2019-JUS/DGTAIPD-DFI, el 13 de septiembre de 2019.

11. Mediante Resolución Directoral Nro. 242-2019-JUS/DGTAIPD-DFI de 2 de diciembre de 2019 (en adelante, la RD de Inicio), la DFI dispone el inicio del procedimiento administrativo sancionador a la administrada; resolución que fue notificada mediante Oficio Nro. 994-2019-JUS/DGTAIPD-DFI, el 4 de diciembre de 2019.

12. La DFI resolvió iniciar procedimiento administrativo sancionador a la administrada, por la presunta comisión de los siguientes hechos infractores:

   (i) La administrada no habría cumplido con implementar las medidas de seguridad para el tratamiento de datos personales de sus clientes, al no generar ni mantener registros de interacción lógica respecto del banco de

datos personales de clientes en soporte automatizado; obligación establecida en el numeral 2 del artículo 39 del Reglamento de la LPDP.

(ii) La administrada no habría garantizado la confidencialidad de los datos personales de sus clientes, al permitir a terceros no autorizados el acceso a estos; obligación establecida en el artículo 17 de la LPDP.

13. Con Hoja de Trámite Nro. 90716-2019MSC de fecha 26 de diciembre de 2019, la administrada presentó sus descargos.

14. La DFI emite Informe Técnico Nro. 03-2020-DFI-ORQR de 6 de enero de 2020, con el fin de complementar el análisis y evaluación de la implementación de las medidas de seguridad por parte de la administrada, en función a la información remitida por el BCP en sus descargos.

15. Con Proveído de 15 de enero de 2020, la DFI dispuso correr traslado de los correos electrónicos enviados por cinco ciudadanos clientes del BCP a la administrada para que se pronuncie sobre el contenido de los mismos en el plazo de cinco (5) días hábiles y, asimismo, se le requirió presentar las comunicaciones efectuadas a dichos ciudadanos y enviar una muestra de cien (100) comunicaciones dirigidas a sus clientes como consecuencia de los ataques ocurridos el 7 de julio de 2019 y el 12 de noviembre de 2019. Con Hoja de Trámite Nro. 6047-2020MSC de fecha 28 de enero de 2020, la administrada dio respuesta a lo solicitado.

16. Mediante la Orden de Visita de Fiscalización Nro. 09-2020-JUS/DGTAIPD-DFI de fecha 12 de febrero de 2020, la DFI dispuso la realización de una visita de fiscalización al BCP, a fin de verificar el envío y contenido de los correos electrónicos remitidos a sus clientes como consecuencia de los ataques ocurridos los días 7 de julio y 12 de noviembre de 2018, dejándose constancia de los hechos verificados en el Acta de Fiscalización Nro. 01-2020-PAS, de 12 de febrero de 2020.

17. Con Informe Técnico Nro. 49-2020-DFI-ORQR de 21 de febrero de 2020, la DFI informó sobre la visita de fiscalización del 12 de febrero de 2020 al BCP, concluyendo lo siguiente:

(i) La administrada ha evidenciado haber mantenido comunicación con novecientos sesenta y nueve mil ciento cuarenta y siete (969 147) clientes, afectados por los ataques ocurridos los días 7 de julio y 12 de noviembre de 2018, mediante correos electrónicos y/o mensajes de texto (SMS). No obstante, el número total de correos electrónicos remitidos y/o mensajes de texto (SMS), no corresponde a la totalidad de los clientes afectados.

18. Por medio de la Resolución Directoral Nro. 044-2020-JUS/DGTAIPD-DFI del 10 de marzo de 2020, la DFI dio por concluidas las actuaciones instructivas correspondientes al procedimiento sancionador.

19. Mediante Informe Final de Instrucción Nro. 030-2020-JUS/DGTAIPD-DFI del 10 de marzo de 2020, la DFI remitió a la Dirección de Protección de Datos Personales (en adelante, la DPDP) los actuados para que resuelva en primera instancia el procedimiento administrativo sancionador iniciado, recomendando lo siguiente:

    (i) Imponer una sanción administrativa de multa ascendente a cinco unidades tributarias impositivas (5 UIT) a la administrada por el cargo acotado en el Hecho Imputado Nro. 01, por 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 norma sobre la materia».
    (ii) Imponer sanción administrativa de multa ascendente a cuarenta unidades impositivas tributarias (40 UIT) a la administrada por el cargo acotado en el Hecho Imputado Nro. 02, por la infracción grave tipificada en el literal g) del numeral 2 del artículo 132 del Reglamento de la LPDP: «Incumplir la obligación de confidencialidad establecida en el artículo 17 de la Ley Nro. 29733».

20. El Informe Final de Instrucción Nro. 030-2020-JUS/DGTAIPD-DFI, así como la Resolución Directoral Nro. 044-2020-JUS/DGTAIPD-DFI, fueron notificados a la administrada mediante Oficio Nro. 291-2020-JUS/DGTAIPD-DFI, el día 13 de marzo de 2020.

21. El 31 de julio de 2020, mediante Resolución Directoral Nro. 1169-2020-JUS-DGTAIPD – DPDP, la Dirección de Protección de Datos Personales resuelve:

    (i) Sancionar a BANCO DE CRÉDITO DEL PERÚ S.A., con una multa ascendente a cuarenta unidades impositivas tributarias (40 UIT) por la comisión de la infracción grave tipificada en el literal g), numeral 2, del artículo 132 de reglamento de la LPDP: *«Incumplir la obligación de confidencialidad establecida en el artículo 17 de la Ley Nro. 29733».*

    (ii) Imponer como medida correctiva a BANCO DE CRÉDITO DEL PERÚ S.A acreditar que ha entregado nuevos números de tarjeta a los clientes cuyos números de tarjetas vinculados a sus nombres y/o número de documento de identidad fueron sustraídos en las brechas detectadas en julio y noviembre de 2018, desvinculándolos de los números de tarjeta que fueron sustraídos en dichas brechas.

Dicho cambio no deberá ser cobrado a los clientes afectados.

Para el cumplimiento de tal medida correctiva, se otorga el plazo de ciento veinte (120) días hábiles contados a partir de la notificación que declare consentida o firme la presente Resolución Directoral, debiendo remitir la documentación sustentatoria de su implementación.

22. Por medio de documento de 25 de agosto de 2020, la administrada presentó recurso de apelación contra la Resolución Directoral Nro. 1160-2020-JUS/DGTAIPD-DPDP, alegando lo siguiente:

(i) La Resolución Directoral materia de impugnación resolvió:

«Imponer como medida correctiva al Banco, acreditar que ha entregado nuevos números de tarjeta a los dientes cuyos números de tarjetas vinculados a sus nombres y/o número de documento de identidad fueron sustraídos en las brechas detectadas en julio y noviembre de 2018, desvinculándolos de los números de tarjeta que fueron sustraídos en dichas brechas. Dicho cambio no deberá ser cobrado a los dientes afectados.
Para el cumplimiento de tal medida correctiva se otorga el plazo de ciento veinte (120) días hábiles contados a partir de la notificación que declare consentida o firme la Resolución Directoral, debiendo remitir la documentación sustentatoria de su Implementación».

(ii) Al respecto, considera que la medida correctiva dictada por la DPDP es nula por carecer de motivación, constituye una intromisión en aspectos que no son competencia de la DPDP y no es idónea ni proporcional.

(iii) Con respecto a la nulidad la administrada señala que la DPDP impone la medida correctiva únicamente en su parte resolutiva no existiendo un razonamiento previo en la parte considerativa que desarrolle dicho acto administrativo, con lo cual no se satisface el requisito de motivación de toda decisión administrativa, al no señalar cómo la carga impuesta a la administrada permitirá eliminar o detener los efectos que se atribuyen. Esta ausencia de motivación vulnera el derecho al debido procedimiento en sede administrativa.

(iv) En lo que se refiere a la competencia, la administrada considera que, si alguna medida correctiva tendría que haber ordenado la DPDP esta debió consistir en la implementación de medidas de seguridad adecuadas para superar la debilidad del sistema informático del BCP, pero no debió consistir en el cambio de tarjetas de los clientes afectados, pues esta medida estaría referida a impedir el fraude o una pérdida financiera de los

clientes o salvaguardar o proteger su patrimonio, finalidades que se apartan del derecho de autoderminación informativa que es competencia de la ANPD.

(v) La protección del fraude de los clientes del banco afectado no justifica la imposición de la medida correctiva impuesta, pues la ANPD no es competente materialmente para ello, pues su competencia está circunscrita al adecuado tratamiento de los datos personales y no a las posibles consecuencias que el conocimiento no autorizado de estos datos pueda generar en los titulares, es decir, no tiene arrogada la facultad de proteger a los clientes del Banco para evitar que estos sean víctimas de fraude, con lo cual imponer esta medida correctiva vulnera el principio de legalidad.

(vi) Con respecto a la idoneidad y razonabilidad de la medida, debe tenerse en cuenta que los datos personales a los cuales terceros habrían tenido acceso no permite la realización de acciones fraudulentas con relación al patrimonio de los clientes de la administrada. Ello, porque para materializar tales actos se requiere un conjunto de información concurrente a los cuales los terceros no han tenido acceso. Además, en el supuesto negado en que las acciones fraudulentas se pudieran dar, no podría generarse un daño a nuestros clientes ya que, al no contar con el CVV2 de las tarjetas, el banco podría realizar el contra cargo de dicha operación sin afectar a los clientes.

(vii) Además, debe tenerse en cuenta que es posible que se generen perjuicios a los clientes con el cambio de número de tarjeta, pues estos podrían producir la desafiliación de los cargos recurrentes que tengan habilitados, lo que dada la coyuntura actual puede dificultar la gestión de sus finanzas.

(viii) La administrada ha realizado medidas necesarias para mitigar cualquier afectación y/o daños que fruto de los incidentes se puedan haber generado a los clientes contando con un servicio de ciberinteligencia y monitoreo de la información, lo que contradice lo afirmado en la resolución materia de impugnación respecto a que no se han realizado acciones destinadas a revertir la sustracción de los datos.

(ix) Asimismo, dado que el acceso no autorizado ya se produjo y los datos personales ya fueron conocidos por terceras personas no autorizadas, con lo cual el acceso no autorizado a los datos personales es un hecho consumado que materialmente no se puede revertir, con lo cual la consecuencia lógica es que, si la infracción ya se consumó, no existe medida correctiva que pueda revertir los efectos del hecho infractor.

(x) Llama la atención que la DPDP nos imponga únicamente un cambio en el número de la tarjeta del cliente afectado (sin identificar el tipo de tarjeta), que no es el único dato personal que ha sido adquirido por los terceros, con lo que la decisión la DPDP resulta aleatoria respecto de las otras condiciones afectadas a las que se deja sin la pretendida acción reparadora. Además, existen determinados datos cuya modificación depende de una decisión exclusiva del cliente como el número de tarjeta. Por ello, la forma de revertir las consecuencias que haya generado la exposición de estos datos es la posibilidad de brindar a los administrados la oportunidad de modificar dichos datos, alternativa que el Banco ya dio.

(xi) Al respecto, el BCP afirma que actualmente el 56.50% de las tarjetas afectadas en las brechas de seguridad estarían activas, el resto de las tarjetas a la fecha se encuentra vencidas o han sido bloqueadas por los propios clientes.

(xii) La medida correctiva impuesta por la resolución recurrida no resultaría idónea porque el sólo cambio de tarjeta no eliminaría los supuestos riesgos que la DPDP pretende mitigar porque la brecha de seguridad ya se produjo con lo cual no se pueden revertir sus efectos.

(xiii) La medida correctiva tampoco resulta proporcional a la infracción atribuida y a la sanción pecuniaria impuesta, pues resulta ser extremadamente gravosa y mucho más onerosa que la propia multa. La DPDP no ha efectuado un análisis del costo que implicaría para el banco el cumplimiento de la medida correctiva, pues la renovación de una tarjeta tiene un costo en el material involucrado, además demanda la utilización de maquinaria especializada; supone un proceso de comunicación al cliente para la comunicación del hecho, el reparto o la necesidad de acudir personalmente a la agencia (durante el Estado de Emergencia Nacional) para la entrega; los procesos de activación; los procesos de adecuación de los nuevos números en las plataformas de servicios que el cliente utiliza; débitos automáticos); etc. Y todo ello multiplicado por el número de clientes afectados.

(xiv) Por último, no resulta razonable que en este contexto de pandemia un número de clientes cuyas tarjetas debieran ser cambiadas por esta medida se acerquen a las oficinas del banco a recogerlas exponiendo su salud en el contexto del Estado de Emergencia Sanitaria, en este sentido esta medida contraviene todas las medidas del Estado para evitar la aglomeración de personas.

II. COMPETENCIA

23. Según lo establecido en el inciso 20 artículo 33 de la LPDP, La Autoridad Nacional de Protección de Datos Personales es la encargada de iniciar fiscalizaciones de oficio o por denuncia por presuntos actos contrarios a lo establecido en la Ley y en su reglamento, y de aplicar las sanciones administrativas correspondientes, sin perjuicio de las medidas cautelares o correctivas que establezca el reglamento.

24. Conforme lo dispuesto en el artículo 70 del Reglamento de Organización y Funciones del Ministerio de Justicia y Derechos Humanos, aprobado por Decreto Supremo Nº 013-2017-JUS, la Dirección General de Transparencia, Acceso a la Información Pública y Protección de Datos Personales ejerce la Autoridad Nacional de Protección de Datos Personales.

25. Asimismo, la Dirección General de Transparencia, Acceso a la Información Pública y Protección de Datos Personales es el órgano encargado de resolver en segunda y última instancia administrativa los procedimientos iniciados por la Dirección de Protección de Datos Personales, conforme con lo establecido por el literal l) del artículo 71 del ROF del Ministerio de Justicia y Derechos Humanos.

III. ADMISIBILIDAD

26. El recurso de apelación ha sido interpuesto dentro de los quince (15) días hábiles de notificada la Resolución Directoral Nro. 1169 - 2020-JUS/DGTAIPD-DPDP y cumple con los requisitos previstos en los artículos 218[1] y 220[2] del Texto Único Ordenando de la Ley Nro. 27444, Ley del Procedimiento Administrativo General, por lo que es admitido a trámite.

---

1 **Artículo 218 del TUO de la LPAG.- Recursos administrativos**

218.1 Los recursos administrativos son:
a) Recurso de reconsideración
b) Recurso de apelación
Solo en caso de 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.

2 **Artículo 220 del TUO de la LPAG.- Recurso de apelación**

El recurso de apelación se interpondrá cuando la impugnación se sustente en diferente interpretación de las pruebas producidas o cuando se trate de cuestiones de puro derecho, debiendo dirigirse a la misma autoridad que expidió el acto que se impugna para que eleve lo actuado al superior jerárquico.

IV. CUESTIONES CONTROVERTIDAS

27. De acuerdo con los antecedentes expuestos en el presente procedimiento recursivo, corresponde determinar lo siguiente:

    (i) Si la medida correctiva impuesta es o no nula por la alegada ausencia de motivación en la resolución materia de impugnación.
    (ii) Si la medida correctiva impuesta resulta ser proporcional.

V. CUESTIÓN PREVIA

Sobre la competencia de la Autoridad Nacional de Protección de Datos Personales en lo que respecta a la medida correctiva impuesta mediante la resolución de primera instancia

28. La administrada considera que, si alguna medida correctiva tendría que haber ordenado la DPDP, esta debió consistir en la implementación de medidas de seguridad adecuadas para superar la debilidad del sistema informático del BCP, pero no debió consistir en el cambio de tarjetas de los clientes afectados, pues esta medida estaría referida a impedir el fraude o una pérdida financiera de los clientes o salvaguardar o proteger su patrimonio, finalidades que se apartan del derecho de autoderminación informativa que es competencia de la ANPD, pues esta no tiene arrogada la facultad de proteger a los clientes del Banco para evitar que estos sean víctimas de fraude, con lo cual imponer esta medida correctiva vulnera el principio de legalidad.

29. Por tanto, corresponde a este despacho dilucidar si la ANPD es o no competente para sancionar con la medida correctiva impuesta por la resolución de primera instancia.

30. Al respecto, cabe advertir que, atendiendo al principio de legalidad se reconoce la facultad de la ANPD de imponer medidas correctivas en los procedimientos sancionadores. Así, de acuerdo con lo establecido en el artículo 33, numeral 20, de la LPDP es función de la ANPD: «Iniciar fiscalizaciones de oficio o por denuncia de parte por presuntos actos contrarios a lo establecido en la presente Ley y en su reglamento y aplicar las sanciones administrativas correspondientes, sin perjuicio de las medidas cautelares o correctivas que establezca el reglamento».

31. Además, el artículo 38 de la LPDP dispone que «Sin perjuicio de las sanciones que en el marco de su competencia imponga la autoridad competente, esta puede ordenar la implementación de una o más medidas correctivas, con el objetivo de corregir o revertir los efectos que la conducta infractora hubiere ocasionado o evitar que ésta se produzca nuevamente».

32. En este orden de ideas, el artículo 118 del Reglamento de la LPDP, dispone que «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».

33. Una medida correctiva es un mandato u orden proveniente de una autoridad competente que tiene como propósito corregir, subsanar o enmendar una situación equivocada o errada. Así, cumple con el objetivo definitivo retrospectivo de: reponer o reestablecer las cosas al estado anterior de la comisión del ilícito, corrigiendo los efectos que la conducta infractora hubiere causado en el interés público[3].

34. El derecho de protección de datos personales supone el deber por parte del titular del banco de datos personales o responsable de su tratamiento de impedir que se produzcan tratamientos ilícitos o inadecuados, pues estos pueden producir en el titular del dato personal diferentes efectos ya sea la vulneración de derechos fundamentales personalísimos, como, por ejemplo, lesiones a su intimidad, vida privada, honor, etc. como también puede conllevar riesgos en su patrimonio o bienes.

35. Por ello, es importante tener en cuenta que, si bien el derecho a la protección de datos tiene sus propias peculiaridades que lo convierten en un derecho con un contenido específico y con un sistema de protección propio, dichas características coexisten con la función de garantía instrumental de otros derechos[4], entre los cuales se encuentra el derecho a la protección de su propiedad o seguridad financiera o patrimonial.

36. Dicho esto, y atendiendo a las disposiciones normativas antes mencionadas, la ANPD se encuentra plenamente facultada para imponer medidas correctivas dirigidas a evitar los efectos que un tratamiento ilícito de datos personales pueda producir.

37. En consecuencia, si existe algún potencial peligro para el titular de los datos personales con respecto a posible uso inadecuado de sus datos por parte de terceros, la ANPD tiene atribuidas las facultades para imponer las medidas correctivas que considere necesarias para evitar se produzcan estos perjuicios

---

3 Miguel CASINO RUBIO, «La indebida confusión entre sanciones y otras medidas administrativas de policía: comentarios a la STS del 2 de febrero de 1998, artículo 2060». *Reala*, Nro. 283, 2000, nota 27, p. 572.

4 Antonio TRONCOS REIGADA, *La protección de datos personales. En busca del equilibro*, Tirant lo Blanch, Valencia, 2010, pp. 1571-1572.

económicos o fraudes que atenten contra el patrimonio u ocasionen pérdidas financieras a los titulares de los datos personales.

38. Por tal motivo, **no corresponde amparar** este extremo de la apelación de la administrada.

VI. ANÁLISIS DE LAS CUESTIONES CONTROVERTIDAS

VI.1 Determinar si la medida correctiva impuesta es o no nula por la alegada ausencia de motivación en la resolución materia de impugnación

39. La administrada advierte que la DPDP impone la medida correctiva únicamente en su parte resolutiva no existiendo un razonamiento previo en la parte considerativa que desarrolle dicho acto administrativo, con lo cual no se satisface el requisito de motivación de toda decisión administrativa, al no indicar cómo la carga impuesta a la administrada permitirá eliminar o detener los efectos que se atribuyen, incurriendo, por ende, en causal de nulidad. Esta ausencia de motivación vulnera el derecho al debido procedimiento en sede administrativa.

40. Al respecto, cabe señalar que, si bien la medida correctiva no posee una naturaleza sancionadora, dado que le es ajena la finalidad puramente aflictiva propia de las sanciones administrativas[5] que castigan la perturbación, infligiendo un mal que no restablece el orden quebrantado por la infracción, las medidas correctivas o reparatorias buscan remediar la situación generada por la infracción, restituyendo las cosas a su estado anterior[6] y, por tanto son medidas represivas sobre los efectos derivados de las conductas indebidas[7].

41. Por ende, aunque las medidas correctivas gozan de un nivel de individualidad al ser posible la interposición de estas sin necesidad de apertura previa de un procedimiento sancionador o la necesidad de ser dictada al interior de este[8], lo cierto es que para su interposición basta que se verifique la existencia de efectos negativos como consecuencia de la conducta indebida u obligación incumplida. En este orden de ideas, si en virtud de un incumplimiento del administrado existe una situación que restablecer o un efecto nocivo que detener, la administración, cuando cuente con potestad legal para hacerlo, puede imponer la medida correctiva que

---

5 Alejando HUERGO LORA, «Las Sanciones Administrativas», IUSTEL, Madrid, 2007, p. 250 y ss.

6 Miguel CASINO RUBIO, «La indebida confusión entre sanciones y otras medidas administrativas de policía: comentarios a la STS del 2 de febrero de 1998, artículo 2060». *Reala*, Nro. 283, 2000, nota 27, p. 572.

7 Severiano FERNANDEZ RAMOS, *La actividad de inspección. El régimen jurídico de la función inspectora,* Comares, Granada, 2002, p. 410 y ss.

8 Juan Carlos MORON URBINA, *Los actos-medidas (medidas correctivas, provisionales y de seguridad) y la potestad sancionadora de la Administración*. Revista del Círculo de Derecho Administrativo, Nro. 9. pp. 142-143.

considere necesaria, pues ella, como gestora y tutora del interés público, está facultada para hacer cumplir a los administrados sus obligaciones legales[9], siempre que tal decisión responda a criterios de razonabilidad, y ajustarse a la intensidad, proporcionalidad y a las necesidades de los bienes jurídicos tutelados que se pretende garantizar en cada supuesto concreto, de acuerdo con lo establecido en el artículo 251.1 del TUO de la LPAG.

42. La administrada alega que no se ha fundamentado la imposición de la medida correctiva. Sin embargo, como se ha advertido, para la interposición de una medida correctiva lo que hace falta es acreditar el incumplimiento de una obligación del administrado y la existencia de una alteración o modificación del estado de las cosas querido por el ordenamiento jurídico que justifique la reacción *a posteriori* de la administración, frente a daños a los bienes de interés público jurídicamente tutelados y derivados del incumplimiento administrativo[10]. De ahí que se afirme que las medidas correctivas tutelan directamente el interés público[11].

43. Visto el expediente, la resolución de primera instancia deja en claro, que: «ha quedado acreditado que producto de las dos brechas de seguridad se ha comprometido la confidencialidad de los datos personales de los clientes de la administrada, toda vez que terceros no autorizados pudieron acceder al aplicativo y/o sistema vulnerado, consultar y sustraer información relacionada a los mismos (producto de la brecha de seguridad de julio se obtuvo información de 34, 242 clientes y de la brecha de noviembre se obtuvo información de 1'116, 242 clientes), para finalmente ser filtrada en la «Deep Web», como fue posteriormente denunciado por algunos de sus clientes ante la DFI (conforme a lo descrito en los considerandos 1, 6, 18 y 23 de la presente Resolución Directoral)»[12].

44. Además, se afirma que si bien la administrada «una vez detectadas las brechas de seguridad, ha actuado de manera reactiva, activando protocolos y tomando acciones internas para mitigar el tratamiento indebido de los datos personales, (…) no ha revertido la situación respecto a los datos personales de sus clientes que fueron sustraídos de forma inadecuada, puesto que no se advierte el cambio de números de tarjeta vinculados a sus clientes afectados por la sustracción indebida de datos personales»[13].

45. Asimismo, la resolución impugnada determina la existencia de una alteración o modificación del estado de las cosas querido por el ordenamiento jurídico que

---

9 Noelia CARRERAS SCHABAUER, «Medidas de policía administrativa y régimen jurídico del servicio público: uso de las medidas correctivas en el Perú», *Derecho,* Nro. 67, 2011, pp. 496 y 505 – 506.

10 En este sentido: *Vid.* Manuel REBOLLO PUIG, *Derecho Administrativo Sancionador*, Lex Nova, Madrid, 2010, p. 68.

11 Noelia CARRERAS SCHABAUER, «Medidas de policía …*Op. Cit.,* pp. 501.

12 Foja 32 de la RD.

13 Foja 32 de la RD.

justifica la reacción *a posteriori* de la administración frente a los daños a los bienes de interés público jurídicamente tutelados derivados del incumplimiento administrativo. Así, al evaluar los criterios de gravedad del daño al interés público y bien jurídico protegido de la infracción cometida, advierte que «Si bien la administrada ha señalado que no se ha producido fraudes relacionados a la información sustraída y filtrada de los clientes, dicha situación no enmienda la omisión incurrida por la administrada respecto a garantizar un nivel de protección adecuado y suficiente en la aplicación vulnerada, lo cual ha quedado evidenciado con la cantidad de información sustraída, la misma que incluso podría ser usada en perjuicio de sus titulares»[14].

46. En este orden de ideas, la resolución impugnada cumple con acreditar el incumplimiento por parte de la administrada en lo que respecta a la obligación de confidencialidad y con advertir que si bien se tomaron ciertas medidas para evitar se sigan produciendo filtraciones de seguridad que permitan que terceros obtengan información personal de los clientes, la administrada no ha realizado acciones que eviten que se produzcan tratamientos indebidos con los datos personales que debido a estas brechas de seguridad ya fueron sustraídos, encontrándose, estos a disposición de terceros ajenos y pasibles de ser utilizados o tratados inadecuadamente o ilícitamente, producto de estas filtraciones en la seguridad del banco, por ejemplo, es posible que se produzca la fabricación de tarjetas falsificadas o clonadas sean físicas o virtuales que posteriormente se utilicen para pagos fraudulentos tanto en el mundo físico como en el mundo *online*[15].

47. Por ende, dadas las facultades que la ANPD tiene atribuidas de imponer medidas correctivas, la determinación en la resolución impugnada de la existencia de un incumplimiento y la necesidad acreditada de evitar los riesgos que la filtración de seguridad ha producido al sustraerse los datos personales de clientes con el potencial efecto de que estos sean utilizados indebida o ilícitamente por terceros, este despacho considera que la resolución impugnada no ha vulnerado la debida motivación de la resolución en lo que respecta a la fundamentación que justifica la imposición de la medida correctiva.

VI.2 Sobre si la medida correctiva impuesta es proporcional

48. La administrada señala que la medida correctiva tampoco resulta proporcional a la infracción atribuida y a la sanción pecuniaria impuesta, pues es extremadamente gravosa y mucho más onerosa que la propia multa. Asimismo, indica que la DPDP no ha señalado a qué tipo de tarjetas se refiere y que no han sido los únicos datos adquiridos por terceros por lo que resulta una medida aleatoria.

---

14 Foja 39 de la RD.

15 Eduardo LIBEROS (Coord.), *El libro del comercio electrónico,* ESIC – Editorial, Madrid, 2011, p. 306.

49. Al respecto, la medida correctiva impuesta por la resolución materia de impugnación consiste en que la entidad bancaria entregue *nuevos números de tarjeta a los dientes cuyos números de tarjetas vinculados a sus nombres y/o número de documento de identidad fueron sustraídos en las brechas detectadas en julio y noviembre de 2018, desvinculándolos de los números de tarjeta que fueron sustraídos en dichas brechas. Dicho cambio no deberá ser cobrado a los clientes afectados. Para el cumplimiento de tal medida correctiva se otorga el plazo de ciento veinte (120) días hábiles contados a partir de la notificación que declare consentida o firme la Resolución Directoral, debiendo remitir la documentación sustentatoria de su Implementación».*

50. La administrada afirma que los datos personales a los cuales terceros habrían tenido acceso no permite la realización de acciones fraudulentas con relación al patrimonio de los clientes de la administrada. Ello, porque para materializar tales actos se requiere un conjunto de información concurrente a los cuales los terceros no han tenido acceso. Además, en el supuesto negado que las acciones fraudulentas se pudieran dar, no podría generarse un daño a nuestros clientes ya que, al no contar con el CVV2 de las tarjetas, el banco podría realizar el contra cargo de dicha operación sin afectar a los clientes.

51. Al respecto, es importante precisar que no todas las operaciones en línea necesitarían el código CVV2 para hacerse efectivas, algunas tiendas online ofrecen la posibilidad de evitar este paso y no transmiten este código secreto a una pasarela de pago[16].

---

16 Tal como se ha relatado en el siguiente enlace: https://www.kaspersky.es/blog/los-riesgos-ocultos-de-las-tarjetas-bancarias/5400/. Cabe señalar que Kaspersky es una compañía internacional dedicada a la seguridad informática con presencia en aproximadamente 195 países del mundo, calificado por AV - TEST Instituto de seguridad informática alemán como uno de los mejores antivirus del mundo, al respecto: https://www.av-test.org/es/antivirus/usuarios-finales-windows/. También resulta interesante un estudio de la Universidad de Newcastle del Reino Unido que afirma que es posible averiguar los valores del código de verificación de tarjetas de crédito y débito VISA, utilizando una red de robots web (programas informáticos que realizan de forma automatizada tareas en internet) que se aprovechan de una debilidad en los sistemas de pagos con tarjeta en la web, que permiten hacer un número de intentos de códigos erróneos muy alto, a veces incluso ilimitado.
Los pasos que seguirían los ladrones serían los siguientes: primero se hacen con los 16 dígitos de una tarjeta de crédito, ya sea mediante ingeniería social (entiéndase obteniendo los números de las tarjetas a través de descuidos) o usando algoritmos que generan número de tarjeta válidos.
A continuación, deben averiguar la fecha de expiración y el CVV o CVV2 de esa tarjeta. Para ello utilizan bots que usando la plataforma de pago de miles de sitios webs de compra, empiezan a probar de forma distribuida las combinaciones de fechas y dígitos. Teniendo una lista de miles de sitios de compras, con hacer menos de 10 intentos por sitio les servirá para encontrar la combinación correcta. El número de posibles combinaciones no es demasiado alto, 999 posibles códigos CVV o CVV2 y menos de 50 posibles fechas de caducidad (teniendo en cuenta que solo se indica mes/año, y que la ventana de caducidad seguramente será inferior a los 5 años).
En el estudio de la Universidad de Newcastle se concluye que pueden obtenerse los datos de las tarjetas de créditos en tan sólo 6 segundos.

52. Además, vistos los datos que han sido objeto de estas filtraciones de seguridad de información, como el nombre completo del titular y, dada la brecha del 12 de noviembre de 2018, la fecha de vencimiento de la tarjeta, esta Dirección General estima que esta información combinada aumenta el peligro de realización de operaciones indebidas.

53. Visto lo anterior es claro que, como la misma entidad bancaria afirma, dado que el acceso no autorizado a la información personal de los clientes ya se produjo, esta continúa circulando en internet, con lo cual el riesgo de que se produzca un tratamiento indebido de datos personales que genere un peligro para el patrimonio de los titulares de los datos es latente. Por ello, la adopción de la medida impuesta es lograr revertir las cosas a su estado anterior, así como minimizar las consecuencias de daño producido, esto quiere decir que disminuya o desaparezca el riesgo de otras posibles afectaciones de los titulares de dichos datos.

54. En cuanto a que la medida impuesta resultaría muy onerosa, es pertinente precisar que la administrada afirma que actualmente el 56.50% de las tarjetas afectadas en las brechas de seguridad estarían activas, siendo que el resto de las tarjetas a la fecha se encuentran vencidas o han sido bloqueadas por los propios clientes, por lo que la medida correctiva no resultaría aplicable al 100% de clientes afectados; además, que no consta en el expediente una evaluación económica que sustente lo señalado por la administrada.

55. Al respecto, el bloqueo de una tarjeta bancaria y la entrega de una nueva es la consecuencia natural de la pérdida de esta, de su robo o sustracción o de la pérdida de su información[17], con lo cual hecha esta operación no se corre el riesgo de que los datos personales sean mal utilizados por terceros ajenos con fines de ocasionar con esta información perjuicios económicos. Lo mismo sucede con el

---

El estudio indica también que esta técnica podría haber sido la utilizada para robar casi 3 millones de euros a la cadena de comercios TESCO en el Reino Unido. Al respecto: *Vid.* *https://eprint.ncl.ac.uk/file_store/production/230123/19180242-D02E-47AC-BDB3-73C22D6E1FDB.pdf*

[17] Al respecto téngase en cuenta lo dispuesto en la Resolución de SBS Nro. 3719-2016, de 6 de julio de 2016, que aprueba las cláusulas generales de contratación aplicables al Contrato de Tarjetas de Crédito, las mismas que en su cláusula 10 titulada: «Que hacer en caso de extravío, robo o sustracción de las tarjetas o de su información», dispone lo siguiente: «Si sufre el extravío, robo o sustracción de la Tarjeta o de la información contenida en ella, Usted deberá comunicarse inmediatamente con el Banco utilizando los medios de comunicación que este ponga a su disposición, a efectos de bloquear la Tarjeta y obtener el código de bloqueo respectivo, precisando la fecha, hora y contenido del mismo.
Dicha comunicación se tendrá por efectuada únicamente respecto de la Tarjeta indicada por Usted, sea la Tarjeta titular y/o adicional, por lo que no afectará a las demás asociadas a la Cuenta.
El Banco procederá a la emisión de una nueva Tarjeta conforme a sus procedimientos y enviará una copia del registro de la comunicación de bloqueo señalada en el primer párrafo de esta cláusula, la cual podrá ser física o electrónica a solicitud de Usted».

vencimiento de la tarjeta bancaria, pues producida esta carece de operatividad con lo cual el riesgo de producción de perjuicios al patrimonio del titular de los datos personales por el uso inadecuado de la información personal filtrada por la brecha de seguridad, no se produce.

56. Por ello, este despacho considera que la medida correctiva impuesta por la resolución de primera instancia, a fin de que se proceda a entregar *nuevos números de tarjeta a los clientes cuyos números de tarjetas vinculados a sus nombres y/o número de documento de identidad fueron sustraídos en las brechas detectadas en julio y noviembre de 2018, desvinculándolos de los números de tarjeta que fueron sustraídos en dichas brechas. Dicho cambio no deberá ser cobrado a los dientes afectados,* debe reformularse en el siguiente sentido:

> «Imponer como medida correctiva a el BANCO DE CRÉDITO DEL PERÚ S.A acreditar que ha entregado nuevos números de tarjetas de crédito y débito a los clientes cuyos números de tarjetas vinculados a sus nombres y/o número de documento de identidad fueron sustraídos en las brechas detectadas en julio y noviembre de 2018, desvinculándolos de los números de tarjeta que fueron sustraídos en dichas brechas, siempre que a la fecha de implementación de la presente resolución, las tarjetas de dichos clientes no se encuentren bloqueadas o vencidas. Dicho cambio no procederá, ademas, en el supuesto que el cliente señale expresamente que no requiere el cambio de los números de sus tarjetas; asimismo, no deberá ser cobrado a los clientes afectados.
>
> Para el cumplimiento de tal medida correctiva, se otorga el plazo de ciento veinte (120) días hábiles contados a partir de la notificación que declare consentida o firme la presente Resolución Directoral, debiendo remitir la documentación sustentadora de su implementación, donde se deberá acreditar, en caso de no entregar una nueva tarjeta a un cliente afectado, la denegación expresa del cliente, así como la condición de la tarjeta afectada de vencida o bloqueada al momento de la implementación de la medida correctiva».

57. Por último, en lo que respecta a lo alegado en el contexto de pandemia, cabe advertir que actualmente el estado se encuentra en la fase 4 de reactivación económica[18], con lo cual la administrada atendiendo a la normativa de prevención

[18] Decreto Supremo Nro. 157-2020-PCM, publicado en el Diario Oficial *El Peruano* el 26 de septiembre de 2020 que aprueba la Fase 4 de la reanudación de actividades económicas dentro del marco de la declaratoria de Emergencia Sanitaria Nacional por las graves circunstancias que afectan la vida de la Nación a consecuencia del COVID-19.

de propagación del virus puede poner en marcha los mecanismos y forma de organización adecuados para el cumplimiento de la medida correctiva[19].

Por las consideraciones expuestas y de conformidad con lo dispuesto por la Ley Nro. 29733, Ley de Protección de Datos Personales, su reglamento aprobado por el Decreto Supremo Nro. 003-2013-JUS, el Texto Único Ordenado de la Ley Nro. 27444, Ley del Procedimiento Administrativo General, aprobado por Decreto Supremo Nro. 006-2017-JUS, el artículo 71, literal l), del Reglamento de Organización y Funciones del Ministerio de Justicia y Derechos Humanos, aprobado por Decreto Supremo Nro. 013-2017-JUS, y el Reglamento del Decreto Legislativo Nro. 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 Nro. 019-2017-JUS;

RESOLUCIÓN:

PRIMERO. Declarar **FUNDADO EN PARTE** el recurso de apelación presentado por BANCO DE CRÉDITO DEL PERÚ , y en consecuencia:

- **CONFIRMAR** la Resolución Directoral Nro. 1169-2020-JUS/DGTAIPD – DPDP de 30 de junio de 2020 en el extremo referido a la atribución de la responsabilidad referido a la obligación de confidencialidad, en los siguientes términos:

  Artículo 1.- Sancionar a BANCO DE CRÉDITO DEL PERÚ S.A., con una multa ascendente a cuarenta unidades impositivas tributarias (40 UIT) por la comisión de la infracción grave tipificada en el literal g), numeral

---

19 Al respecto téngase en cuenta que, de acuerdo con el Reglamento de Tarjetas de Crédito y Débito aprobado mediante Resolución de SBS Nro. 6523-2013:

Artículo 16.- Medidas de seguridad respecto a los usuarios
Las empresas deben adoptar, como mínimo, las siguientes medidas de seguridad con respecto a los usuarios:
1. Entregar la tarjeta y, en caso corresponda, las tarjetas adicionales al titular, excepto cuando este haya instruido en forma expresa que se entreguen a una persona distinta, previa verificación de su identidad y dejando constancia de su recepción.

Asimismo:

Artículo 27.- Manuales aplicables por la expedición y administración de tarjetas
Las empresas deberán contar con manuales relacionados con la expedición y administración de tarjetas, considerando para tal efecto el cumplimiento de las obligaciones desarrolladas en el Reglamento.
Adicionalmente, dichos manuales deberán considerar los procedimientos, plazos, controles y medidas de seguridad utilizados en la elaboración física, asignación de clave, transporte, entrega y custodia de las tarjetas. (Subrayado propio)

2), del artículo 132º del Reglamento de la LPDP: "Incumplir la obligación de confidencialidad establecida en el artículo 17 de la Ley Nº 29733"

- **REVOCAR** la Resolución Directoral Nro. 1169-2020-JUS/DGTAIPD – DPDP de 30 de junio de 2020 en el extremo referido al artículo 2 que dispone la medida correctiva y **REFORMÁNDOLA** en los siguientes términos:

  Artículo 2.- Imponer como medida correctiva a el BANCO DE CRÉDITO DEL PERÚ S.A acreditar que ha entregado nuevos números de tarjetas de crédito y débito a los clientes cuyos números de tarjetas vinculados a sus nombres y/o número de documento de identidad fueron sustraídos en las brechas detectadas en julio y noviembre de 2018, desvinculándolos de los números de tarjeta que fueron sustraídos en dichas brechas, siempre que a la fecha de implementación de la presente resolución las tarjetas de dichos clientes no se encuentren bloqueadas o vencidas. Dicho cambio no procederá, ademas, en el supuesto que el cliente señale expresamente que no requiere el cambio de los números de sus tarjetas; asimismo, no deberá ser cobrado a los clientes afectados.

  Para el cumplimiento de tal medida correctiva, se otorga el plazo de ciento veinte (120) días hábiles contados a partir de la notificación que declare consentida o firme la presente Resolución Directoral, debiendo remitir la documentación sustentadora de su implementación, donde se deberá acreditar, en caso de no generar nuevos números a un cliente afectado, la denegación expresa del cliente con la aclaración previa de los riesgos generados, así como la condición de la tarjeta afectada que se encuentre vencida o bloqueada al momento de la implementación de la medida correctiva.

SEGUNDO. Notificar al interesado la presente resolución, la cual agota la vía administrativa.

TERCERO. Disponer la devolución del expediente administrativo a la Dirección de Protección de Datos Personales para los fines pertinentes.

Regístrese y comuníquese.

PERÚ Ministerio de Justicia y Derechos Humanos
DIRECCIÓN GENERAL DE TRANSPARENCIA, ACCESO A LA INFORMACIÓN PÚBLICA Y PROTECCIÓN DE DATOS PERSONALES
E. LUNA C.

Firmado digitalmente por LUNA CERVANTES Eduardo Javier FAU 20131371617 soft
Fecha: 2020.11.16 19:07:58 -05'00'

Eduardo Luna Cervantes
Director General
Dirección General de Transparencia, Acceso a la Información Pública y Protección de Datos Personales