Resolución Directoral N° 1169 -2020-JUS/DGTAIPD-DPDP

Expediente N°
130-2019-JUS/DGTAIPD-PAS

Lima, 31 de julio de 2020

VISTOS:

El Informe Nº 130-2019-JUS/DGTAIPD-DFI del 10 de marzo de 2020[1], emitido por la Dirección de Fiscalización e Instrucción de la Dirección General de Transparencia, Acceso a la Información Pública y Protección de Datos Personales (en adelante, la DFI), junto con los demás documentos que obran en el respectivo expediente; y,

CONSIDERANDO:

I. Antecedentes

1. Con fecha 26 de julio de 2018, el Banco de Crédito del Perú S.A. (en adelante, el "BCP" o la "administrada") comunicó a la Dirección De Protección de Datos Personales (en adelante, la "DPDP"), mediante escrito ingresado con Hoja de Trámite N° 47126-2018MSC[2], una brecha de seguridad[3], en la que informó lo siguiente:

- El 7 de julio de 2028 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:

[1] Folios 335 a 353
[2] Folios 6 a 7
[3] Según la Agencia Española de Protección de Datos, una brecha de seguridad es un incidente de seguridad que afecta a datos de carácter personal. Este incidente puede tener un origen accidental o intencional y además puede afectar a datos tratados digitalmente o en formato papel. En general, se trata de un suceso que ocasione destrucción, pérdida, alteración, comunicación o acceso no autorizado a datos personales. Referencia extraída de: https://www.aepd.es/reglamento/cumplimiento/brechas-de-seguridad.html

- 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.

- Asimismo, indicó que una vez determinada la existencia de la intrusión informática, procedió con las siguientes acciones:

  - Se aplicó el protocolo establecido por el banco para casos de intrusiones informáticas, el mismo que establece medidas como desafiliación de la opción de Compras por Internet, comunicaciones con los clientes, bloqueos temporales o definitivos de tarjetas de débito, entre otros.
  - Se estableció un monitoreo reforzado 24x7, tanto al aplicativo afectado, como a las transacciones de los clientes afectados.
  - Se convocó al Grupo de Expertos de las Gerencias de Sistemas para la definición y plan de acción, a efectos de reforzar las medidas de seguridad en el aplicativo y componentes impactados, adoptándose diversas medidas en el campo de TI, incluyendo la implementación de controles de seguridad adicionales, entre otros aspectos.
  - Se activaron los Comités de Crisis a nivel de Equipo de Soporte de Crisis (nivel táctico) y Equipo de Manejo de Crisis (nivel estratégico).
  - Se desarrolló una estrategia de atención y comunicación por segmento del cliente, ejecutado por las unidades de negocio involucradas, realizándose comunicaciones a los clientes impactados (llamada telefónica, correo o sms), informándoles que terceros accedieron a la información personal y de su cuenta, y que por seguridad y de manera preventiva habían bloqueado la tarjeta de débito impactada.

2. Mediante Oficio N° 500-2018-JUS/DGTAIPD-DFI[4] de 8 de agosto de 2018, la DFI solicitó la siguiente información al BCP:

- Informar sobre las medidas de seguridad implementadas para el acceso al aplicativo, antes de la intromisión informática.
- Detalle de la intrusión informática realizada al aplicativo, señalando la cuenta usuaria, perfil y medidas de seguridad de acceso y autenticación al aplicativo, así como la fecha de detección del incidente (si es exacta o estimada), medios de detección, fecha de inicio y resolución del incidente.
- Remitir el log de eventos sobre la cuenta vulnerada, asimismo precisar si los datos obtenidos fueron , porque se accedió a cuentas individuales, o de una cuenta administrador el cual permitía identificar el detalle de las cuentas vulneradas,

[4] Folio 9

- Detallar todas la aplicaciones que realiza tratamiento de datos personales de clientes, asimismo, si dichas aplicaciones utilizan las mismas medidas de seguridad de acceso del aplicativo donde se realizó la intrusión informática.
- Informar sobre los planes de acción a la intrusión informática.
- Informar si a la fecha se identificó a los responsables que realizaron la intrusión informática.
- Informar las posibles consecuencias de la intrusión informática de los datos personales.
- Informar la cantidad de clientes a las cuales se les informó sobre la intrusión informática. Asimismo, detalle los canales de comunicación utilizados y adjunte el contenido de la comunicación enviada a los afectados.

3. Mediante escrito ingresado con Hoja de Trámite N°55666-2018MSC[5] de 28 de agosto de 2018, el BCP remitió respuesta al Oficio N° 500-2018-JUS/DGTAIPD-DFI.

4. Mediante Oficio N° 674-2018-JUS/DGTAIPD-DFI[6] de 19 de octubre de 2018, la DFI solicitó la siguiente información al BCP:

- Los planes de acción adoptados respecto a la intrusión informática.
- Si identificó a los responsables de la intrusión informática.
- Detallar las aplicaciones que realizan tratamiento de datos personales de clientes. Asimismo, si dichas aplicaciones utilizan las mismas medidas de seguridad de acceso del aplicativo afectado.
- Las posibles consecuencias de la intrusión informática de los datos personales.
- Número de clientes a los cuales se les informó sobre la intrusión informática. Asimismo, detalle los canales de comunicación utilizados y adjunte el contenido de la comunicación enviada a los afectados,
- Si no se les informó, remitir la justificación.

5. Mediante escrito ingresado con Hoja de Trámite N°70361-2018MSC[7] de 8 de noviembre de 2018, el BCP remitió respuesta al Oficio N° 674-2018-JUS/DGTAIPD-DFI.

6. Con fecha 23 de noviembre de 2018, el BCP comunicó a la DPDP, mediante escrito ingresado con Hoja de Trámite N° 74313-2018MSC[8], otra brecha de seguridad, en la que informó lo siguiente:

- El 12 de noviembre de 2018 identificó que se estaba produciendo sustracción de información (datos personales) de sus clientes a través de uno de sus aplicativos por parte de terceras personas.
- 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

[5] Folios 10 a 19
[6] Folio 20
[7] Folios 21 a 24
[8] Folios 26 a 28

mil cuatrocientos veinticuatro (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.

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 con las siguientes acciones:

  - Se aplicó el protocolo establecido por el banco para casos de intrusiones informáticas.
  - Se estableció un monitoreo reforzado 24x7, tanto al aplicativo afectado, como a las transacciones de los clientes afectados.
  - Se convocó al Grupo de Expertos de las Gerencias de Sistemas para la definición y plan de acción, a efectos de reforzar las medidas de seguridad en el aplicativo y componentes impactados, adoptándose diversas medidas en el campo de TI, incluyendo la implementación de controles de seguridad adicionales, entre otros aspectos.
  - Se adoptaron diversas medidas en el campo de TI que van desde la restricción de accesos hasta la implementación de controles de seguridad adicionales, entre otros aspectos.
  - Se activaron los Comités de Crisis a nivel de Equipo de Soporte de Crisis (nivel táctico) y Equipo de Manejo de Crisis (nivel estratégico).
  - Se desarrolló una estrategia de atención y comunicación por segmento del cliente, la cual se viene ejecutando por las unidades de negocio involucradas.
  - Se está realizando comunicaciones a los clientes, ya sea por llamada telefónica, correo o SMS, informándoles que terceros accedieron a la información personal y de sus cuentas y/o tarjetas.

7. Mediante Proveído de 7 de febrero de 2019[9], la DFI dispuso iniciar actuaciones de fiscalización al BCP, a fin de verificar las medidas técnicas y organizativas implementadas respecto a las brechas de seguridad comunicadas a la Autoridad Nacional de Protección de Datos Personales. Asimismo. Dispuso anexar al presente expediente los originales de los escritos presentados por el BCP mediante Hoja de Trámite N° 47126-2018MSC de 26 de julio de 2018, Hoja de Trámite N° 55666-2018MSC de 28 de agosto de 2018, Hoja de Trámite N° 70361-2018MSC de 8 de noviembre de 2018 y Hoja de Trámite N° 74313-2018MSC de 23 de noviembre de 2018.

8. Mediante la Orden de Visita de Fiscalización Nº 014-2019-JUS/DGTAIPD-DFI[10] de fecha 8 de febrero de 2019, la DFI dispuso la realización de una visita de fiscalización al BCP, a fin de verificar si dicha entidad, en el desarrollo de sus actividades, cumple la Ley N° 29733, Ley de Protección de Datos Personales (en adelante, la "LPDP") y su reglamento, aprobado por Decreto Supremo N° 003-2013-JUS (en adelante, el "Reglamento de la LPDP")

9. El 8 de febrero de 2019, se realizó la primera visita de fiscalización, dejándose constancia de los hechos en el Acta de Fiscalización N°01-2019[11].

10. El 14 de febrero de 2019, se realizó la segunda visita de fiscalización, dejándose constancia de los hechos en el Acta de Fiscalización N°02-2019[12].

11. El 25 de febrero de 2019, se realizó la tercera visita de fiscalización, dejándose constancia de los hechos en el Acta de Fiscalización N°03-2019[13].

12. El 5 de marzo de 2019, se realizó la cuarta visita de fiscalización, dejándose constancia de los hechos en el Acta de Fiscalización N°04-2019[14].

13. Mediante Oficio Nº 193-2019-JUS/DGTAIPD-DFI[15], se notificó el Proveído del 7 de febrero de 2019.

14. Mediante escrito ingresado por Hoja de Trámite N° 17396-2019MSC[16] de fecha 11 de marzo de 2019, el BCP remitió información requerida mediante Acta de Fiscalización N° 03-2019.

15. Mediante escrito ingresado por Hoja de Trámite N° 19626-2019MSC[17] de fecha 19 de marzo de 2019, el BCP remitió información requerida mediante Acta de Fiscalización N° 04-2019.

[9] Folio 1
[10] Folio 30
[11] Folios 31 a 40
[12] Folios 41 a 50
[13] Folios 51 a 76
[14] Folios 77 a 86
[15] Folio 87
[16] Folio 88 a 164
[17] Folio 165 a 193

16. Mediante Informe Técnico N° 52-2019-DFI-VARS de 26 de marzo de 2019[18], 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 el BCP ha tenido un proceso de respuesta de incidentes, no obstante no ha sido totalmente levantado, al evidenciarse que no habría implementado la medida de seguridad referente a los registros de interacción lógica para el tratamiento de datos personales, obligación requerida en el numeral 2 del artículo 39 del Reglamento de la LPDP.

17. Mediante Oficio N°483-2019-JUS/DGTAIPD-DFI, la DFI notificó a la administrada con fecha 19 de junio de 2019[19] el Proveído de 17 de junio de 2019[20] mediante el cual se amplía el plazo de la fiscalización por cuarenta y cinco (45) días hábiles adicionales, los cuales se contarán a partir del 19 de junio de 2019.

18. Mediante escrito ingresado por Hoja de Trámite N° 53295-2019MSC[21] de fecha 25 de julio de 2019, el BCP remitió información adicional respecto a las comunicaciones realizadas a la Autoridad:

- 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.
- 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.
- 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.
- 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.

19. Por medio del Informe de Fiscalización N° 131-2019-JUS/DGTAIPD-DFI-AARM de 21 de agosto de 2019[22], el analista legal de fiscalización de la DFI, por los argumentos que desarrolla y la documentación que obra en el expediente, 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 N°759-2019-JUS/DGTAIPD-DFI[23], notificado el 13 de setiembre de 2019[24].

[18] Folios 194 a 198
[19] Folio 200
[20] Folio 199
[21] Folio 88 a 164
[22] Folios 204 a 211
[23] Folio 213
[24] Folio 214

20. Mediante Resolución Directoral Nº 242-2019-JUS/DGTAIPD-DFI de 2 de diciembre de 2019[25] (en adelante, la "RD de Inicio"), la DFI dispone el inicio del procedimiento administrativo sancionador a la administrada; resolución que fue notificada mediante Oficio N° 994-2019-JUS/DGTAIPD-DFI[26], notificado el 4 de diciembre de 2019[27].

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.

21. Mediante escrito ingresado con Hoja de Trámite N°90716-2019MSC de fecha 26 de diciembre de 2019[28], la administrada presentó sus descargos, señalando lo siguiente:

21.1. Fundamentos de hecho

21.1.1. Respecto a las medidas de seguridad

21.1.1.1. Sobre el primer evento comunicado (intrusión informática identificada el 7 de julio de 2018), refirió lo siguiente:

- Que, según la carta de 8 de noviembre de 2018, señaló que *"la aplicación cuenta con registros de auditoría que permiten contar con la trazabilidad de las actividades que se realizan dentro de la aplicación y de la base de datos, así como la gestión centralizada del acceso a las herramientas que son utilizadas para esta aplicación"*. El aplicativo contaba con herramientas informáticas que realizaban la función de registro de eventos como se acreditó en el Acta de Fiscalización N°02.
- Según lo acreditado en el Acta de Fiscalización N°02, el BCP no contaba con una herramienta que cuente con la función de registros de eventos relacionados con la liberación de nuevas versiones de software por lo que no resulta pertinente señalar que el BCP no contaba con función de registro de eventos respecto de las bases de datos.
- Precisó que el aplicativo impactado sí contaba con las medidas de seguridad: i) control de acceso a la aplicación y sus funcionalidades, ii) logs sobre las interacciones lógicas con los servicios (APIs) que se utilizan para las consultas con base de

[25] Folios 216 a 224
[26] Folio 226
[27] Folios 228 a 277
[28] Folios 413 a 416

datos, iii) medidas de autenticación y autorización, para el funcionamiento de la aplicación, además de logs sobre las iteraciones lógicas, lo que se acreditó en las visitas de inspección.

- Que, como consecuencia del incidente de seguridad se identificó en una librería una inyección de código malicioso que permitía el acceso a métodos de la aplicación directamente, evitando los controles de autenticación, autorización, logs de aplicación y a los servicios utilizados; sin embargo, fueron registradas las consultas en los logs de uno de los componentes principales de la aplicación AXIOMA, evidenciándose el abuso de la funcionalidad de consulta de datos de clientes y el impacto ocasionado.

21.1.1.2. Sobre el segundo evento comunicado (intrusión informática identificada el 12 de noviembre de 2018), refirió lo siguiente:

- Conforme lo acreditado en el Acta de Fiscalización N°04, el BCP precisó que sí contaba con logs de eventos, adjuntando en su carta de 19 de marzo el reporte de consultas realizado por el Bot a la aplicación afectada durante el periodo que la aplicación tuvo los eventos.
- El aplicativo impactado sí contaba con las medidas de seguridad: i) control de acceso a la aplicación y sus funcionalidades, ii) logs sobre las interacciones lógicas con los servicios que se utilizan para las consultas con base de datos, iii) medidas de autenticación y autorización, para el funcionamiento de la aplicación, además de logs sobre las interacciones lógicas.
- Que, como consecuencia del segundo evento se identificó un acceso directo a un componente cloud utilizando credenciales válidas del componente, lo cual permitió el acceso directo a los servicios de la aplicación, evitando los controles de autenticación, autorización y logs de aplicación.
- Los softwares que manejan bases de datos personales en el Banco sí contaban y cuentan con log conforme a lo requerido por la norma; por tanto, acreditando el cumplimiento de las medidas de seguridad requeridas por la normativa aplicable.

21.1.1.3. Sobre el Informe de Fiscalización

- La RD de Inicio señala: *"(…) el Informe de Fiscalización N°131-2019-JUS/DGTAIPD-DFI-AARM le fue notificado a la administrada el 13 de setiembre, sin embargo, no ha remitido documentación a efectos de levantar observaciones realizadas en el citado informe"*
- El Informe Final de Fiscalización no determina responsabilidad administrativa. Para ello se requiere iniciar un procedimiento sancionador. La autoridad en base a la recomendación de dicho informe decidirá finalmente si inicia o no un procedimiento sancionador.
- El Informe Final de Fiscalización no constituye un acto administrativo conforme a la LPAG que afecte la esfera jurídica de los administrados. Sin embargo, la Resolución de Inicio sí

constituye un acto administrativo por lo que al haberse incorporado las inconsistencias y omisiones del mencionado informe en la misma, corresponde señalar a través de estos descargos las violaciones al debido proceso y errores de valoración cometidos, las mismas que junto con la información contenida en los anexos adjuntos a estos descargos deberán ser valorados para no contravenir los principios de Verdad Material y Debido Procedimiento.

21.2. Fundamentos de derecho

21.2.1. Tipicidad respecto de la imputación por presunto incumplimiento de medidas de seguridad relativa a los registros de interacción lógica

- Cualquier obligación o prohibición que no esté debidamente recogida en el tipo infractor, no puede ser exigida.
- El numeral 2 del artículo 39 del Reglamento de la LPDP no ha previsto sino solo algunas características mínimas que se deben satisfacer para cumplir con generar y mantener registros que provean evidencia sobre la interacción de los datos lógicos, siendo que estas condiciones mínimas se habrían satisfecho a través del sistema de registros implementados por el BCP. Siendo ello así, las características de la imputación planteadas no son exigibles y exceden el ámbito de lo específicamente reglado por el tipo infractor.
- La medida de seguridad bajo análisis, en ningún lugar establece que el sistema de registros de las interacciones lógicas deje constancia de cada una de las personas que acceden al sistema, el objetivo de esta disposición únicamente requiere que se permita saber desde qué cuenta se accede, pudiendo esta cuenta tratarse de una que se maneja bajo perfil tipo administrador de log de eventos.
- No existe un mandato en contrario ni está planteada una sofisticación especial, en la medida que exista la capacidad de detectar que se genera un acceso desde una cuenta usuaria y el titular del banco de datos tenga definidas a las personas que puedan operar esa cuenta de forma compartida, la trazabilidad exigida por el artículo 39 numeral 2 del Reglamento de la LPDP está garantizada.
- La Directiva de Seguridad de la Información señala que para el caso de los bancos de datos personales de categoría “crítica”, como sería el BCP, es recomendable que el registro de accesos permita identificar a la “persona o personas que realiza el acceso”. Debe tenerse en cuenta que esta exigencia excede lo previsto en el artículo 39 numeral 2 del Reglamento de la LPDP. La Directiva constituye un documento meramente orientativo de cumplimiento solo facultativo para los administrados no constituyendo una fuente legal que constituya obligaciones adicionales.

21.2.2. Tipicidad respecto de la imputación por la presunta violación del deber de confidencialidad

- La presunta vulneración al deber de confidencialidad no se ajusta al principio de tipicidad puesto que esta infracción se configura con: i) la ocurrencia de una difusión consciente y activa desde dentro de la organización que trata los datos hacia terceros no autorizados; y ii) una omisión de seguridad relevante al interior de la organización que facilite y permita que datos que deben estar bajo reserva sean conocibles por terceros no autorizados. Supuestos que en el presente caso no se han configurado.
- La materialización de los incidentes descritos son consecuencia de un riesgo inherente al proceso de transformación digital, el cual requiere el elemento humano para desarrollarse.

21.2.3. El Non Bis In Idem aplicable al ejercicio de la potestad sancionadora administrativa

- El procedimiento iniciado por la Superintendencia de Banca, Seguros y AFP (SBS) notificado el 5 de diciembre de 2019 y el presente procedimiento generan una vulneración al principio de Non Bis In Ídem, en tanto las imputaciones efectuadas por ambas entidades cumplen con la triple identidad de sujeto, hecho y fundamento.
- Sobre la identidad del sujeto, este se verifica en tanto el BCP es parte del procedimiento iniciado por la Autoridad y la SBS, respectivamente, participando ambos en calidad de sujeto imputado a quien se atribuye presuntas infracciones.
- Sobre la identidad de los hechos, también se produce una superposición entre lo investigado por ambas autoridades administrativas, ya que las imputaciones convergen respecto de un mismo incidente y período, y las obligaciones infringidas se encuentran replicadas en ambos ordenamientos.
- Sobre la identidad del fundamento jurídico se advierte que las infracciones administrativas guardan una vinculación directa en relación al bien jurídico que se busca tutelar en cada una de ellas que no es otro que la información de las personas naturales. El objetivo de la LPDP es proteger el derecho fundamental recogido en el artículo 2 numeral 6 de la Constitución Política Peruana, referido a la intimidad personal, familiar y autodeterminación informativa. Por su parte, la Circular SBS N° G-140-2009 de Gestión de la Seguridad de la Información, que es la norma que sustenta el marco sancionador invocado por la SBS, recoge una serie de obligaciones cuya finalidad es la de controlar el “Riesgo Operacional”, entendido este como la posibilidad de ocurrencia de pérdidas en el sistema financiero debido a procesos inadecuados, fallas del personal, de la tecnología, o eventos externos. Sin perjuicio de ello, aun cuando la mitigación del riesgo operacional es el objetivo inmediato, lo cierto es que de forma mediata la referida Circular también protege a los clientes financieros, cuyos datos

personales (autodeterminación informativa) se ven comprometidos ante los incidentes de seguridad.

21.2.4. Sobre el Principio de Concurso de Infracciones:

- En el supuesto negado de que la Autoridad considere responsable al BCP por las dos imputaciones, la Autoridad no podrá sumar las penas y debería imponer únicamente aquella que sea más gravosa, basado en el Principio de Concurso de Infracciones.
- Las infracciones en las que la administrada ha incurrido se derivan de un mismo hecho, por lo que corresponderá ante la pluralidad de posibles sanciones elegir únicamente aquella que resulte más gravosa. En su ejercicio de graduación la Autoridad se encuentra sujeta a privilegiar la consecuencia de mayor gravedad, evitando un exceso de punición.
- El hecho infractor que da origen a la presunta vulneración del deber de confidencialidad engloba el mismo hecho infractor referido al incumplimiento de medidas de seguridad.

21.2.5 Sobre la excepcionalidad de responsabilidad objetiva:

- Este tipo de responsabilidad debe ser excepcional, y no puede ser aplicada a casos como la existencia de medidas de seguridad, que por la naturaleza evolucionarán con el tiempo. Ello es así debido a que en estos casos no es necesario analizar si quien realizó la acción, lo hizo de forma dolosa o negligente, sino acreditar el perjuicio y nexo de causalidad.
- No es razonable adoptar una responsabilidad objetiva ante hechos relacionados a incidentes de seguridad, esto tiene sustento en el Manual de los incidentes de seguridad informática (Computer Security Incident Handling Guide), del National Institute of Standards and Technology del Departamento de Comercio de los Estados Unidos, la misma que establece que "*las acciones preventivas basadas en la evaluación de riesgos, pueden reducir el número de incidentes, pero no todos los incidentes pueden ser prevenidos".*
- Los criterios internacionales reconocen que, no es posible evitar los incidentes de seguridad y, las prácticas de seguridad están pensadas evolucionar con el tiempo, con lo cual no es razonable establecer un mecanismo de responsabilidad objetiva en estas circunstancias.

22. Mediante Informe Técnico N° 03-2020-DFI-ORQR de 6 de enero de 2020[29], el analista de fiscalización en seguridad de la información de la DFI emitió informe complementario de 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 presentados el 26 de diciembre de 2019, concluyendo lo siguiente:

[29] Folios 278 a 281

- La administrada no ha evidenciado realizar tratamiento de datos personales de sus clientes, a través de sistemas y/o aplicativos que cuenten con una correcta y suficiente implementación de medidas de seguridad, como muestra de ello podemos indicar la sustracción de la información de un alto número de clientes acontecida en las intrusiones informáticas ocurridas.
- La administrada, en sus descargos presentados el 26 de diciembre de 2019,no ha evidenciado generar ni mantener registros de evidencias producto de la interacción lógica, que provean de manera precisa y válida información respecto a la trazabilidad de las actividades realizadas por el operador del sistema y(p aplicativos vulnerados en los dos eventos de seguridad acontecidos. Incumpliendo con lo establecido en el numeral 2 del artículo 39 del Reglamento de la LPDP.

23. Mediante Proveído de 15 de enero de 2020[30], 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.

24. Mediante escrito ingresado con Hoja de Trámite N°6047-2020MSC de fecha 28 de enero de 2020[31], la administrada dio respuesta al Proveído del 15 de enero de 2020.

25. Mediante Proveído de 11 de febrero de 2020[32], la DFI dispuso ampliar el plazo de la etapa instructiva por cincuenta (50) días hábiles adicionales.

26. Mediante la Orden de Visita de Fiscalización Nº 09-2020-JUS/DGTAIPD-DFI[33] 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.

27. Mediante Acta de Fiscalización N° 01-2020-PAS de 12 de febrero de 2020[34] se dejó constancia de los hechos verificados.

28. Mediante Informe Técnico N° 49-2020-DFI-ORQR de 21 de febrero de 2020[35], el analista de fiscalización en seguridad de la información de la DFI emitió informe sobre la visita de fiscalización del 12 de febrero de 2020 al BCP, concluyendo lo siguiente:

- 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

[30] Folio 297
[31] Folios 300 a 310
[32] Folio 311
[33] Folio 314
[34] Folios 315 a 327
[35] Folio 328

obstante, el número total de correos electrónicos remitidos y/o mensajes de texto (SMS), no corresponde a la totalidad de los clientes afectados.

29. Mediante Oficio N° 203-2020-JUS/DGTAIPD-DFI de 20 de febrero de 2020[36], la DFI requirió a la administrada remitir la resolución de inicio de procedimiento administrativo sancionador iniciado por la SBS referido en su escrito de descargos.

30. Con fecha 24 de febrero de 2020 la administrada remitió vía correo electrónico[37] con la información solicitada por la DFI.

31. Por medio de la Resolución Directoral N°044-2020-JUS/DGTAIPD-DFI del 10 de marzo de 2020[38], la DFI dio por concluidas las actuaciones instructivas correspondientes al procedimiento sancionador.

32. Mediante Informe Final de Instrucción N°030-2020-JUS/DGTAIPD-DFI del 10 de marzo de 2020[39], la DFI remitió a la Dirección de Protección de Datos Personales de la Dirección General de Transparencia, Acceso a la Información Pública y Protección de Datos Personales (en adelante, la DPDP) los actuados para que resuelva en primera instancia el procedimiento administrativo sancionador iniciado, recomendando lo siguiente:

- Imponer una sanción administrativa de multa ascendente a cinco unidades tributarias impositivas (5UIT) a la administrada por el cargo acotado en el Hecho Imputado N° 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".*
- Imponer sanción administrativa de multa ascendente a cuarenta unidades impositivas tributarias (40 UIT) a la administrada por el cargo acotado en el Hecho Imputado N°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 N° 29733".*

33. El Informe Final de Instrucción N° 030-2020-JUS/DGTAIPD-DFI así como la Resolución Directoral N°044-2020-JUS/DGTAIPD-DFI fueron notificados a la administrada mediante Oficio N°291-2020-JUS/DGTAIPD-DFI[40] el día 13 de marzo de 2020.

II. Competencia

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

[36] Folio 329
[37] Folio 330
[38] Folios 333 a 334
[39] Folios 335 a 353
[40] Folio 355

35. 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

36. 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 del Procedimiento Administrativo General (en adelante, la "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[41].

37. 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 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[42].

38. Dicho artículo debe leerse conjuntamente con lo previsto en el numeral 2 del artículo 257 de la LPAG[43], 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.

---

[41] **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."

[42] **Reglamento de la Ley de Protección de Datos Personales, aprobado por Decreto Supremo Nº 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"

[43] **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**
(…)
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."

IV. Primera cuestión previa: Sobre el Informe de Fiscalización N° 131-2019-JUS/DGTAIPD-DFI-AARM

39. En su escrito de descargos presentado el 26 de diciembre de 2019, la administrada señala que el Informe Final de Fiscalización N° 131-2019-JUS/DGTAIPD-DFI-AARM (en adelante, el "IFF") adolece de inconsistencias y omisiones que han sido también recogidas en la RD de Inicio, motivo por el cual se habrían configurado errores de valoración, pero que al no ser dicho informe un acto administrativo, corresponde hacer notar dichas inconsistencias y omisiones en el presente descargo a la RD de Inicio. Asimismo, adjuntó un Anexo N°5 a su escrito en el cual resalta cuáles serían las supuestas inconsistencias del IFF.

40. Conforme lo ha señalado la DFI en su Informe Final de Instrucción , efectivamente, el IFF no crea obligaciones adicionales a la administrada, ya que solo constituye un documento a través del cual se le pone en conocimiento cuáles serían las infracciones en las que estaría incurriendo la administrada para que ésta efectúe las acciones de enmienda que considere pertinente. De ser estas acciones corroboradas por la DFI, se evitaría el inicio de un procedimiento sancionador al considerarse dicha acción como una acción de subsanación voluntaria de la conducta infractora detectada.

41. Ahora bien, este Despacho procedió a analizar de forma minuciosa toda la documentación que obra en el expediente, así como las precisiones realizadas por la administrada al IFF como al Informe Técnico N°52-2019-DFI-VARS de 26 de marzo de 2019 y considera que no existen inconsistencias u omisiones relevantes que puedan implicar una valoración distinta, si quiera en función de una interpretación sesgada de los hechos. Ello, toda vez que, si bien en los informes referidos no se ha incorporado expresamente algunas precisiones realizadas por la administrada a las declaraciones informativas que ella misma dio frente al personal fiscalizador y que obran en las Actas de Fiscalización N°02-2019, N°03-2019 y N°04-2019, su no incorporación expresa en dichos informes no implica que no se hayan tomado en cuenta para la emisión de las opiniones técnicas.

Por el contrario, a criterio de este Despacho, conforme se desarrollará al momento de analizar si se configuró o no la existencia de los hechos infractores imputados, la consideración de las precisiones realizadas al IFF y al Informe N°52-2019-DFI-VARS, así como toda la documentación obrante en el expediente materia de análisis, sí han sido evaluados de forma integral, que es lo que corresponde para sustentar la recomendación y posterior apertura de un procedimiento administrativo sancionador.

42. Respecto al número de clientes afectados del Segundo Evento comunicado por la administrada, este Despacho también ha detectado un error involuntario en la digitación del número de afectados reportado al haberse consignado en los documentos emitidos por la DFI un millón ciento dieciséis mil cuatrocientos veinticuatro (1´116,424) en lugar de un millón ciento dieciséis mil doscientos cuarenta y dos (1´116, 242), lo cual no afecta en absoluto el análisis de fondo del caso.

V. Segunda cuestión previa: Sobre la aplicación del Principio de Tipicidad

43. La administrada alega que las imputación del incumplimiento de la medida de seguridad contemplada en el artículo 39 del numeral 2 del Reglamento de la LPDP no cumple con la observancia del principio de tipicidad, argumentando que la norma ha previsto algunas características mínimas que se deben de satisfacer para cumplir con generar y mantener registros que provean evidencia sobre la interacción de los datos lógicos, las mismas que sí habrían cumplido. Concretamente, señala que el objetivo de la disposición establecida en numeral 2 del artículo 39° del Reglamento de la LPDP, en ningún lugar establece que el sistema de registro de las interacciones lógicas deje constancia de cada una de las personas que acceden al sistema, el objetivo de esta disposición únicamente requiere que se permita saber desde qué cuenta se accede

44. Revisados los argumentos de la administrada, resulta oportuno desarrollar a detalle la obligación contenida en el artículo 39, numeral 2 del Reglamento de la LPDP sobre la medida de seguridad materia de observación por parte de la administrada, a efectos de aclarar el espíritu de la misma.

45. El tenor del numeral 2 del artículo 39 del Reglamento de la LPDP es el siguiente:

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

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

(…)

2. Generar y mantener registros que provean evidencia sobre las interacciones con los datos lógicos, incluyendo para los fines de la trazabilidad, la información de cuentas de usuario con acceso al sistema, horas de inicio y cierre de sesión y acciones relevantes. Estos registros deben ser legibles, oportunos y tener un procedimiento de disposición, entre los que se encuentran el destino de los registros, una vez que éstos ya no sean útiles, su destrucción, transferencia, almacenamiento, entre otros.

Asimismo, se deben establecer las medidas de seguridad relacionadas con los accesos autorizados a los datos mediante procedimientos de identificación y autenticación que garanticen la seguridad del tratamiento de los datos personales. (Resaltado propio)

Esta medida de seguridad consiste en que todo sistema informático, a través del cual se realice o posibilite el tratamiento de datos personales, debe generar y mantener registros que evidencien las interacciones con los datos lógicos, debiendo a su vez ser legibles y oportunos. Ello obedece a la finalidad de trazabilidad que le reconoce el Reglamento de la LPDP a estos registros, los que deben contar como mínimo en su composición con la información de cuentas de usuarios con acceso al sistema, horas de inicio y cierre de sesión del usuario, así como de las acciones relevantes de este último para poder generar con ello un historial que permita evidenciar qué usuario ingresó al sistema o aplicación, en qué momento (hora de inicio y fin) y qué acción u operación ejecutó dentro de los mismos y cómo lo hizo, incluyendo aunque no limitándose a una modificación, actualización, eliminación y/o sustracción de información (acción/evento relevante). Esto permite verificar si se efectúan o no acciones previstas y autorizadas, así como identificar al usuario (al tener este último un ID asignado y autorizado previamente por el responsable del sistema informático que maneje banco de datos personales), como también las acciones realizadas por éste en el sistema informático referido.

46. En este orden de ideas, el último párrafo del acápite normativo analizado reafirma la intención de garantizar la seguridad del tratamiento de los datos personales, en tanto complementa y refuerza la necesidad de poder contar medidas de seguridad relacionadas con los accesos autorizados a los datos mediante procedimientos de identificación y autenticación de los usuarios, permitiendo con ello identificar a las personas detrás de las cuentas de usuario que interactúan en el sistema en un determinado momento. En suma, se trata de que todo titular de banco de datos personales y/o responsable del tratamiento de los mismos debe garantizar la seguridad de los mismos mediante el establecimiento de niveles de protección apropiados según la categoría de datos personales que se trate.

47. En tal sentido, esta Dirección recoge lo establecido por la DFI en el Informe Final de Instrucción desde el punto de vista de medidas de seguridad (Folio 341 reverso):

"Cabe precisar que desde el punto de vista de medidas de seguridad resultaría poco útil conocer únicamente desde que cuenta accede el usuario si desconocemos que es lo que este ingresa a hacer en el sistema. Asimismo, es de vital importancia precisar que las interacciones o acciones realizadas por un usuario con privilegio de administrador pueden estar relacionadas a la sustracción de información ya que las características de una cuenta de administrador muchas veces es no contar con restricciones para acceder a la información.

Por tanto, se puede determinar que la administrada estaría realizando una interpretación y aplicación errada del numeral 2 del artículo 39° del Reglamento de la LPDP, ya que en este artículo describe claramente que para garantizar el correcto tratamiento de los datos personales se debe generar y mantener los registros de interacción lógica, lo que implica saber desde qué cuentas se accede y la identificación plena de las personas que interactúan en el sistema en un determinado momento, lo cual es absolutamente necesario que se pueda identificar a los usuarios que acceden al sistema, así puede identificarse de manera individual qué tipo de acción está efectuando cada uno de ellos y en atención a ello establecer los niveles de responsabilidad en caso se hiciera un tratamiento inadecuado de los datos personales."

48. En lo concerniente a la Directiva de Seguridad de la Información, la administrada refiere a que dicho documento al no tener carácter vinculante como dispositivo legal no se encuentra obligada a observar las recomendaciones que se hacen en dicho documento dirigidas a aquellos titulares de bancos de datos personales de categoría "crítica". Particularmente, refiere a la recomendación de que el registro de accesos permita identificar a la "persona o personas que realiza el acceso", siendo que el objetivo de la disposición bajo análisis únicamente, a su criterio, requiere que se permita saber desde qué cuenta se accede, pudiendo esta cuenta tratarse de una que se maneja bajo perfil tipo administrador de log de eventos.

49. Al respecto, es menester señalar que la Directiva de Seguridad de la Información lo único que hace es plasmar a nivel orientativo las obligaciones contenidas en las disposiciones del Reglamento de la LPDP en materia de medidas de seguridad. Ello, para concretar y ejemplificar lo establecido en el Reglamento de la LPDP, recogiendo la necesidad e importancia de identificar los accesos realizados para garantizar un nivel de protección adecuado exigido por la LPDP. Se trata de un documento facilitador, una especie de guía, cuyo objetivo es orientar y dar lineamientos a los administrados sobre cómo implementar y cumplir con las medidas de seguridad

mínimas requeridas por la normativa de protección de datos personales, siendo que, como bien lo señala la misma Directiva en su presentación, si los administrados pueden cumplir las medidas de seguridad con criterios o protocolos distintos pero igualmente eficientes deben recordar que su obligación es adecuarse a la LPDP y su Reglamento y no necesariamente a la Directiva.

Justamente, esa adecuación y observancia a la LPDP y su Reglamento es lo que busca la Autoridad Nacional de Protección de Datos Personales a través de la emisión de disposiciones complementarias como la Directiva en mención que lo que hace es desarrollar y precisar cómo deberían implementarse las medidas de seguridad en observancia a lo dispuesto por la normativa de protección de datos personales, habiendo sido asignada por la propia LPDP como una de sus funciones la emisión de directivas que permitan una mejor aplicación de las disposiciones de la LPDP y su Reglamento, especialmente aquellas en materia de seguridad de los bancos de datos personales, conforme ha sido reconocido en el numeral 12 del artículo 33 de la LPDP:

"Artículo 33. Funciones de la Autoridad Nacional de Protección de Datos Personales

La Autoridad Nacional de Protección de Datos Personales ejerce las funciones administrativas, orientadoras, normativas, resolutivas, fiscalizadoras y sancionadoras siguientes:

(…)

12. Emitir las directivas que correspondan para la mejor aplicación de lo previsto en esta Ley y en su reglamento, especialmente en materia de seguridad de los bancos de datos personales, así como supervisar su cumplimiento, en coordinación con los sectores involucrados.

(…)" (Subrayado propio)

50. Por lo expuesto, este Despacho concluye que no existe vulneración alguna al principio de tipicidad[44] respecto al incumplimiento de la medida seguridad exigida en el artículo 39 numeral 2 del Reglamento de la LPDP, al no habérsele exigido a la administrada obligaciones adicionales que excedan lo establecido en la normativa de protección de datos personales.

51. Adicionalmente, la administrada considera que se está vulnerando el principio de tipicidad respecto a la imputación por la presunta violación del deber de confidencialidad. Al respecto, es importante señalar que, efectivamente, la infracción al deber de confidencialidad contemplado en el artículo 17 de la LPDP se configura, como bien señala la administrada, con i) la ocurrencia de una difusión consciente y activa desde dentro de la organización que trata los datos hacia terceros no autorizados y, (ii) una omisión de seguridad relevante al interior de la organización que facilite y permita que datos que deben estar bajo reserva sean conocibles por terceros no autorizados. Esto es así, en tanto, en virtud del principio de causalidad que regula la potestad sancionadora de la Autoridad Administrativa, la responsabilidad por las infracciones cometidas no solo se determinan desde una acción activa o concreta del

[44] Artículo 248 del TUO de la LPAG:
"**Artículo 248.- Principios de la potestad sancionadora administrativa**
La potestad sancionadora de todas las entidades está regida adicionalmente por los siguientes principios especiales:
(...)
8. Causalidad.- La responsabilidad debe recaer en quien realiza la conducta omisiva o activa constitutiva de infracción Sancionable"

administrado, sino también a partir de una omisión relevante en el cumplimiento de sus obligaciones.

52. Lo expresado en el numeral anterior encuentra sustento en la propia LPDP y su Reglamento, en tanto uno de los principios rectores y esenciales que deben regir en el marco de actuación de los titulares de bancos de datos personales, encargados y/o responsables de realizar el tratamiento de los mismos para el resguardo de la integridad, disponibilidad y confidencialidad de todo dato personal involucrado en alguna de las etapas o formas de tratamiento es el principio de seguridad contemplado en el artículo 9 de la LPDP y que se encuentra complementado por lo dispuesto por el artículo 16 :

"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.

"Artículo 16. Seguridad del tratamiento de datos personales
Para fines del tratamiento de datos personales, el titular del banco de datos personales debe adoptar medidas técnicas, organizativas y legales que garanticen su seguridad y eviten su alteración, pérdida, tratamiento o acceso no autorizado.
Los requisitos y condiciones que deben reunir los bancos de datos personales en materia de seguridad son establecidos por la Autoridad Nacional de Protección de Datos Personales, salvo la existencia de disposiciones especiales contenidas en otras leyes.
Queda prohibido el tratamiento de datos personales en bancos de datos que no reúnan los requisitos y las condiciones de seguridad a que se refiere este artículo." (Subrayado propio)

53. La confidencialidad de los datos personales debe ser entendida también como uno de los fines de la seguridad que implica que no solamente se divulgue activamente datos personales a terceros no autorizados, sino que además se garantice que la información y/o datos personales necesarios para el tratamiento autorizado por sus titulares, así como la intervención para su tratamiento, sean accesibles únicamente a aquellos estrictamente necesarios y legitimados para realizar dicho tratamiento, para lo cual es imprescindible que todo titular de banco de datos y/o responsable de su tratamiento cuente con un nivel de protección suficiente, adecuado y pertinente no solo a la categoría, sino también a la cantidad de datos personales involucrados en el tratamiento que realice. En tal sentido, la LPDP, en el numeral 12 de su artículo 1, ha contemplado como definición de "Nivel suficiente de protección para los datos personales" al *"Nivel de protección que abarca por lo menos la consignación y el respeto de los principios rectores de esta Ley, así como medidas técnicas de seguridad y confidencialidad, apropiadas según la categoría de datos de que se trate."*

54. Es en este orden de ideas que la obligación de guardar confidencialidad contemplada en el artículo 17 de la LPDP, debe ser interpretada conjuntamente y en observancia del principio de seguridad antes referido, teniendo como propósitos regular tanto la obligación a no divulgar o dar a conocer los datos personales con los que alguien se relaciona en el desempeño de sus funciones, como la obligación de contar con medidas de seguridad que garanticen el nivel de protección esperado tanto por la LPDP y su Reglamento. Tales medidas de seguridad deben buscar evitar el

acceso de terceros y tratamientos no autorizados o ajenos al tratamiento y finalidad para los cuales fueron recopilados, tomando en consideración la evolución constante de la tecnología y el estado de la técnica; evaluando y conociendo los riesgos que ello involucra para propiciar la implementación de medidas técnicas proactivas y preventivas que permitan anticiparse o contrarrestar la aparición de sucesos que pongan en peligro la confidencialidad que debe primar, como regla general, en el tratamiento de todo dato personal.

55. Por lo expuesto, esta Dirección concluye que no existe vulneración alguna al principio de tipicidad, toda vez que la vulneración al deber de confidencialidad también implica una omisión de seguridad relevante que permita o facilite el acceso y tratamiento no autorizados, conforme ha quedado acreditado en el expediente materia de pronunciamiento.

VI. Tercera cuestión previa: Sobre el Non Bis In Idem aplicable al ejercicio de la potestad sancionadora administrativa

56. Los argumentos expuestos por la administrada, recogidos en el considerando 21.2.3 de la presente Resolución Directoral, refieren que se estarían configurando imputaciones que cumplen con la triple identidad de sujeto, hecho y fundamento, respecto a los procedimientos seguidos por la Autoridad Nacional de Protección de Datos Personales y la SBS por el mismo incidente y período de acontecimiento.

57. Conforme lo ha señalado el Tribunal Constitucional en reiteradas oportunidades solo en aquellos casos donde se haya verificado la concurrencia de la identidad de sujeto, hecho y fundamento jurídico se podrá alegar a favor el principio del *Non bis in ídem* y, consecuentemente, la aplicación de una sola sanción administrativa procedente de un único procedimiento administrativo sancionador. Basta que una de las tres identidades de los elementos antes referidos, los cuales deben concurrir simultáneamente, no se configure para que dicha garantía del Non bis in ídem sea desestimada, siendo procedente la tramitación de dos procedimientos en paralelo para la imposición de sanciones independientes, provenientes del análisis que se efectúe en cada procedimiento.

58. Este Despacho concuerda con la DFI respecto a la no configuración de la triple identidad de los elementos que sustentan la aplicación del principio del Non bis in ídem, toda vez que, no se da dicha identidad en el fundamento. Ello, en tanto, los fundamentos jurídicos que respaldan la potestad sancionadora de cada una de las autoridades, la SBS y la Autoridad de Protección de Datos Personales, ejercidas indistintamente dentro del marco de sus procedimientos administrativos sancionadores son distintos. En efecto, cada una de esta autoridades protege bienes jurídicos diferentes, siendo que para el caso de la Autoridad de Protección de Datos Personales el bien jurídico a proteger son los datos personales a todo nivel, garantizando con ello un adecuado tratamiento de los mismos por parte de todo titular de banco de datos personales y/o responsable para dicho tratamiento, siendo que esta protección de datos personales, también conocido como “autodeterminación informativa”, ha sido amparada constitucionalmente como derecho fundamental de toda persona natural en el artículo 2 numeral 6 de la Constitución Política. Por su lado, el bien jurídico tutelado

por la SBS, en observancia de la Ley Nº 26702, Ley General del Sistema Financiero y del Sistema de Seguros y Orgánica de la Superintendencia de Banca y Seguros (en adelante, la "LGSF") es la protección de los intereses del público en el ámbito del sistema financiero y de seguros, en tanto el Estado fomenta y garantiza el ahorro público también a nivel constitucional (artículo 87 de la Constitución Política).

59. Para mayor precisión, es necesario revisar los objetos de protección de las leyes que regulan tanto al sistema financiero y de seguros (la LGSF), así como a la protección y tratamiento de los datos personales (la LPDP), conforme se indica a continuación:

Respecto a la LGSF:

*"**Artículo 2.- Objeto de la Ley***
Es objeto principal de esta ley propender al funcionamiento de un sistema financiero y un sistema de seguros competitivos, sólidos y confiables, que contribuyan al desarrollo nacional."

El objetivo primordial de la LGSF es cautelar el correcto funcionamiento del sistema financiero que contribuya al desarrollo nacional, lo cual se condice con la protección del ahorro público en dicho sistema que reviste de reconocimiento y fomento constitucional, siendo para ello indispensable dotar de autoridad a la SBS para la protección de los aportes económicos que efectúan las personas naturales que hacen uso de los servicios financieros. En aras de este resguardo de los intereses económicos de las personas naturales y jurídicas es que la LGSF delega el rol defensor de estos intereses a la SBS:

*"**Artículo 347.- Finalidad de la Superintendencia***
Corresponde a la Superintendencia defender los intereses del público, cautelando la solidez económica y financiera de las personas naturales y jurídicas sujetas a su control, velando porque se cumplan las normas legales, reglamentarias y estatutarias que las rigen; ejerciendo para ello el más amplio control de todas sus operaciones y negocios y denunciando penalmente la existencia de personas naturales y jurídicas que, sin la debida autorización ejerzan las actividades señaladas en la presente ley, procediendo a la clausura de sus locales, y, en su caso, solicitando la disolución y liquidación del infractor."

La razón de ser de la aplicación de la LGSF se encuentra orientada a la protección del sistema financiero sólido y confiable para lo cual es importante regular la participación y desenvolvimiento de los agentes económicos que intervienen en el mismo, a efectos de garantizar al ahorrista la transparencia del funcionamiento de dicho sistema y que sus intereses económicos están siendo supervisados por el Estado a través de la SBS. En tal sentido es que dentro de las medidas de protección establecidas por la LGSF se contempla a aquellas que directamente guarden relación con la protección del ahorrista, enfocado a garantizar que el sistema financiero al cual acceden para realizar sus transacciones financieras se encuentre debidamente supervisado y alineado a las disposiciones especiales que regulan el sector financiero y de seguros. La LGSF no contiene medidas que establezcan la protección de datos personales de los ahorristas, porque el fundamento jurídico que está detrás de la misma es ajena a los datos personales, sino como se ha señalado, promover el funcionamiento de un sistema financiero y de seguros que sean competitivos, sólidos y confiables. Como muestra de ello, en el artículo 134 de la LGSF se contemplan las medidas para la protección del ahorrista, dentro de las cuales, por no ser parte de la finalidad de dicha ley, no se

contempla la protección de los datos personales de los mismos como eje central de protección.

"Artículo 134.- Medidas para la protección adecuada del ahorrista
A fin de brindar al ahorrista una protección adecuada y sin perjuicio de las demás atribuciones que le confiere la presente ley, corresponde a la Superintendencia:
1. Disponer la práctica de auditorías externas por sociedades previamente calificadas e inscritas en el registro correspondiente.
2. Supervisar que las empresas del sistema financiero se encuentren debidamente organizadas así como administradas por personal idóneo.
3. Supervisar que cumplan las empresas del sistema financiero con las normas sobre límites individuales y globales.
4. Efectuar supervisiones consolidadas de los conglomerados financieros o mixtos, de conformidad con lo dispuesto en el artículo 138.
5. Medir el riesgo de las empresas intermediarias, a través del sistema de la Central de Riesgos, mediante el registro del endeudamiento global, en el país y en el exterior, de las personas que soliciten crédito a las empresas del sistema financiero."

Por otro lado, respecto a la LPDP:

"Artículo 1. Objeto de la Ley
La presente Ley tiene el objeto de garantizar el derecho fundamental a la protección de los datos personales, previsto en el artículo 2 numeral 6 de la Constitución Política del Perú, a través de su adecuado tratamiento, en un marco de respeto de los demás derechos fundamentales que en ella se reconocen."

El objetivo principal de la LPDP es garantizar al titular del dato personal la protección de sus datos personales, orientándolo para el ejercicio de sus derechos de acceso, rectificación, cancelación y oposición (ARCO), estableciendo deberes y obligaciones mínimos a los titulares de banco de datos personales y responsables de su tratamiento, en observancia de los principios rectores reconocidos en dicha ley, para cautelar un uso adecuado de los datos personales a los cuales se accede bajo diversas modalidades de tratamiento.

60. Asimismo, resulta oportuno hacer mención a la regla general respecto al alcance que tiene la LPDP y su Reglamento a todo tratamiento de datos personales de bancos de datos personales, sean administrados por entidades públicas o privadas dentro de territorio peruano, no encontrándose ajeno al mismo toda entidad del sistema financiero.

"Artículo 3 de la LPDP. Ámbito de aplicación
La presente Ley es de aplicación a los datos personales contenidos o destinados a ser contenidos en bancos de datos personales de administración pública y de administración privada, cuyo tratamiento se realiza en el territorio nacional. Son objeto de especial protección los datos sensibles.
(…)"

"Artículo 3 del Reglamento de la LPDP.- Ámbito de aplicación.
El presente reglamento es de aplicación al tratamiento de los datos personales contenidos en un banco de datos personales o destinados a ser contenidos en bancos de datos personales.
Conforme a lo dispuesto por el numeral 6 del artículo 2 de la Constitución Política del Perú y el artículo 3 de la Ley, el presente reglamento se aplicará a toda modalidad de tratamiento de

datos personales, ya sea efectuado por personas naturales, entidades públicas o instituciones del sector privado e independientemente del soporte en el que se encuentren.
La existencia de normas o regímenes particulares o especiales, aun cuando incluyan regulaciones sobre datos personales, no excluye a las entidades públicas o instituciones privadas a las que dichos regímenes se aplican del ámbito de aplicación de la Ley y del presente reglamento.
Lo dispuesto en el párrafo precedente no implica la derogatoria o inaplicación de las normas particulares, en tanto su aplicación no genere la afectación del derecho a la protección de datos personales. (Subrayado propio)

61. Por lo expuesto, este Despacho advierte que ni la LGSF ni la Circular N° G-140-2009 sobre Gestión de la Seguridad de la Información, a la que hace mención la administrada en sus descargos, contiene una regulación que se centre en el tratamiento de datos personales de los ahorristas del sistema financiero y que dé lugar a que se pueda abordar como bien jurídico protegido por la SBS y la LGSF al derecho constitucional a la protección de datos personales. Particularmente, la finalidad de dicha Circular es establecer criterios mínimos para una adecuada gestión de la seguridad de la información, a efectos de, como bien señala la administrada*: "controlar el ´Riesgo Operacional´, entendido este como la posibilidad de ocurrencia de pérdidas en el sistema financiero debido a procesos inadecuados, fallas del personal, de la tecnología, o eventos externos* ", ello dentro de la premisa de la LGSF que -como se ha indicado líneas arriba- es velar por el correcto y transparente funcionamiento del sistema financiero.

Lo indicado en el párrafo anterior se condice con la conducta tipificada como infracción grave, contemplado en el numeral 52, Rubro II, Anexo I del Reglamento de Infracciones y Sanciones, aprobado por Resolución SBS N° 2755-2018: *"Presentar un incidente de seguridad de la información que afecte la operatividad de la empresa o la información de sus clientes, debido a la ausencia o al mal funcionamiento de controles de seguridad de la información requeridos por la normativa vigente"* (Folio 331)

62. En suma, en este escenario, se aprecia que se podría bien sancionar dos veces a un mismo sujeto por el mismo hecho, pero con la salvedad de proteger un bien jurídico distinto; no atentándose en el presente caso contra el principio del Non bis in ídem, en vista de que no concurren las tres identidades requeridas para la activación de esta garantía.

VII. Cuarta cuestión previa: Sobre el Concurso de Infracciones

63. La administrada alega que en el presente caso debería aplicarse el concurso de infracciones en tanto las infracciones imputadas derivan de un mismo hecho, por lo que ante la pluralidad de posibles sanciones debería elegirse la que resulte más gravosa. En dicha línea la administrada refiere que el hecho infractor que da origen a la presunta vulneración del deber de confidencialidad engloba el mismo hecho infractor referido al incumplimiento de medidas de seguridad (considerando 21.2.4 de la presente Resolución Directoral).

64. Al respecto, este Despacho discrepa con lo expresado por la DFI en su Informe Final de Instrucción, toda vez que se está frente a un caso de robo y filtración de datos personales por acceso y tratamiento no autorizados, producto de dos eventos ocurridos dentro del mismo año de intrusión informática, a causa de la falta de medidas de seguridad adecuadas y oportunas, encontrándose dentro de las mismas la no implementación de la medida de seguridad establecida por el numeral 2 del artículo 39 del Reglamento de la LPDP, conforme ha sido desarrollado líneas arriba.

65. El numeral 6 del artículo 248 de la LPAG establece como uno de los principios de la potestad sancionadora el del Concurso de Infracciones, en los siguientes términos:

"Artículo 248.- Principios de la potestad sancionadora administrativa
La potestad sancionadora de todas las entidades está regida adicionalmente por los siguientes principios especiales:
(…)
6. Concurso de Infracciones.- Cuando una misma conducta califique como más de una infracción se aplicará la sanción prevista para la infracción de mayor gravedad, sin perjuicio que puedan exigirse las demás responsabilidades que establezcan las leyes."

66. La Autoridad Administrativa tiene la obligación, en casos de concurso de infracciones, de aplicar la sanción por la infracción que considere más grave, sin que ello, necesariamente, deba determinarse solo por lo gravoso de la sanción -como bien señala Morón- sino por diversas cuestiones como la trascendencia de la norma infringida, de las obligaciones incumplidas o su influencia en los derechos de terceros.

67. En el presente caso, se ha evidenciado, conforme se desarrolla más adelante, que la administrada no contó con el nivel suficiente de protección para resguardar la confidencialidad de los datos personales de sus clientes, en tanto se han producido dos eventos de intrusión informática que implicaron extracción y filtración de los mismos en menos de seis meses entre uno y otro; siendo el segundo evento acontecido en noviembre de 2018 el más gravoso, toda vez que la extracción no autorizada de información de los clientes, según ha sido declarado por la propia administrada, ocurrió durante casi un mes, llegándose a obtener los datos personales de 1´116,242 de clientes adicionales (producto de la primera brecha de seguridad ocurrida en julio de 2018 se obtuvo información de 34,242 clientes).

68. En el presente caso, esta Dirección advierte que la configuración del incumplimiento del deber de confidencialidad es consecuencia de una omisión de nivel de protección adecuado y oportuno por falta de medidas de seguridad suficientes que busquen resguardar la confidencialidad y reserva de los datos personales de los clientes de la administrada.

69. Conforme se ha desarrollado en numerales anteriores, la LPDP contempla dentro de los principios rectores de obligatoria observancia para garantizar la debida protección de los datos personales, sea por el titular de los bancos de datos personales, responsables y/o encargados de su tratamiento, al principio de seguridad, recogido en su artículo 9 y complementado por su artículo 16. Dichos artículos establecen que, independientemente, del tipo de tratamiento que realicen los responsables es obligación de los mismos establecer y mantener medidas técnicas, organizativas y legales necesarias y suficientes para garantizar la seguridad de los

datos personales en su máxima expresión, evitando su alteración, pérdida, tratamiento o acceso no autorizado. En este sentido, el principio de seguridad busca garantizar y resguardar la confidencialidad de los datos personales que debe primar en todo tratamiento que no haya sido liberado de dicha carga por parte de su titular. En consecuencia, la omisión referida afecta a más de una norma jurídica, al incumplir la administrada con el mismo hecho obligaciones recogidas de forma autónoma por la LPDP, pero estrechamente vinculadas entre sí para la aplicación al presente caso.

70. Resulta pertinente tomar en cuenta que los principios rectores representan obligaciones que determinan la licitud del tratamiento de los datos personales, tanto en lo que concierne a los tipos, cantidades u oportunidad de los datos personales (principio de Finalidad, Proporcionalidad y Calidad), como a los requisitos para efectuar tal tratamiento (principio de Consentimiento, principio de Seguridad y entendido como principio, el deber de Confidencialidad)

En tal sentido, esta Dirección considera que si bien solo el principio de Seguridad se encuentra literalmente reconocido como un principio rector en el artículo 9 de la LPDP y complementado por el artículo 16 de la misma ley y el artículo 10 del Reglamento de la LPDP, no se excluye la posibilidad de admitir la misma calidad al artículo 17 de la LPDP, debiendo entenderse también que el listado de principios rectores es enunciativo, no cerrado, de acuerdo con el artículo 12 de la LPDP:

"Artículo 12. Valor de los principios
La actuación de los titulares y encargados de tratamiento de datos personales y, en general, de todos los que intervengan con relación a datos personales, debe ajustarse a los principios rectores a que se refiere este Título. Esta relación de principios rectores es enunciativa.
Los principios rectores señalados sirven también de criterio interpretativo para resolver las cuestiones que puedan suscitarse en la aplicación de esta Ley y de su reglamento, así como de parámetro para la elaboración de otras disposiciones y para suplir vacíos en la legislación sobre la materia."

71. Considerando factores generales, como el mayor ámbito de exigibilidad del cumplimiento del artículo 17 de la LPDP, así como su también valoración como principio rector del tratamiento de datos personales, es que el incumplimiento de tal artículo, que se subsume como infracción en la tipificación del literal g) del numeral 2 del artículo 132 del Reglamento de la LPDP, es la infracción de mayor gravedad.

72. En tal sentido, en caso de verificarse el incumplimiento de la medida de seguridad sobre no generar ni mantener registros de interacción lógica respecto del banco de datos personales de clientes en soporte automatizado, acotado a las aplicación y/o servicio vulnerados, tal hecho infractor no será tomado en cuenta al momento de aplicar la sanción correspondiente a la infracción tipificada en el literal a) del numeral 1 del artículo 132 del Reglamento de la LPDP.

VIII. Quinta cuestión previa: Sobre la excepcionalidad del régimen de responsabilidad objetiva

73. La administrada refiere que la responsabilidad no puede ser aplicada a casos como la existencia de medidas de seguridad, que por la naturaleza evolucionarán con

el tiempo y que en estos casos no es necesario analizar si quien realizó la acción lo hizo de una forma dolosa o negligente, sino que se debe acreditar el perjuicio o nexo de causalidad.

74. Al respecto, esta Dirección concuerda y suscribe lo establecido por la DFI en el Informe Final de Instrucción al señalar que las personas jurídicas responderán por su capacidad de cometer infracciones partiendo de la culpabilidad por defectos de organización, siendo que en el presente caso la falta de cuidado se evidencia por no haber tomado las medidas necesarias para el correcto desarrollo de sus actividades de conformidad con la normativa de protección de datos personales, conforme se desarrolla en el en el acápite VI. Análisis de las cuestiones en discusión.

75. Independientemente de ello, la LPAG establece que se prescindirá del factor subjetivo en la responsabilidad si es que por ley o decreto legislativo se dispone responsabilidad administrativa objetiva por la comisión de infracciones, así el artículo 38 de la LPDP señala lo siguiente: *"(...) Los administrados son responsables objetivamente*
por el incumplimiento de obligaciones derivadas de las normas sobre protección de datos personales". En tal sentido, la responsabilidad objetiva es aquella que no requiere el análisis de ningún factor subjetivo del sujeto infractor, prescindiéndose de los elementos de intencionalidad o imprudencia, y configurándose con la producción de la conducta calificada como infractora para la imposición de la sanción

VI. Cuestiones en discusión

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

76.1. Si la administrada es responsable por 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.

76.2. En el supuesto de resultar responsable, si debe aplicarse la exención de responsabilidad por la subsanación de la infracción, prevista en el literal f) del numeral 1 del artículo 257 de la LPAG, o las atenuantes, de acuerdo con lo dispuesto en el artículo 126 del reglamento de la LPDP.

76.3. Determinar en cada caso, la multa que corresponde imponer, tomando en consideración los criterios de graduación contemplados en el numeral 3 del artículo 248 de la LPAG.

VII. Análisis de las cuestiones en discusión

Sobre el presunto incumplimiento de la medida de seguridad contemplada en el numeral 2 del artículo 39 de la LPDP

77. El El Título I de la LPDP establece los principios rectores para la protección de datos
personales, entre ellos el principio de Seguridad, regulado en el artículo 9 de dicha ley:

*"**Artículo 9. Principio de seguridad***
El titular del banco de datos personales y el encargado de su tratamiento deben adoptar las medidas técnicas, organizativas y legales necesarias para garantizar la seguridad de los datos personales. Las medidas de seguridad deben ser apropiadas y acordes con el tratamiento que se vaya a efectuar y con la categoría de datos personales de que se trate."

78. A mayor abundamiento, el artículo 16 de la LPDP y el artículo 10 del Reglamento de la LPDP señalan como objetivo de la adopción de tales medidas técnicas, organizativas y legales, evitar la alteración, pérdida, tratamiento o acceso no autorizado a los datos personales, en los siguientes términos:

Artículo 16 de la LPDP:

"Artículo 16. Seguridad del tratamiento de datos personales
Para fines del tratamiento de datos personales, el titular del banco de datos personales debe adoptar medidas técnicas, organizativas y legales que garanticen su seguridad y eviten su alteración, pérdida, tratamiento o acceso no autorizado.
Los requisitos y condiciones que deben reunir los bancos de datos personales en materia de seguridad son establecidos por la Autoridad Nacional de Protección de Datos Personales, salvo la existencia de disposiciones especiales contenidas en otras leyes.
Queda prohibido el tratamiento de datos personales en bancos de datos que no reúnan los requisitos y las condiciones de seguridad a que se refiere este artículo."

Artículo 10 del Reglamento de la LPDP:

"Artículo 10.- Principio de seguridad.
En atención al principio de seguridad, en el tratamiento de los datos personales deben adoptarse las medidas de seguridad que resulten necesarias a fin de evitar cualquier tratamiento contrario a la Ley o al presente reglamento, incluyéndose en ellos a la adulteración, la pérdida, las desviaciones de información, intencionales o no, ya sea que los riesgos provengan de la acción humana o del medio técnico utilizado."

79. Por su parte, sobre el tratamiento automatizado de datos personales, el artículo 39 del Reglamento de la LPDP contempla el requisito de tener documentados los procedimientos de gestión de accesos, de privilegios, de verificación periódica de privilegios, así como los registros de interacción lógica:

"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.

2. Generar y mantener registros que provean evidencia sobre las interacciones con los datos lógicos, incluyendo para los fines de la trazabilidad, la información de cuentas de usuario con acceso al sistema, horas de inicio y cierre de sesión y acciones relevantes. Estos registros deben ser legibles, oportunos y tener un procedimiento de disposición, entre los que se encuentran el destino de los registros, una vez que éstos ya no sean útiles, su destrucción, transferencia, almacenamiento, entre otros.

Asimismo, se deben establecer las medidas de seguridad relacionadas con los accesos autorizados a los datos mediante procedimientos de identificación y autenticación que garanticen la seguridad del tratamiento de los datos personales."

80. En la RD de Inicio se le imputó a la administrada el incumplimiento de la obligación contenida en el numeral 2 del artículo 39 del Reglamento de la LPDP al no haber cumplido con implementar la medida de seguridad relativa a la generación y mantenimiento de registros de interacción lógica respecto del banco de datos personales de clientes en soporte automatizado, acotando dicho supuesto a las aplicaciones/sistemas que sufrieron intrusiones informáticas en los meses de julio y noviembre de 2018 de acuerdo a lo comunicado por la administrada el 26 de julio de 2018 y el 23 de noviembre de 2018, respectivamente.

81. Dicha disposición establece, para el caso materia de análisis, la obligación a cargo de los titulares de banco de datos personales y/o responsables de su tratamiento de tener registro de los pormenores de cada operación relacionada al tratamiento de los mismos, como la identidad de quién la efectuó, el momento en que se realizó y en qué consistió. Como ha sido desarrollado en el acápite correspondiente a la Segunda Cuestión Previa, el fin de la trazabilidad de las acciones relevantes realizadas que regula el artículo 39 inciso 2 del Reglamento de la LPDP es generar y mantener un historial que permita evidenciar qué usuario ingresó al sistema o aplicación, en qué momento (hora de inicio y fin) y qué acción u operación ejecutó dentro de los mismos y cómo lo hizo (acción/evento relevante), permitiendo evidenciar con ello las acciones realizadas en el sistema respecto al manejo de la información por parte de aquellos involucrados en el tratamiento de los datos personales vinculados a dicho sistema o aplicación.

82. En el presente caso, a pesar que la administrada alega haber cumplido con la medida de seguridad exigida por el numeral 2 del artículo 39 del Reglamento de la LPDP no ha logrado acreditar fehacientemente que la aplicación vulnerada por las intrusiones acontecidas en los meses de julio y noviembre de 2018 (que evidentemente manejaba banco de datos personales, siendo estos últimos sustraídos) incluyó en su funcionamiento la generación y mantenimiento de registros que evidencien sobre las interacciones con los datos lógicos, incluyendo para los fines de trazabilidad, información de quiénes accedieron al mismo, en qué momento y cuáles fueron las acciones que llevó a cabo en el mismo.

83. De la documentación obrante en el expediente, respecto al primer evento de julio 2018 (Brecha de seguridad ocurrida el 7 de julio de 2018), se evidencia que la administrada no ha acreditado que la aplicación y/o sistema vulnerado haya contado con la medida de seguridad referida al generar y mantener registros de interacción

lógica, ni siquiera antes de la fecha de ocurrencia del evento, lo cual a criterio de esta Dirección resultaba sumamente importante tener implementada, considerando que, como ha sido declarado por la propia administrada y obra en el Acta N° 02-2019: i) sobre el esquema de desarrollo de la aplicación vulnerada, el acceso tipo administrador lo tenía el personal de la mesa ágil y ii) no contaban con herramientas informáticas que contaran con la función de registro de los eventos relacionados con la liberación de nuevas versiones del software (Folio 49).

Conforme obra en el Acta de Fiscalización N°02-2019, respecto al evento notificado con fecha 26 de julio de 2018, la administrada precisó al personal fiscalizador *"que la aplicación en cuestión sí contaba con medidas de seguridad, sin embargo, al contar con una infraestructura diferente a otras aplicaciones del Banco, la capacidad de monitorear todas la actividades se encontraba en proceso de implementación, por tanto en dicho momento no se encontraba completamente alineado a las políticas de seguridad"* (Folio 49), siendo que previamente a ello, había informado que una de las medidas de seguridad implementadas a consecuencia del incidente de seguridad era justamente "*la implementación de herramientas automatizadas para la generación de los log de eventos"* (literal c) del numeral 5 del Acta N°02-2019 sobre las medidas de seguridad implementadas a consecuencia del incidente de seguridad-Folio 48). Asimismo, frente a lo declarado en el numeral 3 de dicha acta respecto a que no contase con log de eventos debido a que el responsable de la intrusión deshabilitó la generación de los log de eventos (Folio 47), la administrada precisó que *"la carencia de los logs de eventos no obedecen necesariamente a una deshabilitación de los logs"* (Folio 49).

84. Lo descrito en el considerando anterior guarda relación con la declaración brindada por la administrada en su escrito de absolución de requerimiento de información complementaria a la DFI ingresado con Hoja de Trámite N° 55666-2018MSC de 28 de agosto de 2018, en el cual señaló lo siguiente (Folio 11):

"Por otro lado, con respecto a las medidas de seguridad del aplicativo antes de la intrusión, indicamos que el mismo contaba con lo siguiente:
i) Roles y perfiles de usuarios para la administración de la infraestructura y las herramientas.
ii) Alertas para cualquier modificación a nivel de accesos.
iii) Procedimiento de altas y bajas de usuarios.
iv) Matriz de herramientas y sus respectivos niveles de acceso.
Sin embargo, este aplicativo tenía una infraestructura diferente a otras aplicaciones del BCP, dado que al residir parte de sus componentes en la infraestructura cloud de Amazon, nuestra capacidad de monitorear completamente todas las actividades sobre estos componentes se encontraba en proceso de implementación; por tanto, no se encontraba en dicho momento completamente alineado a nuestras políticas de seguridad." (Subrayado propio)

85. Respecto al evento de noviembre 2018 (Brecha de seguridad identificada el 12 de noviembre de 2018), también se evidencia de la documentación analizada que la administrada no ha acreditado que la aplicación y/o sistema vulnerado contaba con la medida de seguridad referida al generar y mantener registros de interacción lógica.

86. En este escenario, resulta oportuno remitirnos a las conclusiones de los Informes Técnicos N° 052-2019-DFIVARS del 26 de marzo de 2019 (Folios 194 a 198) y N°03-2020-DFI-ORQR del 6 de enero de 2020 (Folios 278 a 281),emitidos por personal de

fiscalización en seguridad de la información de la DFI, sobre el resultado de la evaluación de implementación de medidas de seguridad respecto a las dos vulneraciones informáticas comunicadas por la administrada, de las cuales se desprende que la administrada no ha acreditado haber contado con la medida de seguridad requerida por el numeral 2 del artículo 39 del Reglamento de la LPDP implementada en el aplicativo/sistema vulnerado, ni antes ni después de los momentos en los que se identificaron cada una de las brechas de seguridad reportadas por la administrada.

87. Por lo expuesto en el presente acápite, este Despacho concluye que sí se ha configurado la infracción imputada respecto al incumplimiento de la medida de seguridad contenida en el numeral 2 del artículo 39 del Reglamento de la LPDP. No obstante ello, tal y como ha sido referido en el desarrollo de la Cuarta Cuestión Previa, en aplicación del concurso de infracciones advertido, para el presente caso, la responsabilidad derivada de este incumplimiento de medida de seguridad sobre no generar ni mantener registros de interacción lógica respecto del banco de datos personales de clientes en soporte automatizado, acotado a la aplicación y/o servicio vulnerados, será subsumida en la sanción de multa correspondiente a la infracción de mayor gravedad por incumplimiento de la obligación de confidencialidad del artículo 17 de la LPDP.

Sobre el presunto incumplimiento del deber de confidencialidad

88. En la RD de Inicio se imputó como hecho infractor que la administrada no habría garantizado la confidencialidad de los datos personales de sus clientes al permitir a terceros no autorizados el acceso a estos, incumpliendo con el deber de confidencialidad recogido en el artículo 17 de la LPDP.

89. Conforme ha sido desarrollado en la Segunda Previa, la configuración de la infracción al deber de confidencialidad se da por i) la ocurrencia de una difusión consciente y activa desde dentro de la organización que trata los datos hacia terceros no autorizados o, (ii) una omisión de seguridad relevante al interior de la organización que facilite y permita que datos que deben estar bajo reserva y resguardo de un titular de banco de datos personales sean conocibles por terceros no autorizados.

Conforme se verá en el presente acápite, a criterio de esta Dirección, la administrada ha incurrido en este segundo escenario de incumplimiento al quedar evidenciado que la misma no contó con un nivel suficiente de protección de los datos personales, implementado de forma preventiva, en los sistemas automatizados que sufrieron las brechas de seguridad notificadas con fecha 26 de julio y 23 de noviembre de 2018.

90. Debe entenderse el deber de confidencialidad como un pilar clave que debe regir en toda forma de tratamiento de datos personales para garantizar una adecuada protección de los mismos, evitando que sean expuestos y/o tratados para fines distintos sin el consentimiento de sus titulares. Es en este sentido que este deber de confidencialidad está estrechamente vinculado, como ha sido expuesto en la Segunda Cuestión Previa (considerandos 51 a 55 de esta Resolución Directoral) al principio de seguridad en tanto no puede garantizarse la primera sin la implementación de medidas técnicas, organizativas y legales preventivas a los riesgos conocidos e inherentes de

toda actividad relacionada a sistemas y/o servicios informáticos a través de los cuales se traten datos personales o estén vinculados al acceso de los mismos.

91. En reconocimiento de dicha importancia y carácter esencial de confidencialidad y privacidad que deben revestir *per se* para la protección de los datos personales, es que
los Estándares Iberoamericanos de Protección de Datos[45] regulan la privacidad por diseño y privacidad por defecto en su artículo 38:

*"**38. Privacidad por diseño y privacidad por defecto***
38.1. El responsable aplicará, desde el diseño, en la determinación de los medios del tratamiento de los datos personales, durante el mismo y antes de recabar los datos personales, medidas preventivas de diversa naturaleza que permitan aplicar de forma efectiva los principios, derechos y demás obligaciones previstas en la legislación nacional del Estado Iberoamericano que le resulte aplicable.
38.2. El responsable garantizará que sus programas, servicios, sistemas o plataformas informáticas, aplicaciones electrónicas o cualquier otra tecnología que impliquen un tratamiento de datos personales, cumplan por defecto o se ajusten a los principios, derechos y demás obligaciones previstas en la legislación nacional del Estado Iberoamericano que le resulte aplicable.
Específicamente, con el fin de que únicamente sean objeto de tratamiento el mínimo de datos personales y se limite la accesibilidad de éstos, sin la intervención del titular, a un número indeterminado de personas." (Subrayado propio)

Si bien, se advierte un error material en el último párrafo de este artículo 38 (en tanto debe limitarse el acceso a los datos personales involucrados en algún tratamiento a un número determinado de personas), el espíritu del mismo es el reconocer la importancia y necesidad de que todo titular de banco de datos personales y/o responsable de su tratamiento aplique una política de privacidad a lo largo del ciclo de vida, de algún programa, servicio, sistema, plataforma informática, aplicación o cualquier otra tecnología que desarrolle o implemente y que implique cualquier forma de tratamiento de datos personales de sus clientes, inclusive desde antes que dicho proyecto se lleve a cabo y/o materialice; ello, a efectos de prever eventos y riesgos antes de que los mismos puedan concretarse. Y esto, únicamente, puede darse instaurando medidas de seguridad que respondan a un nivel suficiente y adecuado de protección de los datos personales, más aún cuando el titular de banco de datos ha sido previamente – en un plazo no menor de cuatro meses, considerando que la primera brecha tuvo lugar el 7 de julio de 2018 y la segunda brecha, conforme lo informado por la administrada a la SBS desde el 8 de octubre de 2018 - pasible de una brecha de seguridad de características similares como en el presente caso de análisis.

92. La pérdida de la confidencialidad que debe revestir todo tratamiento de datos personales -sea por una conducta proactiva o negligente al interior de una organización o por una omisión relevante en la implementación de medidas de seguridad para el resguardo de la misma que permita o facilite en ambos casos que terceros no legitimados accedan o traten tales datos personales de forma indebida-, implica un riesgo para los derechos y poder de control sobre la información personal

[45] Red Iberoamericana de Protección de Datos (2017). Estándares de Protección de Datos Personales para los Estados Iberoamericanos, p.30

de cada uno de sus titulares, cuya gravedad se encuentra condicionada al tipo de tratamiento y fines a los que se destine el uso de los mismos.

93. En el presente caso, 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)

94. En opinión de esta Dirección, el quebrantamiento del deber de confidencialidad de la administrada se arraiga en el hecho de no haber implementado medidas de seguridad suficientes y adecuadas a los procesos de desarrollo de la aplicación/sistema vulnerados de manera proactiva que anticipen y prevengan escenarios de riesgo por accesos o tratamientos no autorizados respecto a los datos personales que custodian, más aún cuando se encontraban en posibilidad de hacerlo. Nos encontramos frente a una entidad que una vez detectadas las brechas de seguridad, si bien ha actuado de manera reactiva, activando protocolos y tomando acciones internas para mitigar el tratamiento indebido de los datos personales de sus clientes, también estuvo en mejor posición para llevar a cabo acciones preventivas a fin de evitar la generación de las mismas, mas no lo hizo. Además de ello, cabe resaltar que 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.

95. Por el contrario, respecto a la primera brecha seguridad acontecida en el mes de julio de 2018 la propia administrada ha reconocido en sus declaraciones que no contaba con medidas de seguridad suficientes en el aplicativo vulnerado. Conforme consta en el escrito de absolución de requerimiento de información complementaria a la DFI ingresado con Hoja de Trámite N° 55666-2018MSC de 28 de agosto de 2018, en el cual señaló lo siguiente (Folio 11):

"Por otro lado, con respecto a las medidas de seguridad del aplicativo antes de la intrusión, indicamos que el mismo contaba con lo siguiente:
i) Roles y perfiles de usuarios para la administración de la infraestructura y las herramientas.
ii) Alertas para cualquier modificación a nivel de accesos.
iii) Procedimiento de altas y bajas de usuarios.
iv) Matriz de herramientas y sus respectivos niveles de acceso.
Sin embargo, este aplicativo tenía una infraestructura diferente a otras aplicaciones del BCP, dado que al residir parte de sus componentes en la infraestructura cloud de Amazon, nuestra capacidad de monitorear completamente todas las actividades sobre estos componentes se encontraba en proceso de implementación; por tanto, no se encontraba en dicho momento completamente alineado a nuestras políticas de seguridad." (Subrayado propio)

Asimismo, tal como consta en el Acta de Fiscalización N°02-2019, el Gerente del Área de Infraestructura de TI de la administrada precisó al personal fiscalizador *"que la*

aplicación en cuestión sí contaba con medidas de seguridad, sin embargo, al contar con una infraestructura diferente a otras aplicaciones del Banco, la capacidad de monitorear todas la actividades se encontraba en proceso de implementación, por tanto en dicho momento no se encontraba completamente alineado a las políticas de seguridad" (Folio 49). (Subrayado propio)

Así también en dicha fiscalización se dejó constancia respecto al esquema bajo el cual fue implementado el desarrollo de la aplicación vulnerada (Folio 47):

"a) Acceso de tipo administrador en todo el proceso de desarrollo del aplicativo (servidor, base de datos, herramientas de desarrollo, servicio de extracción de datos y administración de log de eventos) al personal encargado (equipo de desarrollo).
b) Utilización de metodología de desarrollo de software sin contar con los controles de seguridad suficientes.
c) No contar con las herramientas informáticas que cuenten con la función de registro de los eventos."

Sobre el esquema informado, la administrada precisó lo siguiente (i) *"sobre el literal a) cabe precisar que el acceso tipo administrador lo tenía el personal de mesa ágil que gestionaba el aplicativo afectado"* y (ii) "*sobre el punto c) precisamos que no se contaba con herramientas informáticas que cuenten con la función de registro de los eventos relacionados con la liberación de nuevas versiones del software."* (Folio 49)

96. De lo hasta aquí descrito, este Despacho advierte que la administrada no actuó con un nivel adecuado de protección suficiente para el resguardo de la confidencialidad de los datos personales involucrados en el desarrollo del aplicativo vulnerado. Prueba de ello, es que la administrada a pesar de saber que se trataba de un aplicativo distinto en cuanto a la infraestructura usada y que la misma no se encontraba alineada completamente a sus políticas de seguridad, decidió continuar con el desarrollo del aplicativo bajo un esquema de implementación que no buscara garantizar la confidencialidad, integridad y disponibilidad de los datos personales vinculados a dicho aplicativo. Esto último, en tanto ni siquiera implementó controles necesarios para identificar y segregar las acciones realizadas por cada una de las personas que conformaban el equipo de la mesa ágil que gestionaba el desarrollo de la aplicación vulnerada, resultando dicha omisión crítica a nivel preventivo en tanto cada una de dichas personas manejaban acceso tipo administrador, implicando ello, a criterio de esta Dirección, una falta de adopción de metodología de desarrollo segura para minimizar el riesgo de una posible vulneración a sus sistemas.

97. Sobre la segunda brecha de seguridad detectada en noviembre de 2018, la administrada no implementó medidas de seguridad suficientes y efectivas que eviten la existencia de vulnerabilidades similares a la acontecida por acceso y tratamiento no autorizados de terceros, siendo prueba de ello, i) el no haber incluido en el funcionamiento del aplicativo vulnerado la generación y mantenimiento de registros que evidencien sobre las interacciones con los datos lógicos, incluyendo para los fines de trazabilidad, información de quiénes accedieron al mismo, en qué momento y cuáles fueron las acciones que llevó a cabo en él (medida de seguridad exigida por el numeral 2 del artículo 39 del Reglamento de la LPDP), y ii) el no haber implementado previamente y de forma integral aquellas medidas técnicas de seguridad que declaró haber implementado como consecuencia de la primera intrusión informática, las

mismas que constan en el numeral 5 del Acta de Fiscalización N°03-2019 (Folio 57) y en el escrito de la administrada ingresado mediante Hoja de Trámite N° 17396-2019-MSC (Folios 89 a 91)

98. Efectivamente, en el Acta de Fiscalización N° 04-2019 consta la declaración de la administrada respecto a lo señalado en el considerando anterior: *"si bien se habían implementado las medidas del numeral 5 del Acta N° 02-2019 en la fecha en que se identificó este evento las medidas del numeral 1 del Acta N°03-2019 se encontraban a noviembre de 2018 en proceso de implementación. Cabe precisar que a la fecha estas medidas se encuentran implementadas."* (Folio 85). (Subrayado propio)

En tal sentido, este Despacho aprecia que las medidas referidas en el numeral 1 del Acta N°03-2019 (Folio 57) que no habían sido aún implementadas y que hubieren servido a su vez para mitigar el riesgo de la comisión de esta segunda brecha fueron las siguientes:

"1. La fiscalizada informó que a raíz de la intrusión informática de 26 de julio de 2018, implementó las siguientes medidas respecto a las aplicaciones que desarrollan:
a. Análisis del código fuente de las aplicaciones a través de la aplicación Fortify.
b. Análisis de los servidores por aplicación Qualys.
c. Revisión de pares (revisión de código por parte de un encargado).
d. Revisión de la arquitectura (alineación a los estándares NIST-Framework JF).
e. No pase a producción de las aplicaciones consideras críticas.
f. Análisis de seguridad funcional por parte de los analistas de seguridad."

99. Lo descrito en el considerando anterior guarda relación con la declaración brindada por la administrada en su escrito de absolución de requerimiento de información complementaria a la DFI ingresado con Hoja de Trámite N° 74313-2018MSC de 23 de noviembre de 2018, en el cual señaló lo siguiente (Folio 26):

"Así, el 12 de noviembre, durante la ejecución de un pase a producción del aplicativo en cuestión y cuando éste se encontraba fuera de línea, se identificó que aún continuaban ingresando operaciones de consultas de datos de clientes. Al realizar la revisión se encontró que desde una IP externa, a través de un BOT (robot) que contaba con el "Apikey" (llave), se estaba permitiendo el ingreso a la infraestructura del BCP a fin de capturar datos de clientes." (Subrayado propio)

100. Acerca de la segunda brecha, este Despacho observa que dentro del contexto en el que se encontraba la administrada (esto es el haber sufrido una brecha de seguridad reciente que implicó sustracción de datos personales de sus clientes a causa de un acceso no autorizado en la etapa de desarrollo de un aplicativo propio), ésta se encontraba en mejor posición para prevenir y contrarrestar un suceso similar, siendo que, nuevamente, actuó de forma negligente. Prueba de ello, es que recién detectaron que se ha había generado una segunda brecha de seguridad el 12 de noviembre de 2018 cuando la misma venía ocurriendo durante casi un mes, implicando con ello la sustracción de información correspondiente a 1´116, 242 de sus clientes y, su posterior filtración en el "Deep Web"

La propia administrada informó a la DFI que la segunda brecha de seguridad se produjo por un periodo aproximado de un mes. Ello puede apreciarse del numeral 5

del Acta de Fiscalización N° 04-2019 (Folio 84): *"5. La fiscalizada informó que la intrusión informática fue realizada por un período aproximado de un mes"*, así como en el Oficio N° 47405-2019-SBS de la SBS notificado a la administrada el 05 de diciembre de 2019 (Folio 331): *"Al respecto, se cuenta con información que indica que entre el 08.10,2018 y el 12.11.2018 se produjo sustracción de la información personal de 1'116,242 clientes a través del sistema web Loans, provisto por el Banco, el cual permite la solicitud y desembolso de créditos efectivos en línea para un grupo de clientes"* (Subrayado propio)

101. Asimismo, resulta pertinente traer a colación el incumplimiento de medida de seguridad sobre no generar ni mantener registros de interacción lógica respecto del banco de datos personales de clientes en soporte automatizado, respecto al aplicativo vulnerado, desarrollado en los considerandos 77 a 87 anteriores. Ello, toda vez que demuestra la falta de implementación de los controles necesarios para el seguimiento, verificación y determinación de las acciones realizadas por el personal involucrado en el desarrollo de la aplicación vulnerada, tomando en cuenta que el acceso tipo administrador lo tenía el personal de la mesa ágil, conforme lo declarado por la propia administrada, para lo cual resultaba esencial y necesario identificar quién, en qué momento y qué acción relevante llevó a cabo en la aplicación vulnerada a manera de prevención y alerta ante el primer indicio de tratamiento no autorizado y/o indebido.

102. Conociendo el riesgo que ello implicaba, la administrada no implementó correctamente la medida de seguridad establecida en el numeral 2 del artículo 39 del Reglamento de la LPDP, ni alguna otra que permita evitar o mitigar el riesgo que implicaba otorgar el uso de cuenta tipo administrador a todo el personal de la mesa ágil sin poder identificar las acciones que realizaba cada uno sobre el aplicativo vulnerado, constituyendo un agravante el hecho de que la mesa ágil estaba conformada por personal interno y externo, tal y como declaró la administrada en el Acta de Fiscalización N° 04-2018 (Folio 83) al hacer referencia a la medida correctiva de desvinculación de personal.

Tal situación no le permitió a la administrada tener un control sobre el tratamiento al que estaban expuestos los datos personales de sus clientes por parte del personal de la mesa ágil de desarrollo de la aplicación vulnerada desde el mes de julio de 2018, en adelante, hasta la ocurrencia de la segunda brecha de seguridad, detectada recién en noviembre de 2018 (después de que se venían sustrayendo datos personales de los clientes desde hace casi un mes atrás).

103. Conforme obra en el Acta de Fiscalización N° 04-2018 (Folio 83), la administrada señaló que la intrusión de 12 de noviembre de 2018, se originó debido a que un IP externo administraba un Bot (robot) que contaba con el Apikey (llave) que validaba el acceso a dicha aplicación y permitía la sustracción de los datos personales de sus clientes. Así también informó que como medidas correctivas (i) procedió a desvincular a todos los trabajadores (internos y externos) que participaron en el desarrollo de la aplicación vulnerada, (ii) dio de baja el servicio de manera temporal con la finalidad de cambiar el Apikey vulnerado y (iii) no realizó nuevas versiones de dicha aplicación. Al respecto, este Despacho concuerda con la DFI al señalar que ello exterioriza la falta de medidas de seguridad necesarias para poder identificar qué y quién realizó determinada actividad, siendo que pese a que se sabía que la intrusión fue efectuada

por alguien que contaba con una llave que validaba el acceso, no se pudo identificar quién realizó la extracción de los datos personales, vulnerando con ello el deber de confidencialidad exigida a los titulares de los bancos de datos personales.

104. Finalmente, en lo que concierne a lo señalado por la administrada respecto a que la materialización de los incidentes descritos son consecuencia del riesgo inherente al proceso de transformación digital, el cual requiere del elemento humano para desarrollarse, este Despacho suscribe lo señalado por la DFI al indicar que la seguridad en los tratamientos debe de entenderse como un proceso y no como un estado. Las medidas de seguridad necesariamente tienen que evolucionar paralelamente al entorno en el que los tratamientos tienen lugar, para lo cual es estrictamente necesario que todo titular de banco de datos personales identifique de forma anticipada riesgos asociados a posibles debilidades de las que puedan ser pasibles sus sistemas y actúe de manera proactiva y preventiva para evitar que amenazas a los mismos se materialicen. En el presente caso, conforme se ha podido advertir, la administrada pudo prevenir la generación de ambas brechas de seguridad, por el contexto en el que se encontraba frente a cada brecha. Esto es, para la primera brecha, porque teniendo la certeza que la aplicación vulnerada no se encontraba completamente alineada a sus protocolos de seguridad decidió proceder con el desarrollo de nuevas versiones de la misma, así como por no tener implementado correctamente la medida de seguridad del numeral 2 del artículo 39 del Reglamento de la LPDP y otorgar al personal desarrollador acceso tipo administrador lo cual incrementa la probabilidad para la generación de una vulneración asociada a un acceso no autorizado y/o indebido. Respecto a la segunda brecha, porque continuó sin haber implementado la medida de seguridad del numeral 2 del artículo 39 del Reglamento de la LPDP y por no haber instaurado en su totalidad las medidas de seguridad referidas en el numeral 1 del Acta N°03-2019 (Folio 57) descritas en el numeral 98 de esta Resolución pese a haber sufrido un incidente de características similares y encontrarse propensos a lo mismo.

105. Por lo expuesto en el presente acápite, este Despacho concluye que sí se ha configurado la infracción imputada respecto al incumplimiento de la obligación de confidencialidad contemplada en el artículo 17 de la LPDP.

Sobre las sanciones a aplicar a la infracción

106. La Tercera Disposición Complementaria Modificatoria del Reglamento del Decreto Legislativo N° 1353, 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 de dicho reglamento, que en adelante tipifica las infracciones.

107. 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 cero coma cinco (0,5) unidades impositivas tributarias hasta una multa de cien (100) unidades impositivas tributarias[46], sin perjuicio de las medidas correctivas que puedan determinarse de acuerdo con el artículo 118 del Reglamento de la LPDP[47].

[46] **Ley N° 29733, Ley de Protección de Datos Personales**

108. En el presente caso, se ha establecido la responsabilidad de la administrada por lo siguiente:

i) No 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, incumpliendo la obligación contenida en el numeral 2 del artículo 39 del Reglamento de la LPDP; con lo cual se configuraría la infracción leve tipificada en el literal a) del numeral 1 del artículo 132 del Reglamento de la LPDP, infracción sancionable con una multa mínima desde cero coma cinco de una unidad impositiva tributaria (0,5UIT) hasta cinco unidades impositivas tributarias (5UIT).

ii) No haber garantizado la confidencialidad de los datos personales de sus clientes, al permitir a terceros no autorizados el acceso a estos, a causa de una omisión de seguridad relevante; incumpliendo lo dispuesto en el artículo 17 de la LPDP; con lo cual se configuraría la infracción grave tipificada en el literal g) del numeral 2 del artículo 132 del Reglamento de la LPDP, infracción sancionable con una multa desde más de cinco unidades impositivas tributarias (5UIT) hasta cincuenta unidades impositivas tributarias (50UIT).

109. Por la existencia del concurso de infracciones detallado en la Cuarta Cuestión Previa, debe reiterarse en este punto que la sanción por la responsabilidad derivada del primer hecho infractor será será subsumida en la sanción de multa correspondiente a la infracción de mayor gravedad por incumplimiento de la obligación de confidencialidad del artículo 17 de la LPDP.

110. Cabe señalar que esta Dirección determina el monto de la multa a ser impuesta tomando en cuenta para su graduación los criterios establecidos en el numeral 3 del artículo 248 de la LPAG. En tal sentido, debe prever que la comisión de la conducta sancionable 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.

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

[47] **Reglamento de la Ley de Protección de Datos Personales, aprobado por Decreto Supremo 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."

111. En el presente caso, se considera como criterios relevantes para graduar las sanciones, los siguientes:

Respecto al hecho infractor a sancionar:

a) El beneficio ilícito resultante por la comisión de la infracción:

La administrada ha evitado el costo asociado a la implementación de medidas de seguridad idóneas que garanticen la confidencialidad de la información los datos personales de sus clientes que se encontraban vinculados a la aplicación/sistema vulnerados. Conforme ha sido expuesto en la presente Resolución Directoral, la administrada se encontraba en posibilidad de actuar preventivamente y evitar la ocurrencia de las brechas de seguridad detectadas en julio y noviembre de 2018. La primera, por decidir realizar actividades de desarrollo sin que la aplicación se encuentre totalmente alineada a sus protocolos de seguridad, otorgando acceso tipo administrador a todo el personal de la mesa ágil encargada de la gestión de desarrollo lo cual aunado al hecho de no tener debidamente implementado lo dispuesto en el numeral 2 articulo 39 del Reglamento de la LPDP acentuó la probabilidad de un acceso no autorizado y/o indebido. Respecto a la segunda brecha, porque continuó sin haber implementado la medida de seguridad del numeral 2 del artículo 39 del Reglamento de la LPDP y por no haber instaurado en su totalidad las medidas de seguridad referidas en el numeral 1 del Acta N°03-2019 (Folio 57) descritas en el numeral 98 de esta Resolución pese a haber sufrido un incidente de características similares y encontrarse propensos a lo mismo.

b) La probabilidad de detección de las infracciones:

La probabilidad de detección de la conducta infractrora es baja, debido a que fue la propia administrada quien comunicó a la Autoridad Nacional de Protección de Datos Personales la ocurrencia de las brechas de seguridad, con fechas 26 de julio de 2018 y 23 de noviembre de 2018, respectivamente.

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

En particular, se ha evidenciado que la administrada no ha cumplido con garantizar un nivel suficiente de protección de los datos personales de sus clientes vinculados a la aplicación vulnerada, al no haber implementado medidas de seguridad idóneas que busquen resguardar la confidencialidad de los mismos, orientando su actuar a prevenir el acceso y tratamiento por terceros no autorizados.

Como consecuencia de la primera brecha de seguridad detectada en el mes de julio de 2018 se ha comprometido la confidencialidad de 34, 242 clientes, respecto a la siguiente información:

- 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.
- Saldos de 21,129 cuentas pertenecientes a 18,305 clientes.

De la segunda brecha de seguridad detectada en noviembre, pero que venía produciendo efectos de sustracción de información desde el mes de octubre de 2018 se comprometió la confidencialidad de 1´116, 242 clientes, respecto a 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.
- Saldos de las cuentas de 1,176 clientes

En menos de cuatro meses la administrada sufrió dos brechas de seguridad de similares características, siendo que frente amabas aquella se encontró en la posibilidad de evitar la materialización de tales brechas conforme ha sido desarrollado. 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.

d) <u>El perjuicio económico causado:</u>

No se evidencia un perjuicio económico resultante de la comisión de la infracción.

e) <u>La reincidencia en la comisión de la infracción:</u>

La administrada no fue sancionada anteriormente por la infracción.

f) Las circunstancias de la comisión de la infracción:

Este Despacho advierte que la administrada no ha llevado a cabo actuaciones de enmienda, en tanto no ha cumplido con implementar medidas de seguridad necesarias para impedir que se genere una nueva brecha de seguridad en un período de tiempo corto desde el acontecimiento de la primera brecha de seguridad. Así tampoco ha evidenciado que la aplicación vulnerada haya adecuado sus niveles de protección a prevenir brechas similares en la misma, siendo que la administrada ha declarado que como medidas correctivas frente a la segunda brecha acontecida (i) procedió a desvincular a todos los trabajadores (internos y externos) que participaron en el desarrollo de la aplicación vulnerada, (ii) dio de baja el servicio de manera temporal con la finalidad de cambiar el Apikey vulnerado y (iii) no realizó nuevas versiones de dicha aplicación (Folio 83).

Asimismo, se evidenció que la administrada envió comunicaciones de alertas y notificaciones, mediante correos electrónicos y/o mensajes de texto (SMS), a 969, 147 clientes afectados por los ataques ocurridos los días 7 de julio de 2018 y 12 de noviembre de 2018, siendo que el número total de correos electrónicos remitidos y/o mensajes de texto (SMS) no corresponde a la totalidad de los clientes afectados, conforme obra en la conclusión del Informe Técnico N° 49-2020-DFI-ORQR (Folio 329), motivo por el cual no puede considerarse dicho actuar como una acción de enmienda efectiva que pueda ser tomada como un atenuante de responsabilidad a favor de la administrada.

Cabe señalar además, que la administrada no ha realizado acciones destinadas a revertir la sustracción de los datos de sus clientes en julio y noviembre de 2018, puesto que no se han realizado cambios de números de tarjeta vinculados a dichos clientes.

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

En el presente caso, ha quedado probada la responsabilidad de la administrada en la comisión de las infracciones imputadas, no habiéndose advertido por este Despacho acción de enmienda efectiva y probada respecto a tales situaciones.

112. 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 a lo largo de la presente Resolución Directoral.

SE RESUELVE:

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 2, del artículo 132° de Reglamento de la LPDP: *"Incumplir la obligación de confidencialidad establecida en el artículo 17 de la Ley N° 29733".*

Artículo 2.- 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.

Artículo 3.- Informar a BANCO DE CRÉDITO DEL PERÚ S.A., que el incumplimiento de las medidas correctivas constituye la comisión de la infracción tipificada como muy grave en el literal d) del numeral 3 del artículo 132 del Reglamento de la LPDP[48].

Artículo 4.- Informar a BANCO DE CRÉDITO DEL PERÚ S.A., que contra la presente Resolución, de acuerdo con lo indicado en el artículo 218 de la LPAG, proceden los recursos de reconsideración o apelación dentro de los quince (15) días hábiles posteriores a su notificación[49].

Artículo 5.- Informar a BANCO DE CRÉDITO DEL 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 sesenta por ciento (60%) de la multa impuesta conforme a lo dispuesto en el artículo 128 del Reglamento de la LPDP[50].

---

[48] **Reglamento de la Ley de Protección de Datos Personales, aprobado por Decreto Supremo Nº 003-2013-JUS**
"TÍTULO VI INFRACCIONES Y SANCIONES
CAPÍTULO IV
INFRACCIONES
Artículo 132.- Infracciones
Las infracciones a la Ley Nº 29733, Ley de Protección de Datos Personales, o su Reglamento se califican como leves, graves y muy graves y se sancionan con multa de acuerdo al artículo 39 de la citada Ley.
(…)
3.Son infracciones muy graves:
(…)
d) No cesar en el indebido tratamiento de datos personales cuando existiese un previo requerimiento de la Autoridad como resultado de un procedimiento sancionador o de un procedimiento trilateral de tutela."

[49] **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."

[50] **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

Artículo 6.-Notificar a BANCO DE CRÉDITO DEL PERÚ S.A., la presente Resolución Directoral.

Regístrese y comuníquese.

PERÚ Ministerio de Justicia y Derechos Humanos
DIRECCIÓN DE PROTECCIÓN DE DATOS PERSONALES
M. GONZÁLEZ L.

Firmado digitalmente por GONZALEZ LUNA Maria Alejandra FAU 20131371617 soft
Fecha: 2020.08.03 12:57:01 -05'00'

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

MAGL/gcg

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."