REPÚBLICA DEL PERÚ

Resolución Directoral

Expediente N.°
04-2017-JUS/DPDP-PS

Resolución N° 802-2017-JUS/DGTAIPD-DPDP

Lima, 09 de noviembre de 2017.

VISTOS: El Informe Nº 015-2016-JUS/DGPDP-DSC del 3 de febrero de 2017, que se sustenta en el Acta de Fiscalización N° 01-2016 del 29 de septiembre de 2016 (Expediente de Fiscalización Nº 063-2016-DSC), emitido por la Dirección de Supervisión y Control de la Dirección General de Protección de Datos Personales (en adelante, DSC); y demás documentos que obran en el respectivo expediente y;

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

CONSIDERANDO:

I. Antecedentes

1. Mediante Orden de Visita de Fiscalización Nº 063-2016-JUS/DGPDP-DSC, la DSC dispuso la realización de una visita de fiscalización a PAPAYA PERÚ SOCIEDAD ANÓNIMA CERRADA - PAPAYA PERÚ S.A.C., identificada con R.U.C. N° 20547228775 (en adelante, PAPAYA PERÚ S.A.C.).

2. La indicada visita de fiscalización fue llevada a cabo por personal de la DSC el 29 de septiembre de 2016, dejando constancia de lo verificado en el Acta de Fiscalización Nº 01-2016.

3. El 3 de febrero de 2017, se puso en conocimiento de DS el resultado de la fiscalización realizada a PAPAYA PERÚ S.A.C. por medio del Informe Nº 015-2017-JUS/DGPDP-DSC, adjuntando el acta mencionada en el considerando precedente así como los demás anexos y documentos que conforman el respectivo expediente administrativo.

4. Mediante la Resolución Directoral Nº 036-2017-JUS/DGPDP-DS del 27 de febrero de 2017, la DS resolvió iniciar procedimiento administrativo sancionador a PAPAYA PERÚ S.A.C., por la presunta comisión de las infracciones previstas en los literales a. y e. del numeral 2 del artículo 38 de la Ley Nº 29733, Ley de Protección de Datos Personales (en adelante, LPDP), consideradas como infracciones graves y pasibles de ser sancionadas con multa.

En el primer caso, se atribuye a PAPAYA PERÚ S.A.C. realizar el tratamiento a los datos personales de sus clientes incumpliendo lo dispuesto en los numerales 1 y 2 del artículo 39 y en el artículo 43 del Reglamento de la LPDP, contraviniendo el principio de seguridad recogido en el artículo 9 de la LPDP; por ello, se le imputó la comisión de la infracción grave tipificada en el literal a. del numeral 2 del artículo 38 de la LPDP, esto es: *"Dar tratamiento a los datos personales contraviniendo los principios establecidos en la presente Ley o incumpliendo sus demás disposiciones o las de su Reglamento."*

En el segundo caso, se atribuye a PAPAYA PERÚ S.A.C. no inscribir los bancos de datos personales de su titularidad en el Registro Nacional de Protección de Datos Personales, imputándosele la comisión de la infracción grave tipificada en el literal e. del numeral 2 del artículo 38 de la referida Ley, esto es: *"No inscribir el banco de datos personales en el Registro Nacional de Protección de Datos Personales".*

5. La Resolución Directoral N° 036-2017-JUS/DGPDP-DS fue notificada a PAPAYA PERÚ S.A.C. el 11 de abril de 2017 mediante Oficio Nº 089-2017-JUS/DGPDP-DS.

6. Mediante la comunicación ingresada con Hoja de Trámite N° 26738 el 5 de mayo de 2017, PAPAYA PERÚ S.A.C. presentó sus descargos, en los siguientes términos:

Sobre la no inscripción del banco de datos personales en el Registro Nacional de Protección de Datos Personales.-

6.1 PAPAYA PERÚ S.A.C. sí cumplió con inscribir los bancos de datos personales de su titularidad en fecha anterior a la de la notificación de la imputación de cargos (Resolución Directoral N° 036-2017-JUS/DGPDP-DS), teniendo como sustento las siguientes resoluciones (Anexo II):

- Resolución Directoral N° 325-2017-JUS/DGPDP-DRN del 24 de febrero de 2017, correspondiente al banco de datos personales denominado "Videovigilancia", con código RNPDP-PJP N° 11892.
- Resolución Directoral N° 326-2017-JUS/DGPDP-DRN del 24 de febrero de 2017, correspondiente al banco de datos personales denominado "Recursos Humanos", con código RNPDP-PJP N° 11893.
- Resolución Directoral N° 327-2017-JUS/DGPDP-DRN del 24 de febrero de 2017, correspondiente al banco de datos personales denominado "Usuarios y/o Clientes", con código RNPDP-PJP N° 11894.
- Resolución Directoral N° 328-2017-JUS/DGPDP-DRN del 24 de febrero de 2017, correspondiente al banco de datos personales denominado "Proveedores", con código RNPDP-PJP N° 11895.

6.2 Asimismo, PAPAYA PERÚ S.A.C. cumplió con comunicar la realización de flujo transfronterizo de datos personales respecto de los bancos de datos personales denominados "Recursos Humanos", "Usuarios y/o Clientes" y "Proveedores" (Anexo III).

Sobre el tratamiento de datos personales contraviniendo lo establecido en la Ley 29733 y su Reglamento (medidas de seguridad del tratamiento de datos personales).-

6.3 Se han implementado las medidas de seguridad requeridas por la LPDP y su reglamento con anterioridad al 11 de abril de 2017, según consta en el Acta de Constatación Notarial del 8 de marzo de 2017, realizada en el domicilio de PAPAYA

PERÚ S.A.C., suscrita por el Notario de Lima Fermín Antonio Rosales Sepúlveda (Anexo IV), en la que se consignó lo siguiente:

- Dicha entidad realiza el tratamiento de datos personales mediante la utilización de un software de administración que maneja los permisos de accesos diferenciados para sus empleados, según la información que requieran para sus labores, no pudiendo acceder a datos personales si es que por motivo de su cargo no lo requieren.
- El acceso a los datos personales a través del software de administración se limita exclusivamente al personal autorizado, restringiendo el acceso de cada empleado solo a información concerniente a su área de trabajo. Ello se pudo comprobar con la computadora asignada al Gerente de Operaciones (computadora identificada con el IP: 192.168.11.181), así como con la computadora asignada a una empleada del área de Contenidos (computadora identificada con el IP: 192.168.11.94), quienes se encontraron impedidos de acceder a datos personales, debido a que para sus respectivas funciones no lo necesitaban.
- En dicha Acta de Constatación Notarial, también se anotó que dicho software de administración tiene programado realizar la verificación de privilegios de usuarios cada sesenta días.
- De otro lado, se hizo constar también que en el Software de Administración, se tiene un registro de interacciones con los datos lógicos, para fines de trazabilidad de la información de las cuentas de los usuarios. Así también, que dicho software cuenta con el servidor de almacenamiento de datos "Amazon Web Services", donde se realiza el mantenimiento de los registros señalados, almacenándose por noventa días y destruyéndose una vez que ya no sean útiles.
- Por su parte, se anotó en el acta mencionada que existe un procedimiento formal en virtud del cual la generación de copias así como la reproducción de documentos o información almacenada en el sistema "Software de Administración" puede ser realizada únicamente por personal autorizado; así también que dicho sistema no tiene habilitada función alguna que permita la descarga de la información que contiene, por lo que en caso de colocarse un USB, no podrá obtenerse una copia de la misma.

6.4 El 3 de abril de 2017, con la legalización de sus firmas por parte del Notario de Lima Ricardo Fernandini Barreda, entró en vigencia la segunda versión de su "Política de Medidas de Seguridad y Recursos Informáticos" (Anexo V), que ha sido puesta en conocimiento de sus trabajadores, ya que detalla una serie de políticas y procedimientos de seguridad técnica y organizativa que garantizan la adecuación de gestión y protección de los datos personales de sus bancos de datos, tales como:

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

- Establecer procedimientos para asignar entre los trabajadores derechos de acceso a los sistemas, a fin de impedir accesos no autorizados, según la condición de cada trabajador usuario del sistema que corresponda, la gestión de accesos privilegiados y revisión periódica de los mismos, gestión de contraseña, altas y bajas de las cuentas, modificación de perfiles, entre otros.
- Cada vez que un trabajador interactúe con los datos lógicos, se mantendrá un registro para fines de trazabilidad, que se almacenarán por 90 días, destruyéndose una vez que dejen de ser útiles.
- La generación de copias o reproducciones se realizará bajo el control del personal autorizado, debiendo destruirse las copias que no se vayan a utilizar, a fin de evitar el acceso a ellas o su recuperación posterior.

7. Por medio de la Resolución Directoral Nº 091-2017-JUS/DGPDP-DS del 9 de junio de 2017, notificada el 30 de junio de 2017, la Dirección de Sanciones, de acuerdo con lo establecido en el artículo 122 del Reglamento de la Ley de Protección de Datos Personales, aprobado con Decreto Supremo Nº 003-2013-JUS, cerró la etapa instructiva del presente procedimiento administrativo sancionador.

8. Con el Memorando N° 05-2017-JUS/DGTAIPD de fecha 21 de julio de 2017, la Dirección General de Transparencia, Acceso a la Información Pública y Protección de Datos Personales conforme a las funciones establecidas en el Reglamento de Organización y Funciones del Ministerio de Justicia y Derechos Humanos aprobado por Decreto Supremo N° 013-2017-JUS remite a la Dirección de Protección de Datos Personales los actuados para que resuelva en primera instancia el procedimiento administrativo sancionador iniciado.

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

9. Mediante el Oficio N° 101-2017-JUS/DPDP del 6 de agosto de 2017, la Directora de Protección de Datos Personales solicitó al Director de Fiscalización e Instrucción que, en el plazo de cinco días hábiles, informe si PAPAYA PERÚ S.A.C. ha implementado las medidas de seguridad necesarias para el tratamiento de datos personales, de acuerdo con lo que informó en sus descargos.

10. A través del Oficio N° 32-2017-JUS/DGTAIPD-DFI del 10 de agosto de 2017, el Director de Fiscalización e Instrucción remitió el Informe N° 008-2017-DFI-VARS, por el cual se dio respuesta a lo solicitado por esta Dirección, indicando lo siguiente:

- En el Acta de Constatación Notarial de su descargo, PAPAYA PERÚ S.A.C. documentó la verificación del acceso al "Software de Administración", lo cual no es idóneo, puesto que el sistema utilizado para realizar el tratamiento de datos personales de los clientes es el sistema web denominado "Cinepapaya", de acuerdo con el Informe N° 007-2017-DSC-ORQR.
- No ha demostrado fehacientemente tener documentada la ejecución ni la periodicidad de los procedimientos a través de los cuales que realizaría la revisión de privilegios en el "Software de Administración", por lo que no acreditó cumplir con lo dispuesto en el numeral 1 del artículo 39 del Reglamento de la LPDP.
- PAPAYA PERÚ S.A.C. informó acerca de la generación de registros de interacción lógica en el sistema "Software de Administración", cuando el tratamiento de los datos personales de los clientes se realiza por medio del sistema web denominado "Cinepapaya", por lo que no acreditó cumplir con lo dispuesto en el numeral 2 del artículo 39 del Reglamento de la LPDP.
- PAPAYA PERÚ S.A.C. sustentó tener procedimientos formalizados para centralizar la reproducción de documentos en el personal autorizado así como para el manejo de copias de documentos y su destrucción, en el documento "Política de Medidas de

Seguridad y Recursos Informáticos", cumpliendo con lo dispuesto en el artículo 43 del Reglamento de la LPDP.

11. A través del Oficio N° 151-2017-JUS-DGTAIPD-DPDP del 14 de agosto de 2017, se remitió el Informe N° 008-2017-DFI-VARS a PAPAYA PERÚ S.A.C., otorgándole el plazo de cinco días hábiles para formular alegatos complementarios.
12. Mediante la comunicación ingresada con Hoja de Trámite N° 50537 el 24 de agosto de 2017, PAPAYA PERÚ S.A.C. presentó sus alegatos complementarios, señalando lo siguiente:

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

- Se debe diferenciar entre el sistema web "Cinepapaya", que interactúa con los clientes recopilando sus datos personales, y el "Software de Administración", que es utilizado para gestionar los permisos de accesos para sus empleados, en función a la información a la que necesitan acceder para sus labores, sin dar tratamiento a los datos personales de clientes.
- El cumplimiento de lo requerido por los numerales 1 y 2 del artículo 39 del Reglamento de la LPDP se refiere a los mecanismos que la entidad tiene que implementar respecto de los empleados que tienen acceso a los bancos de datos personales, por lo que no es factible de ser realizado a través del sistema web "Cinepapaya", que cumple la función de interactuar con los clientes, sino a través del "Software de Administración".
- PAPAYA PERÚ S.A.C. ha cumplido con implementar controles de acceso a la información personal (gestiones de acceso y de privilegios), así como realiza la verificación periódica de privilegios, puesto que el "Software de Administración" permite a su Gerente de Operaciones asignar accesos y privilegios a sus empleados respecto de la información que maneja la empresa, incluida la información personal de clientes; así también, permite que se verifiquen periódicamente los privilegios asignados, en casos como el cese de algún empleado, a fin de cancelar el acceso que se le otorgó.
- Lo mencionado tiene sustento en una serie de pantallazos del "Software de Administración" correspondientes a la solicitud programada por dicho sistema para que el usuario cambie su contraseña, así como el pantallazo que corresponde a la lista de trabajadores que tiene acceso al sistema y los roles que estos manejan.
- Acerca de la observación referida a la obligación de establecer procedimientos de seguridad formales, el sistema "Software de Administración" permite mantener un registro sobre el personal que puede acceder a los datos personales y cuál es su rol, por lo que el sistema mantiene el procedimiento documentado digitalmente.
- Por su parte, el sistema "Software de Administración" permite monitorear la actividad de sus usuarios, permitiendo visualizar las opciones a las que accede cada uno,

desde qué terminal se conectan y el detalle de cada actividad, evidenciado la fecha de acceso al sistema y las acciones relevantes.
- El cumplimiento de las medidas de seguridad requeridas por el Reglamento de la LPDP, se ha dado con anterioridad a la notificación de cargos.

II. Competencia

13. La Directora de la Dirección de Protección de Datos Personales es competente para resolver en primera instancia, los procedimientos administrativos sancionadores iniciados por la Dirección de Fiscalización e Instrucción, de conformidad con lo dispuesto en el artículo 74 del Reglamento de Organización y Funciones del Ministerio de Justicia y Derechos Humanos aprobado por Decreto Supremo N° 013-2017-JUS.

III. Análisis

14. En ejercicio de sus facultades y conforme a sus competencias, corresponde a la Dirección de Protección de Datos Personales de la Dirección General de Transparencia, Acceso a la Información Pública y Protección de Datos Personales determinar si se han cometido infracciones a la LPDP y a su reglamento.

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

16. La Tercera Disposición Complementaria Modificatoria del mencionado reglamento incorpora el capítulo de infracciones al Título VI del Reglamento de la LPDP, agregando el artículo 132 que tipifica las infracciones[1].

Por lo tanto, en atención al principio de irretroactividad[2] que rige la potestad sancionadora administrativa, al estar en vigencia el artículo 132 del Reglamento de la

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

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

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

LPDP que tipifica las infracciones y dado que el presente procedimiento sancionador se apertura estando vigentes las infracciones señaladas en el artículo 38 de la LPDP, en el presente caso, se aplicará la disposición sancionadora más favorable al administrado. En tal sentido, para emitir pronunciamiento se debe analizar:

16.1 Si PAPAYA PERÚ S.A.C. cometió infracción a la LPDP y su Reglamento al no inscribir los bancos de datos personales de su titularidad, hecho que configuraría la infracción leve tipificada en el literal e. del numeral 1 del artículo 132 del Reglamento de la LPDP, esto es *"No inscribir o actualizar en el Registro Nacional los actos establecidos en el artículo 34 de la Ley"*.

16.2 Si PAPAYA PERÚ S.A.C. cometió infracción a la LPDP y a su Reglamento, infracción que en este caso, consistiría en: (i) no haber documentado los procedimientos de gestión de acceso y gestión de privilegios para el acceso a los bancos de datos personales de clientes, ni la verificación periódica de tales privilegios; (ii) en no generar ni mantener registros de la interacción lógica en el tratamiento automatizado de dichos datos personales, incumpliendo los incisos 1 y 2 del artículo 39° del Reglamento de la LPDP; y,(iii) en no establecer controles para la generación de copias o reproducción de documentos que contienen datos personales no sensibles de sus clientes, incumpliendo las exigencias del artículo 43 del Reglamento de la LPDP. Tales hechos implicarían la contravención al principio de seguridad recogido en el artículo 9° de la LPDP, configurando la infracción leve tipificada en el literal a. del numeral 1 del artículo 132 del Reglamento de la LPDP, esto es *"Realizar tratamiento de datos personales incumpliendo las medidas de seguridad establecidas en la normativa sobre la materia"*.

17. En relación al aspecto mencionado en el considerando 16.1, se debe indicar lo siguiente:

17.1 En el Informe Nº 015-2017-JUS/DGPDP-DSC, la DSC concluyó lo siguiente:

*"**Papaya Perú Sociedad Anónima Cerrada - Papaya Perú S.A.C.** cuenta con los bancos de datos personales de clientes, trabajadores y videovigilancia.*

***Papaya Perú Sociedad Anónima Cerrada - Papaya Perú S.A.C.** no ha inscrito los bancos de datos personales de su titularidad ante el Registro Nacional de Protección de Datos Personales. Dicha omisión constituiría infracción de conformidad con el literal e) del numeral 2 del artículo 38° de la LPDP."*

17.2 Como se desprende de lo citado, la DSC evidenció que PAPAYA PERÚ S.A.C. es titular del banco de datos personales de sus clientes, de sus trabajadores y del correspondiente a su sistema de videovigilancia.

17.3 En consecuencia, PAPAYA PERÚ S.A.C. tiene la obligación legal de inscribir dichos bancos de datos personales, previa solicitud, en el Registro Nacional de Protección de Datos Personales, de conformidad con lo establecido en el numeral 2 del artículo 77 del Reglamento de la LPDP, que establece que serán objeto de inscripción en dicho registro, los bancos de datos personales de administración privada; y en concordancia con el artículo 78 del mismo Reglamento, el cual señala que: *"Las personas naturales o jurídicas del sector privado o entidades públicas que creen, modifiquen o cancelen bancos de datos personales están obligadas a tramitar la inscripción de estos actos ante el Registro Nacional de Protección de Datos Personales".*

17.4 Sobre el particular, mediante la comunicación electrónica del 30 de enero de 2017, la Dirección de Registro Nacional de Protección de Datos Personales informó a la DSC que PAPAYA PERÚ S.A.C., a dicha fecha, no contaba con ningún banco de datos personales inscrito, así como tampoco tenía en trámite ninguna solicitud de inscripción formulada por dicha entidad; ello demostró que no había cumplido con inscribir los bancos de datos de su titularidad, no obstante estar obligado a ello.

17.5 Sin embargo, PAPAYA PERÚ S.A.C. indicó para la fecha de presentación de su descargo, ya había cumplido con obtener la inscripción de los bancos de datos personales de su titularidad, por medio de las siguientes resoluciones:

- Resolución Directoral N° 325-2017-JUS/DGPDP-DRN del 24 de febrero de 2017, correspondiente al banco de datos personales denominado "Videovigilancia".
- Resolución Directoral N° 326-2017-JUS/DGPDP-DRN del 24 de febrero de 2017, correspondiente al banco de datos personales denominado "Recursos Humanos".
- Resolución Directoral N° 327-2017-JUS/DGPDP-DRN del 24 de febrero de 2017, correspondiente al banco de datos personales denominado "Usuarios y/o Clientes".
- Resolución Directoral N° 328-2017-JUS/DGPDP-DRN del 24 de febrero de 2017, correspondiente al banco de datos personales denominado "Proveedores".

17.6 Asimismo, indicó que dicha inscripción se realizó en fecha previa a la notificación de la Resolución Directoral N° 036-2016-JUS/DGPDP-DS, efectuada el 11 de abril de 2017.

17.7 Al respecto, es preciso señalar que el literal f. del artículo 255 del Texto Único Ordenado de la Ley del Procedimiento Administrativo General, aprobado mediante Decreto Supremo N° 006-2017-JUS (en adelante, LPAG), establece como una causal eximente de la responsabilidad por infracciones la subsanación voluntaria del acto imputado como constitutivo de infracción administrativa, si es realizada de forma previa a la notificación de imputación de cargos.

17.8 En el presente caso, se aprecia que PAPAYA PERÚ S.A.C. obtuvo la inscripción de los bancos de datos personales de su titularidad el 27 de febrero de 2017, antes de que se le notifique el documento mediante el cual se le imputaron las presuntas infracciones administrativas.

En tal sentido, se entiende que si bien a la fecha de emisión del Informe Nº 015-2017-JUS/DGPDP-DSC, se había configurado la infracción tipificada en el literal e. del numeral 2 del artículo 38 de la referida Ley, esto es *"No inscribir el banco de datos personales en el Registro Nacional de Protección de Datos Personales"*, PAPAYA PERÚ S.A.C., al obtener la inscripción de los cuatro bancos de datos de su titularidad antes de que se le notifique la imputación de cargos, subsanó dicho acto infractor.

Por consiguiente, respecto de la presente imputación, se configuró la situación prevista en el literal f. del artículo 255 de la LPAG, por lo que debe declararse la inexistencia de responsabilidad por parte de PAPAYA PERÚ S.A.C.

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

18. En relación al aspecto mencionado en el considerando 16.2, señalamos lo siguiente:

18.1 En el Informe Nº 015-2017-JUS/DGPDP-DSC, la DSC señaló los siguientes hechos referidos a la recopilación de datos personales por parte de PAPAYA PERÚ S.A.C., en virtud del Acta de Fiscalización N° 01-2016:

> *"5. Se verificó que para realizar el tratamiento de los datos personales de los clientes,* ***Papaya Perú*** *cuenta con el sistema web denominado "Cinepapaya" (al cual se accede por la página web www.cinepapaya.com), mediante el cual se recopilan los siguientes datos del cliente a registrar: Correo electrónico, nombre, apellido, contraseña (creada por el cliente) y género (...)"*

En este punto, es necesario precisar que los datos recopilados no pertenecen a la categoría de datos personales sensibles.

18.2 Asimismo, el mencionado informe concluyó lo siguiente:

> *"5.* ***Papaya Perú Sociedad Anónima Cerrada - Papaya Perú S.A.C.*** *no cuenta con las medidas de seguridad necesarias para la protección de los datos personales de sus clientes, de acuerdo con las exigencias de la LPDP y su Reglamento. Dicha omisión constituiría infracción conforme con el literal a) del numeral 2 del artículo 38° de la LPDP. (...)"*

18.3 Durante la fiscalización realizada a PAPAYA PERÚ S.A.C., se verificó que esta entidad administra el banco de datos personales de sus clientes solo en soporte automatizado.

18.4 Al respecto los numerales 1 y 2 del artículo 39 del Reglamento de la LPDP señalan lo siguiente:

*"**Artículo 39°**.- Seguridad para el tratamiento de la información digital.*
Los sistemas informáticos que manejen bancos de datos personales deberán incluir en su funcionamiento:

1. *El control de acceso a la información de datos personales incluyendo la gestión de accesos desde el registro de un usuario, la gestión de los privilegios de dicho usuario, la identificación del usuario ante el sistema, entre los que se encuentran usuario, contraseña, uso de certificados digitales, tokens, entre otros, y realizar una verificación periódica de los privilegios asignados, los cuales deben estar definidos mediante un procedimiento documentado a fin de garantizar su idoneidad.*

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.*

   (...)"

18.5 En consecuencia, PAPAYA PERÚ S.A.C. está obligada a definir los procesos de gestión de accesos y privilegios, las identificaciones de usuarios ante el sistema, así como el proceso de verificación periódica de dichos privilegios, mediante procedimientos documentados a fin de garantizar su idoneidad. Así también, debe generar y mantener registros que evidencien las interacciones de los usuarios con los datos lógicos para fines de la trazabilidad.

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

18.6 Sin embargo, en el mencionado informe emitido por la DSC, se señala respecto de la fiscalización lo siguiente:

"24. (...) se informó al personal fiscalizador que en dicha entidad, no realizan una verificación periódica de privilegios asignados, ni poseen la documentación referente a la misma; así también, se manifestó que no tienen documentados los procedimientos de gestión de accesos y gestión de privilegios de los usuarios que tienen acceso a los datos personales.

(...)

26. Asimismo, se constató que en la entidad no se generan ni mantienen registros de interacción lógica en el sistema web "Cinepapaya", sobre lo cual se informó al personal fiscalizador que se debía a que solo un colaborador (el Jefe Técnico) realiza el tratamiento de datos personales de los clientes."

Con esta verificación, la DSC ha evidenciado que PAPAYA PERÚ S.A.C., respecto al banco de datos automatizado de sus clientes, no cuenta con la documentación de sus procedimientos de gestión de accesos y gestión de privilegios; así como tampoco genera ni mantiene registros de evidencias producto de la interacción lógica de la base de datos, incumpliendo la obligación establecida en los numerales 1 y 2 del artículo 39 del Reglamento de la LPDP.

18.7 Además, el artículo 43 del Reglamento de la LPDP señala que: *"La generación de copias o la reproducción de los documentos únicamente podrán ser realizadas bajo el control del personal autorizado. Deberá procederse a la destrucción de las copias o reproducciones desechadas de forma que se evite el acceso a la información contenida en las mismas o su recuperación posterior."*

18.8 Sin embargo, en el Informe N° 021-2016-JUS/DGPDP-DSC la DSC se señala haberse verificado lo siguiente que dicha entidad carece de restricciones de copias en las computadoras asignadas al Jefe de Operaciones y al Jefe Técnico, en las que se realiza el tratamiento de los datos personales de los clientes, teniendo ambas computadoras los puertos USB habilitados para grabar y visualizar archivos.

Con esta verificación, la DSC ha evidenciado que PAPAYA PERÚ S.A.C. no restringe la generación de copias o reproducción de documentos en las computadoras y que los usuarios que tienen acceso a los datos personales de los clientes de dicha entidad, tienen irrestricta la posibilidad de reproducir documentos que contengan tales datos personales, ya que los puertos USB de las computadoras examinadas se encuentran habilitados para grabar y visualizar archivos, incumpliendo con la obligación establecida en el artículo 43 del Reglamento de la LPDP.

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

Respecto a los hechos evidenciados, cabe señalar que de acuerdo a lo establecido en el artículo 101 del Reglamento de la LPDP[3], el personal de la DSC está dotado de fe pública para constatar la veracidad de los hechos en relación con los trámites a su cargo.

19. <u>Sobre las presuntas infracciones a los numerales 1 y 2 del artículo 39 del Reglamento de la LPDP</u>

19.1 Respecto de la imputación por la presunta infracción al numeral 1 del artículo 39 del Reglamento de la LPDP, PAPAYA PERÚ S.A.C. señala en su descargo y en sus alegatos complementarios, desarrollados en los considerandos 6.3, 6.4 y 12 de la presente Resolución, que la gestión de los accesos a la información que contiene datos personales (cuya recopilación y almacenamiento se realiza en el sistema web "Cinepapaya"), así como la gestión de los privilegios a asignar a cada empleado según su función, se realiza desde el sistema denominado "Software de Administración", el mismo que tiene programado realizar la verificación de privilegios de los usuarios cada sesenta días. Dicha entidad sustenta la efectiva asignación de accesos a dicho sistema de acuerdo con los roles de cada usuario, con los pantallazos adjuntos a sus alegatos complementarios.

Asimismo, indicaron que cuentan con la segunda versión del documento denominado "Política de Medidas de Seguridad y Recursos Informáticos", vigente desde el 3 de

[3] **Reglamento de la Ley de Protección de Datos Personales, aprobado por Decreto Supremo N° 003-2013-JUS:** "***Artículo 101.- Fe pública:*** *En el ejercicio de las funciones de fiscalización, el personal de la Dirección de Supervisión y Control estará dotado de fe pública para constatar la veracidad de los hechos en relación con los trámites a su cargo.*"

abril de 2017, en el que se establecen políticas de seguridad técnica aplicable a la gestión y protección de los recursos informáticos e información concerniente a los datos personales de sus clientes. Acerca de la gestión de accesos, dicho documento presenta la siguiente política:

"3.1. <u>CONTROL DE REGISTROS Y ACCESOS.-</u>

- *<u>Gestión de accesos:</u> Para impedir accesos no autorizados a los recursos informáticos de la empresa se deben establecer procedimientos para asignar derechos de acceso a los sistemas. Para ello se debe tomar en consideración la condición de los trabajadores que son usuarios de los sistemas en la empresa, desde su ingreso como trabajador y su cese, tomando especial consideración en los trabajadores que tienen accesos privilegiados. Los procedimientos deben considerar: (i) registro de trabajadores que serán los usuarios de los sistemas de la empresa; (ii) gestión de accesos privilegiados y revisión periódica de los mismo; (iii) gestión de contraseñas; (iv) altas y bajas de las cuentas; (v) cancelación de accesos debido al cese de la relación laboral; (vii) modificación de los perfiles de los trabajadores, toda modificación debe ser revisada por el jefe inmediato y validada por el área de recursos humanos; (viii) conformidad de los trabajadores activos, lo que ayudará a llevar un control de la vigencia de los trabajadores que están activos en la empresa de manera periódica."*

19.2 Sobre la implementación de la gestión de accesos y de privilegios en el sistema "Software de Administración", debe precisarse que los pantallazos presentados por la entidad sirve para demostrar que efectivamente se asigna accesos y privilegios para el uso de dicho sistema, según el cargo de cada usuario, así como se efectúa la asignación de contraseñas a quienes, según su cargo, les corresponda tener acceso.

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

19.3 Sin embargo, respecto del documento transcrito en el considerando 19.1, se debe señalar que se trata de directrices que se deben seguir para establecer los procedimientos de asignación de acceso a los sistemas que maneja PAPAYA PERÚ S.A.C.; vale decir, que se trata de un documento genérico, que no desarrolla los procedimientos de asignación de accesos y de privilegios específicos del sistema "Software de Administración", en lo referido a los datos personales de sus clientes.

19.4 Por otro lado, en sus alegatos complementarios, dicha entidad indica sobre la asignación de accesos y privilegios, que el "Software de Administración" permite mantener el registro del personal que puede acceder a los datos personales y cuál es su rol, manteniendo el procedimiento documentado digitalmente.

19.5 Al respecto, es preciso señalar que lo referido en este punto se trataría de un compendio del personal que accede al mencionado sistema, y no de una documentación que establezca la forma en la que se otorgan los accesos y privilegios al personal usuario de dicho sistema. Así también, debe mencionarse que PAPAYA PERÚ S.A.C. no sustentó la existencia de documentación digital que mencionó en sus alegatos complementarios, referida a las gestiones de acceso y de privilegios.

19.6 De lo expuesto en los considerandos anteriores, se desprende que PAPAYA PERÚ S.A.C. no ha sustentado tener debidamente documentados sus procedimientos de gestión de accesos y gestión de privilegios, lo cual significa el incumplimiento de lo dispuesto en el numeral 1 del artículo 39 del Reglamento de la LPDP.

19.7 Ahora bien, respecto de la imputación por la presunta infracción al numeral 2 del artículo 39 del Reglamento de la LPDP, PAPAYA PERÚ S.A.C. señala en su

descargo desarrollado en los considerandos 6.3 y 6.4 de la presente Resolución, que el sistema "Software de Administración" cuenta con un registro de interacciones con los datos lógicos y con el servidor de almacenamiento de datos "Amazon Web Services", donde se almacena el registro de interacciones señalado durante noventa días, luego de lo cual se destruyen en caso de que ya no sean útiles.

19.8 Asimismo, en el documento "Política de Medidas de Seguridad y Recursos Informáticos", vigente desde el 3 de abril de 2017, se tiene contemplado que se mantendrá un registro de cada interacción que haya entre un determinado trabajador y los datos lógicos, para ser almacenados durante dicho lapso, según los siguientes términos:

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

*"3.2. **REGISTROS DE INTERACCIONES.-***

- *Generación de registros: cada vez que los trabajadores interactúen con los datos lógicos, se mantiene un registro para fines de trazabilidad.*
- *Registros: Se deben mantener registros de los trabajadores con acceso al sistema y actividades más relevantes realizadas en el sistema.*
- *Procedimiento de disposición: Los registros serán almacenados por 90 días para finalidades de seguridad y una vez que estos ya no sean útiles se efectuará su destrucción."*

19.9 Por su parte, en sus alegatos complementarios, desarrollados en el considerando 12 de la presente resolución, sostuvieron que el sistema "Software de Administración" permite visualizar las opciones a las que accede cada uno de sus usuarios, la ubicación de su terminal, la fecha de acceso al sistema y sus acciones relevantes, hecho que se sustenta con los pantallazos en los que se puede visualizar el detalle de la actividad (terminal, cuenta del usuario, actividad, fecha, hora y opciones a las que accede cada usuario) realizada por determinados usuarios del mencionado sistema.

19.10 En efecto, con los medios probatorios adjuntos a esta última comunicación demuestran que la entidad genera registros de interacción con los datos lógicos desde el sistema "Software de Administración", según se puede apreciar en los pantallazos 7 y 8.

19.11 No obstante, en el primero de los pantallazos mencionados se observa que los registros que figuran corresponden a un lapso de tres minutos del 23 de agosto de

2017 (de las 17:53 horas a las 17:56 horas), así como el pantallazo 8, que muestra el detalle de una interacción con los datos lógicos de la misma fecha, lo que constituye acciones de enmienda, de acuerdo a lo señalado en el artículo 126 del Reglamento de la LPDP.

20. Sobre la presunta infracción al artículo 43 del Reglamento de la LPDP

20.1 Respecto de la imputación por la presunta infracción al artículo 43 del Reglamento de la LPDP, PAPAYA PERÚ S.A.C. señala en su descargo y en sus alegatos complementarios, desarrollados en los considerandos 6.3, 6.4 y 12 de la presente Resolución, que cuenta con un procedimiento en virtud del cual la generación de copias y la reproducción de documentos o información almacenada en el sistema "Software de Administración", puede ser realizada únicamente por personal autorizado, así como dicho sistema no tiene habilitada funciones que permitan la descarga de la información que contiene en cualquier dispositivo que se coloque en la computadora desde la cual se acceda.

Asimismo, señala que en la segunda versión del documento denominado "Política de Medidas de Seguridad y Recursos Informáticos", vigente desde el 3 de abril de 2017, se establecen políticas de seguridad técnica aplicables a la gestión y protección de los recursos informáticos e información concerniente a los datos personales de sus clientes. Sobre la seguridad de los equipos y la generación de copias o reproducciones se tiene previsto en dicho documento lo siguiente:

*"**3.4. COPIAS O REPRODUCCIONES.-***

- *Generación de copias: La generación de copias o la reproducción de los documentos únicamente podrán ser realizadas bajo el control del personal autorizado.*

- *Destrucción de copias: Se deben destruir o eliminar las copias o reproducciones que ya no se vayan a utilizar. Deberá procederse a la destrucción de las copias o reproducciones desechadas de forma que se evite el acceso a la información contenida en las mismas o su recuperación posterior.*

(...)

3.6. SEGURIDAD DE LOS EQUIPOS.-

(...)

- *Dispositivos de almacenamiento externo o medios informáticos removibles: El uso de este tipo de medios de almacenamiento externo (cintas de respaldo, memorias USB, disco duro externo, entre otros) debe de ser autorizado por el Jefe del área del trabajador que desea hacer su uso.*

- *Eliminación de la información de los medios informáticos removibles: Cuando se requiera eliminar información en un medio informático removible se deben utilizar mecanismos seguros de eliminación que garanticen la destrucción total de la información."*

20.2 Respecto de tales estipulaciones, debe señalarse que determinan medidas de control sobre la generación de copias al condicionarlas al control del personal autorizado, así como se dispone la destrucción de las copias de documentos que no se vaya a utilizar, con el fin de evitar el acceso a la información que estas contenían.

20.3 Así también, acerca de los dispositivos de almacenamiento externo removibles, se supedita su uso a la autorización del jefe del área, así como la eliminación de la información que el dispositivo contenga se puede realizar solo mediando la utilización de mecanismos seguros para tal fin.

20.4 En vista de ello, se puede concluir que a través del documento descrito, PAPAYA PERÚ S.A.C. cumple con el mandato previsto en el artículo 43 del Reglamento de la LPDP, que consiste en establecer medidas de control en la generación de copias de documentos y adicionalmente, medidas de destrucción de las copias desechables con la finalidad de evitar que se accede a la información que contienen.

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

20.5 En este punto, es necesario recordar la disposición del literal f. del artículo 255 de la LPAG, establece como una causal eximente de la responsabilidad por infracciones la subsanación voluntaria del acto imputado como constitutivo de infracción administrativa, si es realizada de forma previa a la notificación de imputación de cargos

20.6 En tal sentido, se debe tomar en cuenta que las disposiciones internas de PAPAYA PERÚ S.A.C. citadas en el considerando 20.1, de acuerdo con la fecha que consta en el documento descrito, entraron en vigencia antes de haberse notificado la imputación de cargos a dicha entidad.

Entonces, se entiende que si bien a la fecha de emisión del Informe N° 015-2017-JUS/DGPDP-DSC, se había configurado la infracción tipificada en el literal a. del numeral 2 del artículo 38 de la referida Ley, *"Dar tratamiento a los datos personales contraviniendo los principios establecidos en la presente Ley o incumpliendo sus demás disposiciones o las de su Reglamento"*, por medio de la inobservancia de la disposición del artículo 43 del Reglamento aludido, PAPAYA PERÚ S.A.C. demostró haber satisfecho el mandato de dicho artículo, al establecer controles a la generación de copias o reproducciones en uso de dispositivos móviles de almacenamiento (USB) en su documento "Política de Medidas de Seguridad y Recursos Informáticos", que entró en vigencia el 3 de abril de 2017.

Por consiguiente, respecto de la imputación analizada en el presente subtítulo, se configuró la situación prevista en el literal f. del artículo 255 de la LPAG, por lo que debe declararse la inexistencia de responsabilidad por parte de PAPAYA PERÚ S.A.C.

21. En concordancia con los considerandos 19.1 al 19.11 de la presente resolución, al no haber implementado las medidas de seguridad acordes con lo dispuesto en el Reglamento de la LPDP y con las características del tratamiento de datos personales que efectúa, el administrado contraviene el principio de seguridad establecido en el artículo 9 de la LPDP.

22. No obstante estar obligada a mantener documentados los procedimientos de gestión de accesos, de gestión de privilegios y de revisión periódica de privilegios, como medidas técnicas necesarias para garantizar la seguridad de los datos personales, conforme a lo establecido en el numeral 1 del artículos39 del Reglamento de la LPDP y en observancia del principio de seguridad previsto en el artículo 9 de la LPDP, PAPAYA PERÚ S.A.C. no ha cumplido con las mismas, a pesar de ser necesarias para la protección de los datos personales contenidos en el banco de datos personales de sus clientes, en soporte automatizado, manteniéndose tal situación a la fecha de expedición de la presente resolución.

23. Resulta necesario indicar que tanto la LPDP como su reglamento, reconocen no sólo la existencia de determinados principios rectores a los que deben ajustarse tanto los titulares como los encargados de bancos de datos personales, así como todo quien efectúe tratamiento de datos personales, sino que también contienen disposiciones que se constituyen como normas de cumplimiento obligatorio.

22. En tal sentido, a fin de sancionar el incumplimiento de dichos principios y disposiciones, es que la LPDP tipifica como infracción no sólo la contravención de los referidos principios, sino también el incumplimiento de las demás disposiciones contenidas en dicha ley o en su reglamento.

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

23. En mérito de los argumentos expuestos en los considerandos 19.1 al 19.15 de la presente resolución, esta Dirección entiende que en este caso se ha configurado la infracción tipificada en el literal a. del numeral 1 del artículo 132 del Reglamento de la LPDP, esto es: *"Realizar tratamiento de datos personales incumpliendo las medidas de seguridad establecidas en la normativa sobre la materia"*, toda vez que PAPAYA PERÚ S.A.C. efectúa el tratamiento de datos personales no sensibles de sus clientes, contraviniendo el principio de seguridad establecido en el artículo 9 de la LPDP, con la inobservancia de lo dispuesto en los numerales 1 y 2 del artículo 39 del Reglamento de la LPDP.

24. El artículo 38 de la LPDP establece los hechos que constituyen infracciones, clasificándolas como leves, graves o muy graves. Por su parte, el artículo 39 establece las sanciones aplicables a cada infracción según su clasificación, imponiendo multas que van desde 0,5 de una unidad impositiva tributaria hasta las 100 unidades impositivas

tributarias[4], sin perjuicio de las medidas correctivas que puedan determinarse de acuerdo con lo establecido en el artículo 118 del Reglamento de la LPDP[5].

25. La Dirección de Protección de Datos Personales determina el monto de las multas a ser impuestas tomando en cuenta para su graduación los criterios establecidos en el numeral 3 del artículo 246 de la LPAG. En ese sentido, debe prever que la comisión de las conductas sancionables no resulte más ventajosa para el infractor que cumplir las normas infringidas o asumir la sanción administrativa, por lo que la sanción deberá ser proporcional al incumplimiento calificado como infracción, observando para ello los criterios que dicha disposición señala para su graduación.

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

26. En el presente caso, la Dirección de Protección de Datos Personales considera como criterios relevantes para graduar las infracciones evidenciadas a los siguientes:

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

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

---

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

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

*"**Artículo 39. Sanciones administrativas:** En caso de violación de las normas de esta Ley o de su reglamento, la Autoridad Nacional de Protección de Datos Personales puede aplicar las siguientes multas:*

1. Las infracciones leves son sancionadas con una multa mínima desde cero coma cinco de una unidad impositiva tributaria (UIT) hasta cinco unidades impositivas tributarias (UIT).
2. Las infracciones graves son sancionadas con multa desde más de cinco unidades impositivas tributarias (UIT) hasta cincuenta unidades impositivas tributarias (UIT).
3. Las infracciones muy graves son sancionadas con multa desde más de cincuenta unidades impositivas tributarias (UIT) hasta cien unidades impositivas tributarias (UIT).
(...)".

[5] **Reglamento de la Ley de Protección de Datos Personales, aprobado por Decreto Supremo N° 003-2013-JUS:**

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

b) La probabilidad de detección de la infracción:

Respecto a la comisión de la infracción imputada, vinculada al incumplimiento del principio de seguridad previsto en el artículo 9 de la LPDP, se tiene que la probabilidad de detección de la conducta infractora (realizar el tratamiento de datos personales de clientes sin contar con las medidas necesarias para garantizar su seguridad), es baja, puesto que ha sido necesario realizar una fiscalización para la detección de la misma, así como analizar la documentación y las medidas adoptadas por la entidad.

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

Las infracciones detectadas afectan el derecho fundamental a la protección de datos personales, el cual se encuentra reconocido en el artículo 2, numeral 6 de la Constitución Política del Perú, siendo desarrollado por la Ley Nº 29733, Ley de Protección de Datos Personales y su reglamento.

Se ha demostrado que la entidad carece de las medidas de seguridad que la LPDP y su reglamento exigen al titular del banco de datos personales, configurándose una infracción que afecta el derecho de los ciudadanos a que se dé un tratamiento adecuado de sus datos personales, al no haberse adoptado medidas técnicas, organizativas y legales necesarias para garantizar su seguridad.

d) El perjuicio económico causado:

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

e) La reincidencia en la comisión de la infracción:

Del mismo modo, se tiene en cuenta que PAPAYA PERÚ S.A.C. no es reincidente, ya que no ha sido sancionado por la infracción imputada en el presente procedimiento sancionador.

f) Las circunstancias de la comisión de la infracción:

Respecto de dar tratamiento a los datos personales de sus clientes contraviniendo el principio de seguridad recogido en el artículo 9 de la LPDP, al incumplir lo dispuesto en los numerales 1 y 2 del artículo 39 del Reglamento de la LPDP, se advierte que PAPAYA PERÚ S.A.C. ha realizado acciones de enmienda respecto al incumplimiento del numeral 2 del artículo 39 del Reglamento de la LPDP.

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

No se ha evidenciado que haya elementos que acrediten la no intencionalidad de la infracción cometida.

27. Habiendo la Dirección de Protección de Datos Personales realizado el análisis de las conductas infractoras aplicando el principio de irretroactividad de la potestad sancionadora administrativa señalado en el numeral 5 del artículo 246 de la LPAG, se tiene que las infracciones cometidas por PAPAYA PERÚ S.A.C. están tipificadas como leves, y conforme con lo establecido por el numeral 1. del artículo 39 de la LPDP que regula las sanciones administrativas aplicables, las infracciones calificadas de leves son sancionadas con multa desde más de cero coma cinco (0,5) hasta cinco (5) unidades

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

impositivas tributarias (UIT); por lo que a efectos de establecerse la sanción de multa se tiene en cuenta la suma de todos los criterios que permiten graduarlas conforme a los argumentos desarrollados en el considerando 26 de la presente resolución directoral, a efectos de determinar la sanción de multa a imponerse.

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

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

SE RESUELVE:

Artículo 1.- Sancionar a PAPAYA PERÚ SOCIEDAD ANÓNIMA CERRADA - PAPAYA PERÚ S.A.C., con la multa ascendente a dos unidades impositivas tributarias (2 UIT) por *"Dar tratamiento a los datos personales contraviniendo los principios establecidos en la Ley o incumpliendo sus demás disposiciones o las de su Reglamento"*, toda vez que PAPAYA PERÚ SOCIEDAD ANÓNIMA CERRADA da tratamiento a los datos personales de sus clientes contraviniendo el principio de seguridad recogido en el artículo 9 de la LPDP, al incumplir lo dispuesto en los numerales 1 y 2 del artículo 39 del Reglamento de la LPDP, configurándose la infracción leve prevista en el literal f. del numeral 1 del artículo 132 del Reglamento de la LPDP [6], modificado por el Decreto Supremo N° 019-2017-JUS.

Artículo 2.- Informar a PAPAYA PERÚ SOCIEDAD ANÓNIMA CERRADA - PAPAYA PERÚ S.A.C. que contra la presente resolución, de acuerdo a lo indicado en el artículo 216 del Texto Único Ordenado de la Ley N° 27444, Ley del Procedimiento Administrativo General, aprobado por Decreto Supremo Nº 006-2017-JUS, proceden los

[6] **Reglamento de la Ley de Protección de Datos Personales, modificado por el Decreto Supremo N° 019-2017-JUS:**
"Artículo 132.- Infracciones
Las infracciones a la Ley N° 29733, Ley de Protección de Datos Personales, o su Reglamento se califican como leves, graves y muy graves y se sancionan con multa de acuerdo al artículo 39 de la citada Ley.
1. Son infracciones leves
(...)
f) Dar tratamiento a los datos personales contraviniendo las disposiciones de la Ley y su Reglamento."

recursos de reconsideración o apelación dentro de los quince (15) días de notificada la presente[7].

Artículo 3.- El pago de la multa será requerido una vez que la resolución que impone la sanción quede firme. En el requerimiento de pago se le otorgará diez (10) días hábiles para realizarlo y se entiende que cumplió con pagar la multa impuesta, si antes de que venza el plazo establecido en el requerimiento de pago, cancela el 60% de la multa impuesta conforme a lo dispuesto en el artículo 128 del Reglamento de la LPDP[8].

Artículo 4.- Notificar a PAPAYA PERÚ SOCIEDAD ANÓNIMA CERRADA - PAPAYA PERÚ S.A.C. la presente resolución.

Regístrese y comuníquese.

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

[7] **Artículo 216. Recursos administrativos**
216.1 Los recursos administrativos son:
a) Recurso de reconsideración
b) Recurso de apelación
Solo en caso que por ley o decreto legislativo se establezca expresamente, cabe la interposición del recurso administrativo de revisión.
216.2 El término para la interposición de los recursos es de quince (15) días perentorios, y deberán resolverse en el plazo de treinta (30) días.

[8] **Artículo 128.- Incentivos para el pago de la sanción de multa.**
Se considerará que el sancionado ha cumplido con pagar la sanción de multa si, antes de vencer el plazo otorgado para pagar la multa, deposita en la cuenta bancaria determinada por la Dirección General de Protección de Datos Personales el sesenta por ciento (60%) de su monto. Para que surta efecto dicho beneficio deberá comunicar tal hecho a la Dirección General de Protección de Datos Personales, adjuntando el comprobante del depósito bancario correspondiente. Luego de dicho plazo, el pago sólo será admitido por el íntegro de la multa impuesta.