Resolución Directoral

Resolución Directoral N° 1138-2019-JUS/DGTAIPD-DPDP

Expediente N°
077-2018-JUS/DPDP-PS

Resolución N° 1138-2019-JUS/DGTAIPD-DPDP

Lima, 30 de abril de 2019

VISTOS:

El Informe N° 102-2018-JUS/DGTAIPD-DFI[1] del 19 de octubre de 2018, 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. Por medio de la Orden de Visita de Fiscalización N° 047-2017-JUS/DGTAIPD-DFI[2], la DFI dispuso la realización de una visita de fiscalización a Clínica Monte Horeb S.A., identificada con R.U.C. N° 20128890891, dedicada a actividades de hospitales (en adelante, la administrada).

Dirección de Protección de Datos Personales
M. GONZALEZ L.

2. Dicha visita de fiscalización se realizó en Jr. Inmaculada N° 529, distrito de Callería (ciudad de Pucallpa), provincia de Coronel Portillo, departamento de Ucayali, el 19 de octubre de 2017; registrándose lo hallado en las Actas de Fiscalización N° 01-2017[3] y N° 02-2017[4].

3. Durante tal visita, se informó al personal fiscalizador que la administrada contaba con los bancos de datos personales "Pacientes", "Trabajadores", "Proveedores" y "Videovigilancia", que aún no habían sido inscritos en el Registro Nacional de Protección de Datos Personales (en adelante, RNPDP).

[1] Folios 114 al 124
[2] Folio 13
[3] Folios 14 al 23
[4] Folios 26 al 34

4. Asimismo, se verificó que las historias clínicas (que contienen la información de los pacientes) son almacenadas en estantes de madera sin llave, dispuestas en un ambiente con puerta sin cerradura. Dichas historias contienen información concerniente a los exámenes físicos y auxiliares, así como de los diagnósticos (Dx) y recetas médicas (Rp)[5].

5. Por su parte, se constató que efectúan el tratamiento automatizado de los datos personales de sus pacientes por medio del "Sistema de Gestión de Clínicas", sobre el cual se informó que no cuentan con la documentación de los procedimientos de gestión de accesos, de privilegios y de verificación periódica de los privilegios asignados; verificándose también que no generan ni mantienen registros de interacción lógica con el banco de datos personales "Pacientes".

6. Se verificó que por medio del "Sistema de Gestión de Clínicas", se tiene acceso a los datos del paciente, así como se da la posibilidad de crear historias clínicas[6].

7. Así también, se constató que el centro de datos donde se almacena la información de los pacientes está ubicado en un ambiente compartido con el área de caja, careciendo de detector de humo, extintores, alarma contra incendio y de gabinete.

8. De otro lado, se informó que los datos personales recopilados a través de las opciones "Contáctanos" y "Quejas y Reclamos" de la página web www.clinicamontehoreb.com.pe son direccionadas a la cuenta de correo electrónico clinicamontehoreb@hotmail.com, manejada por un Asistente Administrativo, siendo dichos datos almacenados por tiempo indefinido.

9. Mediante el Informe Técnico N° 62-2017-DFI-ORQR del 27 de diciembre de 2017[7], el Analista de Fiscalización en Seguridad de la Información de la DFI, indicó sobre la administrada lo siguiente:

Dirección de Protección de Datos Personales
M. GONZALEZ

- Realiza el flujo transfronterizo de los datos personales recopilados a través de su página web hacia los Estados Unidos de América.
- No documenta los procedimientos de gestión de accesos, de privilegios ni de la verificación periódica de estos, respecto de los usuarios del "Sistema de Gestión de Clínicas".
- No genera ni mantiene registros de interacción lógica con el banco de datos personales "Pacientes".
- No mantiene medidas de seguridad apropiadas para el centro de datos donde se ubica el servidor que almacena los datos personales de sus pacientes.
- Almacena la documentación no automatizada en ambientes que no cuentan con cerradura ni con llave asignada a un trabajador.

10. Por medio del correo electrónico del 26 de marzo de 2018, personal de 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) informó a la abogada fiscalizadora de la DFI que la administrada contaba en el RNPDP, con los siguientes bancos de datos personales:

[5] Folio 25
[6] Folio 36
[7] Folios 37 al 44

REPÚBLICA DEL PERÚ

Resolución Directoral

Resolución Directoral N° 1138-2019-JUS/DGTAIPD-DPDP

Banco de Datos Personales	N° de Resolución Directoral	Código de Inscripción
Proveedores	861-2017-JUS/DGTAIPD-DPDP	RNPDP-PJP N° 13165
Pacientes	862-2017-JUS/DGTAIPD-DPDP	RNPDP-PJP N° 13166
Trabajadores	928-2017-JUS/DGTAIPD-DPDP	RNPDP-PJP N° 13218
Videovigilancia	929-2017-JUS/DGTAIPD-DPDP	RNPDP-PJP N° 13219

11. En dicho correo electrónico se informó también que la administrada no contaba con la inscripción de comunicación de flujo transfronterizo de los datos personales recopilados por medio de su página web, ni con solicitudes para tal fin[8].

Dirección de Protección de Datos Personales
M. GONZALEZ

12. El 3 de abril de 2018 se puso en conocimiento de la directora de la DFI el resultado de la fiscalización realizada a dicha entidad por medio del Informe N° 54-2018-JUS/DGTAIPD-DFI-RCCDL[9], adjuntando las actas de fiscalización, así como los demás anexos y documentos que conforman el respectivo expediente administrativo.

13. Mediante la Resolución Directoral N° 129-2018-JUS/DGTAIPD-DFI del 20 de agosto de 2018[10], la DFI resolvió iniciar procedimiento administrativo sancionador a la administrada, por la presunta comisión de las siguientes infracciones:

- Recopilar datos personales a través de los formularios "Contáctanos" y "Quejas y Reclamos" de la página web www.clinicamontehoreb.com.pe sin facilitar a los usuarios algún enlace a la política de privacidad que informe sobre lo requerido en el artículo 18 de la Ley N° 29733, Ley de Protección de Datos Personales (en adelante, LPDP); con lo cual se configuraría la infracción grave tipificada en el literal a) del numeral 2 del artículo 132 del Reglamento de la LPDP, aprobado por Decreto Supremo N° 003-2013-JUS (en adelante, Reglamento de la LPDP), *"no atender, impedir u obstaculizar el ejercicio de los derechos del titular de datos personales de acuerdo a lo establecido en el título III de la Ley N° 29733 y su Reglamento"*.
- No haber inscrito en el RNPDP el banco de datos personales de los usuarios de la página web www.clinicamontehoreb.com.pe, incumpliendo con la obligación señalada en el artículo 78 del Reglamento de la LPDP; con lo cual se configuraría la infracción leve tipificada en el literal e) del numeral 1 del artículo 132 de dicho

[8] Folios 50 al 51
[9] Folios 54 al 58
[10] Folios 62 al 69

reglamento, *"no inscribir o actualizar en el Registro Nacional los actos establecidos en el artículo 34 de la Ley"*.

- No haber comunicado al RNPDP la realización de flujo transfronterizo de los datos personales recopilados a través de los formularios mencionados, teniendo el servidor de datos de su página web en los Estados Unidos de América, incumpliendo lo dispuesto en el artículo 26 del Reglamento de la LPDP; con lo cual se configuraría la infracción leve tipificada en el literal e) del numeral 1 del artículo 132 de dicho reglamento, *"no inscribir o actualizar en el Registro Nacional los actos establecidos en el artículo 34 de la Ley"*.
- No haber implementado las medidas de seguridad para el tratamiento de datos personales, dispuestas en los numerales 1 y 2 del artículo 39, así como en los artículos 40 y 42 del Reglamento de la LPDP, dicha situación configuraría la infracción grave tipificada en el literal c) del numeral 2 del artículo 132 del señalado reglamento, esto es, *"realizar tratamiento de datos personales sensibles incumpliendo las medidas de seguridad establecidas en la normativa sobre la materia"*.

14. Dicha Resolución Directoral fue notificada a la administrada el 24 de agosto de 2018, a través del Oficio N° 524-2018-JUS/DGTAIPD-DFI[11].

15. A través de la comunicación ingresada con la Hoja de Trámite N° 59944-2018 del 18 de septiembre de 2018[12], la administrada presentó sus descargos, alegando lo siguiente:

- Realizaron los cambios necesarios en su página web, generando el link de las políticas de privacidad en cada formulario, de manera accesible e identificable para sus usuarios.
- Han procedido con la inscripción de los bancos de datos personales, que son los de "Prospectos de Clientes" y "Quejas y Reclamos", con expedientes N° 059666 y N° 059701 respectivamente.
- En virtud del artículo 26 del Reglamento de la LPDP, consideran que no transfieren a ninguna empresa del extranjero, solo cuentan con un alojamiento web (servidor de la plataforma Wix), que funge como servidor de su plataforma web, sin que haya realizado comunicación de flujo transfronterizo de datos personales.
- Asimismo, la autoridad debe tomar en cuenta que, siguiendo lo establecido en el artículo 15 de la LPDP, cuentan con un servidor con sede en el estado de California, Estados Unidos de América, que cumple con estrictas políticas de seguridad y protección de datos personales, ya que la empresa "Wix" cuenta con políticas de privacidad y seguridad detalladas, en cumplimiento de la normativa de privacidad en internet promulgada en dicho estado.
- En la inscripción de los bancos de datos personales antes mencionados, hacen referencia al flujo transfronterizo realizado hacia los Estados Unidos.
- Han implementado un sistema de gestión de accesos con contraseñas personalizada, el mismo que cuenta con herramientas necesarias para conocer los pormenores de las interacciones de los usuarios con los datos.
- Asimismo, se han implementado medidas de seguridad para sus bancos de datos como son los detectores de humo, extintores, así como lo establecido por Defensa Civil, modificando también el acceso a su cuarto de archivo de información no automatizada, que tiene una cerradura, siendo la persona designada para el acceso a él su Administradora General.

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

[11] Folio 71
[12] Folios 72 al 97

16. En el Informe Técnico N° 231-2018-DFI-ORQR del 10 de octubre de 2018[13], el Analista de Fiscalización en Seguridad de la Información concluyó respecto de las medidas de seguridad mostradas por la administrada en sus descargos, lo siguiente:

- No documenta los procedimientos de gestión de accesos, de privilegios y de verificación periódica de estos últimos, respecto del "Sistema de Gestión de Clínicas".
- No genera ni mantiene registros de interacción lógica con los datos personales de los pacientes.
- Ha evidenciado contar con las medidas de seguridad perimetral para el servidor que almacena los datos personales de sus pacientes.
- Ha evidenciado almacenar la documentación no automatizada en ambientes dotados con cerraduras, cuya llave se encuentra debidamente asignada a una trabajadora.

Dirección de Protección de Datos Personales
M. GONZALEZ

17. El 11 de octubre de 2018, personal de la DFI tomó conocimiento de las resoluciones directorales N° 2433-2018-JUS/DGTAIPD-DPDP y N° 2492-2018-JUS/DGTAIPD-DPDP[14], mediante las cuales se inscribió en el RNPDP los bancos de datos personales "Prospectos de Clientes" y "Quejas y Reclamos".

18. Asimismo, se tomó una impresión de la política de privacidad de la página web de la administrada, en la cual se tiene el siguiente texto:

> **"POLÍTICA DE PRIVACIDAD**
> El presente Política de Privacidad establece los términos en que Clínica Monte Horeb usa y protege la información que es proporcionada por sus usuarios al momento de utilizar su sitio web. Esta compañía está comprometida con la seguridad de los datos de sus usuarios. Cuando le pedimos llenar los campos de información personal con la cual usted pueda ser identificado, lo hacemos asegurando que sólo se empleará de acuerdo con los términos de este documento. Sin embargo, esta Política de Privacidad puede cambiar con el tiempo o ser actualizada por lo que le recomendamos y enfatizamos revisar continuamente esta página para asegurarse que está de acuerdo con dichos cambios.

[13] Folios 99 al 105
[14] Folios 106 al 109

Información que es recogida

Nuestro sitio web podrá recoger información personal, por ejemplo: Nombre, información de contacto como su dirección de correo electrónica e información demográfica. Así mismo cuando sea necesario podrá ser requerida información específica para procesar algún pedido o realizar una entrega o facturación.

Uso de la información recogida

Nuestro sitio web emplea la información con el fin de proporcionar el mejor servicio posible, particularmente para mantener un registro de usuarios, de pedidos en caso que aplique, y mejorar nuestros productos y servicios. Es posible que sean enviados correos electrónicos periódicamente a través de nuestro sitio con ofertas especiales, nuevos productos y otra información publicitaria que consideremos relevante para usted o que pueda brindarle algún beneficio, estos correos electrónicos serán enviados a la dirección que usted proporcione y podrán ser cancelados en cualquier momento.

Clínica Monte Horeb está altamente comprometido para cumplir con el compromiso de mantener su información segura. Usamos los sistemas más avanzados y los actualizamos constantemente para asegurarnos que no exista ningún acceso no autorizado.

Cookies

Una cookie se refiere a un fichero que es enviado con la finalidad de solicitar permiso para almacenarse en su ordenador, al aceptar dicho fichero se crea y la cookie sirve entonces para tener información respecto al tráfico web, y también facilita las futuras visitas a una web recurrente. Otra función que tienen las cookies es que con ellas las webs pueden reconocerte individualmente y por tanto brindarte el mejor servicio personalizado de su web.

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

Nuestro sitio web emplea las cookies para poder identificar las páginas que son visitadas y su frecuencia. Esta información es empleada únicamente para análisis estadístico y después la información se elimina de forma permanente. Usted puede eliminar las cookies en cualquier momento desde su ordenador. Sin embargo, las cookies ayudan a proporcionar un mejor servicio de los sitios web, estás no dan acceso a información de su ordenador ni de usted, a menos de que usted así lo quiera y la proporcione directamente, visitas a una web. Usted puede aceptar o negar el uso de cookies, sin embargo, la mayoría de navegadores aceptan cookies automáticamente pues sirve para tener un mejor servicio web. También usted puede cambiar la configuración de su ordenador para declinar las cookies. Si se declinan es posible que no pueda utilizar algunos de nuestros servicios.

Enlaces a Terceros

Este sitio web pudiera contener en laces a otros sitios que pudieran ser de su interés. Una vez que usted de clic en estos enlaces y abandone nuestra página, ya no tenemos control sobre al sitio al que es redirigido y por lo tanto no somos responsables de los términos o privacidad ni de la protección de sus datos en esos otros sitios terceros. Dichos sitios están sujetos a sus propias políticas de privacidad por lo cual es recomendable que los consulte para confirmar que usted está de acuerdo con estas.

Control de su información personal

En cualquier momento usted puede restringir la recopilación o el uso de la información personal que es proporcionada a nuestro sitio web. Cada vez que se le solicite rellenar un formulario, como el de alta de usuario, puede marcar o desmarcar la opción de recibir información por correo electrónico. En caso de que haya marcado la opción de recibir nuestro boletín o publicidad usted puede cancelarla en cualquier momento.
Esta compañía no venderá, cederá ni distribuirá la información personal que es recopilada sin su consentimiento, salvo que sea requerido por un juez con un orden judicial.

Clínica Monte Horeb Se reserva el derecho de cambiar los términos de la presente Política de Privacidad en cualquier momento."

M. GONZALES

19. Por medio de la Resolución Directoral N° 186-2018-JUS/DGTAIPD-DFI del 19 de octubre de 2018[15], la DFI, siguiendo lo establecido en el artículo 122 del Reglamento de la LPDP, cerró la etapa instructiva del presente procedimiento administrativo sancionador.

20. A través del Informe N° 102-2018-JUS/DGTAIPD-DFI del 19 de octubre de 2018, la DFI remitió a la DPDP el expediente del presente caso, recomendando lo siguiente:

- Imponer una multa ascendente a ocho unidades impositivas tributarias (8 UIT) a la administrada por la infracción grave prevista en el literal a) del numeral 2 del artículo 132 del Reglamento de la LPDP, esto es, *"no atender, impedir u obstaculizar el ejercicio de los derechos del titular de datos personales de acuerdo a lo establecido en el título III de la Ley N° 29733 y su Reglamento"*.
- Imponer una multa ascendente a cero coma cinco unidades impositivas tributarias (0,5 UIT) a la administrada por 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"*, referida a la no inscripción en el RNPDP de bancos de datos personales recopilados por medio de su página web.

[15] Folios 111 al 113

- Imponer una multa ascendente a una coma cinco unidades impositivas tributarias (1,5 UIT) a la administrada por 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"*, referida a la no inscripción en el RNPDP del flujo transfronterizo de los datos personales recopilados por medio de su página web.
- Imponer una multa ascendente a cinco coma cinco unidades impositivas tributarias (5,5 UIT) a la administrada por la infracción grave tipificada en el literal c) del numeral 2 del artículo 132 del Reglamento de la LPDP, esto es, *"realizar tratamiento de datos personales sensibles incumpliendo las medidas de seguridad establecidas en la normativa sobre la materia"*, por la inaplicación de las medidas de seguridad contempladas en los artículos 39, 40 y 42 de dicho reglamento.

21. A través de la comunicación ingresada con la Hoja de Trámite N° 69022-2018 del 31 de octubre de 2018[16], la administrada alegó lo siguiente:

- Antes del inicio del procedimiento sancionador, han estado implementando sus procedimientos y sistemas de seguridad.
- Al momento de la fiscalización, la implementación de las medidas de seguridad de la información venía desarrollándose.
- Generaron un enlace en su página web, para comunicar sus políticas de privacidad a los usuarios de la misma, en cada uno de sus formularios.
- No han infringido de manera dolosa el artículo 18 de la LPDP.
- Toda la información recabada por medio de su página web era almacenada en el banco de datos "Pacientes", por lo que no es razonable que se les sancione por la omisión de inscripción de un banco de datos personales, no siendo tal error pasible de sanción.
- Cuentan con los bancos de datos personales vinculados con la información recopilada por medio de su página web, debidamente inscritos en el RNPDP.
- El 22 de octubre de 2018, ingresaron por mesa de partes las solicitudes de comunicación de flujo transfronterizo de los datos personales almacenados en los bancos de datos "Prospectos de Clientes" y "Quejas y Reclamos".
- Se debe tener en consideración que no realiza de forma premeditada ninguna transferencia al extranjero, aun cuando el sistema que usan tiene su central en el extranjero, puesto que utilizan una plataforma con la tecnología suficientemente segura para proteger los datos personales.
- Al haber transmitido datos personales a California, pionero en la revolución tecnológica, cumplen con la disposición del artículo 15 de la LPDP, al tratarse de un destinatario que tiene niveles de protección adecuados.
- Se encuentran implementando todos los procedimientos de gestión de accesos y de privilegios, al haber implementado un nuevo sistema, que permite saber los pormenores de acceso de cada usuario.
- Las multas propuestas por la DFI son excesivas, pues han cumplido con las disposiciones de la LPDP.
- Todo lo anterior evidencia su predisposición para implementar las mejoras necesarias.

22. Habiendo solicitado la administrada el uso de la palabra, se realizó el informe oral respectivo el 4 de diciembre de 2018, fecha en la que el personal de la DPDP accedió a la política de privacidad de la página web de la administrada.

Dirección de Protección de Datos Personales
M. GONZALEZ I.

[16] Folios 127 al 176

23. Mediante el Oficio N° 748-2019-JUS/DGTAIPD-DPDP[17], se solicitó a la administrada remitir copia de lo siguiente:

- Copia de su Declaración Jurada anual del ejercicio fiscal 2018 o documento equivalente.
- Documentación que acredite el cumplimiento de las medidas de seguridad establecidas en los numerales 1 y 2 del artículo 39 del Reglamento de la LPDP.

24. Por medio del escrito ingresado con Hoja de Trámite N° 26409-2019 del 12 de abril de 2019[18], la administrada remitió los documentos solicitados, señalando además que su conducta debe ser eximida de responsabilidad, de acuerdo con el literal f) del numeral 1 del artículo 257 del Texto Único Ordenado de la Ley del Procedimiento Administrativo General (en adelante, LPAG), puesto que subsanaron sus conductas antes de que la autoridad haya decidido ejercer su potestad sancionadora.

Dirección de Protección de Datos Personales
M. GONZALES

25. Mediante el Oficio N° 935-2019-JUS/DGTAIPD-DPDP, se solicitó a la DFI evaluar los documentos que la administrada remitió, a fin de verificar si sustentan la aplicación de medidas de seguridad.

26. Por medio del Oficio N° 348-2019-JUS/DGTAIPD-DFI, se remitió a esta dirección el Informe Técnico N° 063-2019-DFI-ETG, en el que se indica respecto de la administrada, lo siguiente:

- Documenta los procedimientos de gestión de accesos y gestión de privilegios, pero no documenta los procedimientos de verificación de tales privilegios.
- No genera ni mantiene registros de interacción lógica respecto del banco de datos automatizado de pacientes.

27. El 26 de abril de 2018, personal de esta dirección accedió a las resoluciones directorales N° 3071-2018-JUS/DGTAIPD-DPDP y N° 3072-2018-JUS/DGTAIPD-DPDP, así como a la página web de la administrada, a fin de verificar sus políticas de privacidad.

[17] Folio 194
[18] Folios 195 al 226

II. Competencia

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

29. 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

30. Acerca de la responsabilidad de la administrada, se deberá tener en cuenta que el literal f) del numeral 1 del artículo 257 de 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[19].

31. 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[20].

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

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

[19] Texto Único Ordenado de la Ley N° 27444, Ley del Procedimiento Administrativo General, aprobado por Decreto Supremo N° 004-2019-JUS
"Artículo 257.- Eximentes y atenuantes de responsabilidad por infracciones
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."

[20] Reglamento de la Ley de Protección de Datos Personales, aprobado por Decreto Supremo N° 003-2013-JUS
"Artículo 126.- Atenuantes.
La colaboración con las acciones de la autoridad y el reconocimiento espontáneo de las infracciones acompañado de acciones de enmienda se considerarán atenuantes. Atendiendo a la oportunidad del reconocimiento y a las fórmulas de enmienda, la atenuación permitirá incluso la reducción motivada de la sanción por debajo del rango previsto en la Ley"

[21] Texto Único Ordenado de la Ley N° 27444, Ley del Procedimiento Administrativo General, aprobado por Decreto Supremo N° 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. Cuestiones en discusión

33. Corresponde a esta dirección determinar si se han cometido infracciones a la LPDP y su Reglamento, para lo cual se deberá analizar:

33.1 Si la administrada es responsable por los siguientes hechos infractores:

- Recopilar datos personales a través de los formularios "Contáctanos" y "Quejas y Reclamos" de la página web www.clinicamontehoreb.com.pe sin facilitar a los usuarios algún enlace a la política de privacidad que informe sobre lo requerido en el artículo 18 de la LPDP; configurando la infracción grave tipificada en el literal a) del numeral 2 del artículo 132 del Reglamento de la LPDP
- No haber inscrito en el RNPDP el banco de datos personales de los usuarios de la página web www.clinicamontehoreb.com.pe, incumpliendo con la obligación señalada en el artículo 78 del Reglamento de la LPDP; configurando la infracción leve tipificada en el literal e) del numeral 1 del artículo 132 de dicho reglamento.
- No haber comunicado al RNPDP la realización de flujo transfronterizo de los datos personales recopilados a través de los formularios mencionados, teniendo el servidor de datos de su página web en los Estados Unidos de América, incumpliendo lo dispuesto en el artículo 26 del Reglamento de la LPDP; configurando la infracción leve prevista en el literal e) del artículo 132 de aludido reglamento.
- No haber implementado las medidas de seguridad para el tratamiento de datos personales, dispuestas en los numerales 1 y 2 del artículo 39, así como en los artículos 40 y 42 del Reglamento de la LPDP; configurando la infracción grave prevista en el literal c) del numeral 2 del artículo 132 del reglamento señalado.

Dirección de Protección de Datos Personales
M. GONZALEZ

33.2 En el supuesto de ser responsable en cada caso, 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.

33.3 De ser el caso, el monto de la multa que corresponde imponer, tomando en consideración los criterios de graduación contemplados en el numeral 3) del artículo 248 de la LPAG.

V. Cuestión previa: Acerca del carácter objetivo de las infracciones

34. Mediante el Decreto Legislativo N° 1272, se añadió a los principios de la potestad sancionadora administrativa el principio de Culpabilidad, con el siguiente texto:

> **"Artículo 248.- Principios de la potestad sancionadora administrativa**
> La potestad sancionadora de todas las entidades está regida adicionalmente por los siguientes principios especiales:
> (...)
> **10. Culpabilidad. -** La responsabilidad administrativa es subjetiva, salvo los casos en que por ley o decreto legislativo se disponga la responsabilidad administrativa objetiva."

35. Dicho principio establece como regla que, para la evaluación de la responsabilidad administrativa, se deberá evaluar también los factores personales del agente, como son el dolo, la culpa, y factores como el conocimiento y la diligencia en casos de personas jurídicas, yendo más allá de la constatación de un incumplimiento tipificado como infracción.

36. A su vez, contempla como excepciones los casos en los que, por ley o decreto legislativo, se establece la responsabilidad objetiva para las infracciones.

37. Dicha situación es la que acontece con la LPDP desde el 16 de septiembre de 2017, fecha en la que entró en vigencia la modificatoria establecida por la Cuarta Disposición Complementaria Modificatoria del Decreto Legislativo N° 1353, Decreto Legislativo 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; norma mediante la cual se modificó el artículo 38 de dicha ley en los términos siguientes:

> **"Artículo 38. Tipificación de infracciones**
> Las infracciones se clasifican en leves, graves y muy graves, las cuales son tipificadas vía reglamentaria, de acuerdo a lo establecido en el numeral 4) del artículo 230 de la Ley N° 27444, Ley del Procedimiento Administrativo General, mediante Decreto Supremo con el voto aprobatorio del Consejo de Ministros.
>
> Sin perjuicio de las sanciones que en el marco de su competencia imponga la autoridad competente, esta puede ordenar la implementación de una o más medidas correctivas, con el objetivo de corregir o revertir los efectos que la conducta infractora hubiere ocasionado o evitar que ésta se produzca nuevamente.
>
> Los administrados son responsables objetivamente por el incumplimiento de obligaciones derivadas de las normas sobre protección de datos personales."

38. De acuerdo con las normas transcritas, para el caso de las infracciones detectadas a partir del 16 de septiembre de 2017, no existe la obligación de analizar el ámbito subjetivo de la responsabilidad de la administrada, bastando con la comprobación de índole objetivo, vale decir, centrándose en la existencia o no de una conducta antijurídica.

VI. Análisis de la cuestión en discusión

Sobre el presunto incumplimiento de lo dispuesto en el artículo 18 de la LPDP

39. El artículo 18 de la LPDP establece como uno de los derechos del titular de los datos personales a ser informado acerca del tratamiento que se efectuará sobre los mismos, según se cita a continuación:

> **"Artículo 18. Derecho de información del titular de datos personales**
> El titular de datos personales tiene derecho a ser informado en forma detallada, sencilla, expresa, inequívoca y de manera previa a su recopilación, sobre la finalidad para la que sus datos personales serán tratados; quiénes son o pueden ser sus destinatarios, la existencia del banco de datos en que se almacenarán, así como la identidad y domicilio de su titular y, de ser el caso, del encargado del tratamiento de sus datos personales; el carácter obligatorio o facultativo de sus respuestas al cuestionario que se le proponga, en especial en cuanto a los datos sensibles; la transferencia de los datos personales; las consecuencias de proporcionar sus datos personales y de su negativa a hacerlo; el tiempo durante el cual se conserven sus datos personales; y la posibilidad de ejercer los derechos que la ley le concede y los medios previstos para ello.
>
> Si los datos personales son recogidos en línea a través de redes de comunicaciones electrónicas, las obligaciones del presente artículo pueden satisfacerse mediante la publicación de políticas de privacidad, las que deben ser fácilmente accesibles e identificables.
> (...)"

40. Si bien el contenido de este artículo se relaciona con el requisito de validez de obtención del consentimiento concerniente a la información, primordialmente hace referencia a una obligación del responsable del tratamiento de datos personales, independiente de lo vinculado al consentimiento: Brindar al titular de los datos personales, información acerca del tratamiento que se realizará sobre sus datos, la finalidad de estos y la identidad de otros partícipes en tal tratamiento.

41. Durante la etapa de fiscalización, se detectó que la administrada recopilaba datos personales de los visitantes de su página web www.clinicamontehoreb.com.pe a través de los formularios "Contáctanos" y "Quejas y Reclamos", sin presentar adecuadamente la información requerida por el artículo 18 de la LPDP, de acuerdo con la imputación realizada por medio de la Resolución Directoral N° 129-2018-JUS/DGTAIPD-DFI.

42. En sus descargos, la administrada señaló haber generado el *link* para sus políticas de privacidad, lo cual fue constatado por el personal de la DFI, siendo dicha política de privacidad transcrita en el considerando 18 de esta resolución directoral.

43. Al respecto, esta dirección aprecia que en dicha política de privacidad, la administrada cumple con especificar las finalidades del tratamiento, detallando las acciones a desarrollar ("mantener un registro de usuarios, de pedidos en caso que aplique, y mejorar nuestros productos y servicios"); sin embargo, dicho documento carece de información respecto de la existencia del banco de datos personales donde se almacenan los datos recopilados, el tiempo durante el cual se conservarán tales datos, lo referente a su transferencia internacional (por la ubicación de su servidor de datos) y de la posibilidad del titular de ejercer sus derechos.

44. Por su parte, en su comunicación del 31 de octubre, la administrada alegó no haber cometido la infracción dolosamente.

45. Al respecto, conviene tomar en cuenta lo concluido en la cuestión previa a este acápite, siendo que la infracción se detectó en una fiscalización iniciada el 16 de octubre de 2017, luego de la entrada en vigencia del actual texto del artículo 38 de la LPDP; motivo por el cual, en este caso no se tendrá al dolo como elemento constitutivo de la responsabilidad de la administrada.

Dirección de Protección de Datos Personales
M. GONZALEZ L.

46. De otro lado, es preciso señalar que el personal de esta dirección detectó que la administrada no implementó cambios en su política de privacidad, como se puede apreciar en las impresiones adjuntas al expediente el 26 de abril de 2019, lo cual denota la ausencia de medidas de enmienda de la conducta infractora.

47. Por lo expuesto, la administrada resulta responsable por no haber proporcionado la información requerida en el artículo 18 de la LPDP a los visitantes de su página web, incurriendo en la infracción grave prevista en el literal a) del numeral 2 del artículo 132 del Reglamento de dicha ley.

Sobre el deber de inscribir los bancos de datos personales ante el Registro Nacional de Protección de Datos Personales

48. El artículo 34 de la LPDP dispone la creación del Registro Nacional de Protección de Datos Personales, que tiene entre sus finalidades inscribir los bancos de datos personales de administración pública o privada[22]; así también, permite que cualquier

[22] Ley N° 29733, Ley de Protección de Datos Personales
"Artículo 34. Registro Nacional de Protección de Datos Personales
Créase el Registro Nacional de Protección de Datos Personales como registro de carácter administrativo a cargo de la Autoridad Nacional de Protección de Datos Personales, con la finalidad de inscribir en forma diferenciada, a nivel nacional, lo siguiente:
1. Los bancos de datos personales de administración pública o privada, así como los datos relativos a estos que sean necesarios para el ejercicio de los derechos que corresponden a los titulares de datos personales, conforme a lo dispuesto en esta Ley y en su reglamento.
(...)
Cualquier persona puede consultar en el Registro Nacional de Protección de Datos Personales la existencia de bancos de datos personales, sus finalidades, así como la identidad y domicilio de sus titulares y, de ser el caso, de sus encargados."

ciudadano realice en él consultas sobre la existencia y finalidad de los bancos de datos personales inscritos, así como sobre la identidad y domicilio de sus titulares.

49. Por su parte, el artículo 78 del Reglamento de la LPDP establece el carácter obligatorio de la inscripción en el mencionado registro de los bancos de datos personales que las entidades generen:

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

> **"Artículo 78.- Obligación de inscripción.**
> 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.
> (...)"

50. El 26 de marzo de 2018, el personal a cargo del RNPDP informó a la DFI que la administrada contaba con los siguientes bancos de datos personales inscritos:

Banco de Datos Personales	N° de Resolución Directoral	Código de inscripción
Proveedores	861-2017-JUS/DGTAIPD-DPDP	RNPDP-PJP N° 13165
Pacientes	862-2017-JUS/DGTAIPD-DPDP	RNPDP-PJP N° 13166
Trabajadores	928-2017-JUS/DGTAIPD-DPDP	RNPDP-PJP N° 13218
Videovigilancia	929-2017-JUS/DGTAIPD-DPDP	RNPDP-PJP N° 13219

51. Durante la fiscalización, se detectó que la página web de la administrada contaba con las opciones "Contáctanos" y "Quejas y Reclamos", por medio de las cuales se recopilaba datos personales, sin que existiese un registro para el banco de datos personales correspondiente; siendo tal omisión imputada como infracción en la Resolución Directoral Nº 129-2018-JUS/DGTAIPD-DFI.

52. En sus descargos, la administrada indicó haber procedido con el trámite de inscripción de ambos bancos de datos personales, "Prospectos de Clientes" así como el denominado "Quejas y Reclamos".

53. Se puede apreciar en las resoluciones directorales N° 2433-2018-JUS/DGTAIPD-DPDP y N° 2492-2018-JUS/DGTAIPD-DPDP que dichas solicitudes fueron presentadas por la administrada el 17 de septiembre de 2018, vale decir, después de la notificación de imputación de cargos.

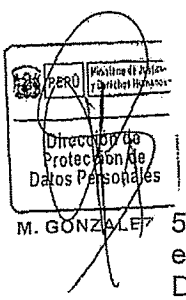
54. En tal sentido, se tiene que la administrada perfeccionó la acción de enmienda de esta infracción, por lo que corresponde atenuar su responsabilidad administrativa de acuerdo con el artículo 126 del Reglamento de la LPDP.

55. Por consiguiente, la administrada es responsable por la comisión de la infracción tipificada como leve en el literal e) del numeral 1 del artículo 132 del Reglamento de la LPDP, debiendo aplicarse en su caso la atenuación de su responsabilidad administrativa prevista en el artículo 126 del Reglamento de la LPDP.

Sobre la obligación de inscribir las comunicaciones de flujo transfronterizo de datos personales ante el Registro Nacional de Protección de Datos Personales

56. El numeral 2 del artículo 34 de la LPDP, describe una de las funciones del RNPDP, en los siguientes términos:

> **"Artículo 34. Registro Nacional de Protección de Datos Personales**
> Créase el Registro Nacional de Protección de Datos Personales como registro de carácter administrativo a cargo de la Autoridad Nacional de Protección de Datos Personales, con la finalidad de inscribir en forma diferenciada, a nivel nacional, lo siguiente:
> (...)
> 2. Las comunicaciones de flujo transfronterizo de datos personales."



57. Por su parte, el segundo párrafo del artículo 26 del Reglamento de la LPDP establece el deber de poner en conocimiento de la Autoridad Nacional de Protección de Datos Personales los flujos transfronterizos de datos personales que realice cada titular de bancos de datos personales, en todos los casos:

> **"Artículo 26.- Participación de la Dirección General de Protección de Datos Personales respecto del flujo transfronterizo de datos personales.**
>
> (...)
>
> En cualquier caso, el flujo transfronterizo de datos personales se pondrá en conocimiento de la Dirección General de Protección de Datos Personales, incluyendo la información que se requiere para la transferencia de datos personales y el registro de banco de datos."

58. Según se indicó en el Informe Técnico N° 62-2017-DFI-ORQR, la administrada efectuaba el flujo transfronterizo de los datos personales recopilados a través de los "Contáctanos" y "Quejas y Reclamos" de la página web www.clinicamontehoreb.com.pe, al ser dicha información dirigida al servidor de datos de la página web señalada, ubicada fuera del territorio peruano (Estados Unidos de América).

59. Habiendo sido imputada por tal omisión a través de la Resolución Directoral N° 129-2018-JUS/DGTAIPD-DFI, la administrada señaló que de acuerdo con el artículo 26 del Reglamento de la LPDP, ellos no transferían los datos personales, toda vez que los

remitían hacia el servidor de datos de su página web, manejado por una empresa encargada.

60. Para dilucidar dicha cuestión, es pertinente acudir a las definiciones presentes en el artículo 2 de la LPDP:

> **"Artículo 2. Definiciones**
> Para todos los efectos de la presente Ley, se entiende por:
> (...)
> **8. Flujo transfronterizo de datos personales.** Transferencia internacional de datos personales a un destinatario situado en un país distinto al país de origen de los datos personales, sin importar el soporte en que estos se encuentren, los medios por los cuales se efectuó la transferencia ni el tratamiento que reciban.
> (...)
> **16. Transferencia de datos personales.** Toda transmisión, suministro o manifestación de datos personales, de carácter nacional o internacional, a una persona jurídica de derecho privado, a una entidad pública o a una persona natural distinta del titular de datos personales.
>
> **19. Tratamiento de datos personales.** Cualquier operación o procedimiento técnico, automatizado o no, que permite la recopilación, registro, organización, almacenamiento, conservación, elaboración, modificación, extracción, consulta, utilización, bloqueo, supresión, comunicación por transferencia o por difusión o cualquier otra forma de procesamiento que facilite el acceso, correlación o interconexión de los datos personales."

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

61. De tales definiciones, se desprende que la LPDP establece que todo acto de traslado de datos personales a cualquier entidad o persona que no sea el titular de tal información constituye transferencia.

62. Ahora bien, es conveniente señalar que la definición del flujo transfronterizo de datos personales consta de una similar amplitud, pues lo único determinante es la transferencia de tales datos fuera del territorio nacional, sin importar los medios ni lo concerniente al tratamiento que vayan a recibir.

63. Así, tampoco es relevante el lapso durante el cual dure el almacenamiento efectuado que, en el presente caso, se efectúa en el servidor de datos de propiedad de la empresa contratada para el alojamiento de la información recopilada por medio de la página web de la administrada.

64. Sabiendo entonces que hubo remisión de datos personales por parte de la administrada a su proveedor de servicios de alojamiento web ubicado en el extranjero, es preciso reiterar lo establecido en el considerando 57 de esta resolución directoral, lo cual configura la obligación de inscripción del flujo transfronterizo descrito, más allá del nivel de protección que ofrezca cada país, no siendo determinante que la transferencia se efectúe a un país de alto o bajo nivel de protección para eximirse de la obligación de inscripción del flujo transfronterizo.

65. Por otro lado, es preciso advertir que la administrada, el 22 de octubre de 2018, presentó la solicitud de inscripción de flujo transfronterizo de los datos personales almacenados en los bancos de datos personales "Prospectos de Clientes" y "Quejas y Reclamos", inscripciones que se otorgaron por medio de las resoluciones directorales N° 3071-2018-JUS/DGTAIPD-DPDP y N° 3072-2018-JUS/DGTAIPD-DPDP.

66. En el presente caso, se tiene que la administrada, apenas obtuvo la inscripción de dichos bancos de datos personales, tramitó la inscripción de flujo transfronterizo, lo cual constituye una acción de enmienda oportuna, la cual fue perfeccionada con la emisión de las resoluciones directorales señaladas.

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

67. La situación descrita habilita la aplicación de la atenuante de responsabilidad administrativa de esta infracción, de acuerdo con lo previsto en el artículo 126 del Reglamento de la LPDP.

68. Por consiguiente, la administrada es responsable por la comisión de la infracción tipificada como leve en el literal e) del numeral 1 del artículo 132 del Reglamento de la LPDP, responsabilidad administrativa atenuada en mérito del artículo 126 del Reglamento de la LPDP.

Sobre el incumplimiento de las disposiciones reglamentarias referidas a las medidas de seguridad y la contravención al principio de Seguridad de la LPDP

69. 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."

70. A mayor abundamiento, el artículo 16 de dicha ley señala 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. 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."

71. 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, según se cita a continuación:

"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."

72. Dicha disposición establece la obligación a cargo de los responsables del tratamiento de controlar la gestión de los accesos y las acciones a realizar con los datos personales que maneja, debiendo predeterminar accesos y privilegios de acción sobre los mismos de acuerdo con un criterio documentado, así como la de tener registro de

los pormenores de cada operación de tratamiento de los datos personales relevante, como la identidad de quién la efectuó, el momento en que se realizó y en qué consistió.

73. Durante la fiscalización, se informó al personal fiscalizador que la administrada no cuenta con los procedimientos de gestión de accesos, de privilegios y de verificación periódica de privilegios asignados respecto al banco de datos de pacientes.

74. Las situaciones descritas fueron reportadas a través del Informe N° 54-2018-JUS/DGTAIPD-DFI-KAT y, por ende, fueron objeto de imputación por medio de la Resolución Directoral N° 129-2018-JUS/DGTAIPD-DFI.

75. En sus descargos, la administrada señala haber implementado un sistema de gestión de accesos, de privilegios y de verificación de estos, adjuntando una imagen que corresponde al inicio del sistema; sin embargo, no remite la documentación específica de dichos procedimientos.

76. El 28 de marzo de 2019, mediante Oficio N° 748-2019-JUS/DGTAIPD-DPDP, se solicitó a la administrada que acredite el cumplimiento de las medidas de seguridad establecidas en el numeral 1 del artículo 39 del Reglamento de la LPDP.

77. Posteriormente, en su escrito del 12 de abril de 2019, la administrada remitió el documento denominado "Protocolo de Acceso a Base de Datos de 'Sistema de Gestión de Clínica'", con el cual, según el Informe Técnico N° 063-2019-DFI-ETG, cumpliría con documentar sus procedimientos de gestión de accesos y gestión de privilegios, mas no documenta el procedimiento de verificación periódica de privilegios respecto al banco de datos de pacientes.

78. Dicha circunstancia demuestra que la administrada no perfecciona la acción de enmienda prevista en el artículo 126 del Reglamento de la LPDP, respecto del incumplimiento del numeral 1 del artículo 39 del mismo; aun así, se tomará en cuenta la presentación del mencionado documento de seguridad al momento de determinar la sanción.

79. De otro lado, al verificarse el presunto incumplimiento del numeral 2 del artículo 39 del Reglamento de la LPDP, se reportó este por medio del Informe N° 54-2018-JUS/DGTAIPD-DFI-RCCDL, imputándose tal incumplimiento como una infracción en la Resolución Directoral N° 129-2018-JUS/DGTAIPD-DFI.

80. En sus descargos, la administrada señaló que el sistema de gestión de procedimientos que había implementado en el tratamiento automatizado de los datos personales, tenía las herramientas necesarias para saber sobre las interacciones efectuadas por los usuarios del sistema; sin embargo, no adjuntó la documentación que sustente tal afirmación.

81. El 28 de marzo de 2019, mediante Oficio N° 748-2019-JUS/DGTAIPD-DPDP, se solicitó a la administrada que acredite el cumplimiento de las medidas de seguridad establecidas en el numeral 2 del artículo 39 del Reglamento de la LPDP.

82. En su escrito del 12 de abril de 2019, la administrada reitera el haber implementado un sistema que permite saber los pormenores del acceso de cada usuario; sin embargo, en el Informe Técnico N° 063-2019-DFI-ETG, se señala que no presenta evidencia sobre la generación de registros de interacción lógica con los datos personales de pacientes.

83. En tal sentido, se tiene que la administrada es responsable por el incumplimiento de la disposición del numeral 2 del artículo 39 del Reglamento de la LPDP, sobre el cual no adoptó ninguna medida.

84. De otro lado, el artículo 40 del Reglamento de la LPDP establece lo siguiente:

"Artículo 40.- Conservación, respaldo y recuperación de los datos personales.

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

(...)"

85. Dicha disposición establece la obligación de adoptar medidas de seguridad físicas en torno al servidor de datos que contenga información personal, a fin de evitar el deterioro o destrucción de este soporte, buscando preservar con ello la integridad y disponibilidad de los datos personales alojados.

86. Durante la fiscalización, se verificó que el servidor que aloja los datos personales de los pacientes de la administrada, estaba ubicado en un ambiente compartido, careciendo de detector de humo, alarma contra incendios y gabinete para servidor.

87. Tal situación fue reportada en el Informe N° 54-2018-JUSDGTAIPD-DFI-RCCDL, para ser incorporada en una de las imputaciones de la Resolución Directoral N°129-2018-JUS/DGTAIPD-DFI.

88. En sus descargos, la administrada señaló haber implementado los mencionados dispositivos de seguridad señalados, así como lo dispuesto por Defensa Civil, lo cual puede verificarse por medio de las fotos adjuntas a su comunicación[23].

[23] Folio 81 al 82

89. Por ello, en el Informe Técnico N° 231-2018-DFI-ORQR, se concluye que la administrada contaba con las medidas de seguridad requeridas por el artículo 40 del Reglamento de la LPDP.

90. En tal sentido, la administrada ha perfeccionado la acción de enmienda contemplada en el artículo 126 del Reglamento de la LPDP, habilitando la atenuación de la responsabilidad derivada del incumplimiento del artículo 40 de dicho reglamento.

91. Por su parte, el artículo 42 del Reglamento de la LPDP dispone lo siguiente:

> **"Artículo 42.- Almacenamiento de documentación no automatizada.**
> Los armarios, archivadores u otros elementos en los que se almacenen documentos no automatizados con datos personales deberán encontrarse en áreas en las que el acceso esté protegido con puertas de acceso dotadas de sistemas de apertura mediante llave u otro dispositivo equivalente. Dichas áreas deberán permanecer cerradas cuando no sea preciso el acceso a los documentos incluidos en el banco de datos.
>
> Si por las características de los locales que se dispusiera no fuera posible cumplir lo establecido en el apartado anterior, se adoptarán las medidas alternativas, conforme a las directivas de la Dirección General de Protección de Datos Personales."

92. La disposición precitada señala el propósito de mantener la documentación no automatizada que contenga datos personales, fuera del alcance de la generalidad del personal de la entidad responsable del tratamiento, o a disposición de cualquiera que acceda a su establecimiento, proponiendo como herramienta los mecanismos de apertura con llave o equivalentes.

93. Durante la visita de fiscalización, se verificó que las historias clínicas se almacenan en estantes de madera sin llave, en un ambiente cuya puerta carece de cerradura, circunstancia que fue reportada en el Informe N° 54-2018-JUSDGTAIPD-DFI-RCCDL, para ser incorporada en una de las imputaciones de la Resolución Directoral N°129-2018-JUS/DGTAIPD-DFI.

94. En sus descargos, la administrada señaló haber implementado una cerradura para el ambiente donde almacenan las historias clínicas, lo cual sustenta con la fotografía adjunta a su escrito[24].

95. Por ello, en el Informe Técnico N° 231-2018-DFI-ORQR, se concluye que la administrada implementó debidamente las medidas de seguridad requeridas por el artículo 42 del Reglamento de la LPDP.

96. En tal sentido, la administrada ha perfeccionado la acción de enmienda contemplada en el artículo 126 del Reglamento de la LPDP, habilitando la atenuación de la responsabilidad derivada del incumplimiento de dicho artículo.

97. En resumen, se tiene comprobada la responsabilidad de la administrada por la comisión de la infracción tipificada como grave en el literal c) del numeral 2 del artículo 132 del Reglamento de la LPDP, por efectuar el tratamiento de datos sensibles de sus pacientes (datos relativos a salud) en incumplimiento de las disposiciones del artículo 39, 40 y 42, debiendo atenuarse su responsabilidad respecto de los incumplimientos de

[24] Folio 82

los dos últimos artículos mencionados por haber enmendado la conducta infractora, en aplicación del artículo 126 del Reglamento de la LPDP.

Sobre las normas sancionadoras a aplicar a los hechos analizados

98. La Tercera Disposición Complementaria Modificatoria del Reglamento del Decreto Legislativo N° 1353, incorporó el artículo 132 al Título VI sobre Infracciones y Sanciones de dicho reglamento, que en adelante tipifica las infracciones.

99. 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[25], sin perjuicio de las medidas correctivas que puedan determinarse de acuerdo con el artículo 118 del Reglamento de la LPDP[26].

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

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

- Recopilar datos personales a través de los formularios "Contáctanos" y "Quejas y Reclamos" de la página web www.clinicamontehoreb.com.pe sin facilitar a los usuarios algún enlace a la política de privacidad que informe sobre lo requerido en el artículo 18 de la LPDP; configurando la infracción tipificada como grave en el literal

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

[26] **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."

a) del numeral 2 del artículo 132 del Reglamento de la LPDP, sancionable con una multa de entre cero coma cinco (5) y cincuenta (50) unidades impositivas tributarias, de acuerdo con lo establecido en el artículo 39 de dicha ley.

- No haber inscrito en el RNPDP el banco de datos personales de los usuarios de la página web www.clinicamontehoreb.com.pe, incumpliendo con la obligación señalada en el artículo 78 del Reglamento de la LPDP; configurando la infracción leve tipificada en el literal e) del numeral 1 del artículo 132 de dicho reglamento, sancionable con una multa de entre cero coma cinco (0,5) y cinco (5) unidades impositivas tributarias, de acuerdo con lo establecido en el artículo 39 de la LPDP.
- No haber comunicado al RNPDP la realización de flujo transfronterizo de los datos personales recopilados a través de los formularios, teniendo el servidor de datos de la página web en los Estados Unidos de América, incumpliendo lo dispuesto en el artículo 26 del Reglamento de la LPDP; lo cual configura la infracción tipificada como leve en el literal e) del numeral 1 del artículo 132 de dicho reglamento, sancionable con una multa de entre cero coma cinco (0,5) y cinco (5) unidades impositivas tributarias, de acuerdo con lo establecido en el artículo 39 de la LPDP.
- No haber implementado las medidas de seguridad para el tratamiento de los datos personales, dispuestas en los artículos 39, 40 y 42 del Reglamento de la LPDP; dicha situación configura la infracción grave prevista en el literal c) del numeral 2 del artículo 132 del señalado reglamento, sancionable con una multa de entre cero coma cinco (5) y cincuenta (50) unidades impositivas tributarias, de acuerdo con lo establecido en el artículo 39 de dicha ley.

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

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

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

No se ha evidenciado beneficio ilícito alguno resultante de la comisión de las infracciones a sancionar.

b) La probabilidad de detección de las infracciones:

Respecto del incumplimiento del artículo 18 de la LPDP, se debe señalar que el mismo pudo apreciarse en su momento con la sola visita a la página web de la administrada, verificándose el contenido del documento informativo aplicable a dicha página web. Por tal motivo, la probabilidad de detección de dicha infracción es alta.

Sobre la no inscripción en el RNPDP de los bancos de datos personales vinculados a la información recopilada por medio de la página web de la administrada, se tiene que la información concerniente a los registros de bancos de datos está en poder de esta dirección, teniendo los recursos suficientes para detectar tal infracción. En tal sentido, la probabilidad de detección es alta.

Sobre la no inscripción en el RNPDP del flujo transfronterizo de los datos personales recopilados a través de la página web de la administrada, se debe tomar en cuenta

que durante la fiscalización, se utilizó el aplicativo web www.whois.domaintools.com (gratuito) para ubicar el servidor de datos de la mencionada página web[27]; de otro lado, al igual que con la infracción anterior, al tener esta dirección el control del RNPDP, tiene el recurso para detectar esta infracción. Por tal motivo, la probabilidad de detección de esta infracción es alta.

En lo concerniente al incumplimiento en la adopción de medidas de seguridad, debe señalarse que se detectaron los hechos de tal infracción durante la visita de fiscalización realizada, al ser una operación interna de la administrada, con lo que se tiene que su probabilidad de detección es baja.

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

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 LPDP y su reglamento.

Respecto del incumplimiento del artículo 18 de la LPDP, debe señalarse que implica la vulneración del derecho de los titulares de los datos personales a ser informados sobre el tratamiento que efectuará el responsable, al no brindarse de forma completa la información requerida por dicho artículo.

Por su parte, la omisión de la inscripción de los bancos de datos personales y de la comunicación del flujo transfronterizo de los datos personales recopilados a través de la página web de la administrada implica no informar a los titulares de datos personales sobre la transferencia de sus datos fuera del territorio nacional, información que se obtiene a través del RNPDP, lo cual también implica una interferencia al ejercicio de su derecho a ser informado, aparte del cumplimiento de la formalidad establecida en la normativa.

De otro lado, sobre la no aplicación de medidas de seguridad al tratamiento de los datos personales que administra, que configura el incumplimiento de los artículos 39, 40 y 42 del Reglamento de la LPDP, implica que efectúa un tratamiento que en el que no se tiene el suficiente control sobre las personas que lo realizan, ni se tuvo en su momento los dispositivos necesarios para mantener los soportes y documentos

[27] Folio 53

que almacenan datos personales sensibles, lo que incrementa el riesgo de afectación a la confidencialidad e integridad de los datos.

d) El perjuicio económico causado:

No se evidencia un perjuicio económico resultante de la comisión de las infracciones analizadas.

e) La reincidencia en la comisión de las infracciones:

Del mismo modo, se tiene en cuenta que la administrada no es reincidente, ya que no ha sido sancionado en alguna otra ocasión por las infracciones señaladas.

f) Las circunstancias de la comisión de las infracciones:

Respecto del incumplimiento del artículo 18 de la LPDP, es preciso señalar que la administrada implementó una política de privacidad que no cumple con informar sobre todos los factores señalados en dicho artículo, por lo que se tiene por no enmendada la infracción.

Sobre la no inscripción en el RNPDP de los bancos de datos personales vinculados a la información recopilada por medio de la página web de la administrada, se tiene que al haber obtenido las inscripciones de los bancos de datos personales de "Prospectos de Clientes" y "Quejas y Reclamos", se enmendó la conducta infractora, debiendo aplicarse la atenuante de responsabilidad administrativa prevista en el artículo 126 del Reglamento de la LPDP.

Sobre la omisión de inscribir la comunicación del flujo transfronterizo de los datos personales al RNPDP, debe señalarse también que la administrada, obtuvo la inscripción del flujo transfronterizo vinculado con los bancos de datos personales antes señalados, propiciando la atenuación de su responsabilidad, según lo previsto en el artículo 126 del Reglamento de la LPDP.

Respecto del incumplimiento de las disposiciones sobre medidas de seguridad previstas en los artículos 39, 40 y 42 del Reglamento, se debe precisar que la administrada perfeccionó las medidas de enmienda solo en los casos de los dos últimos artículos reglamentarios aludidos, respecto de los cuales también corresponde la atenuación de la responsabilidad, según el artículo 126 del Reglamento de la LPDP.

Por su parte, es necesario tomar en cuenta que, durante todo el procedimiento, la administrada mantuvo un comportamiento colaborador con la autoridad, respondiendo a todos los requerimientos de información que se le hizo.

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

En lo referente a la omisión de poner a disposición de los visitantes de la página web una política de privacidad, se evidenció durante el presente procedimiento la intención de enmendar dicha omisión y revertir su negligencia, pese a no perfeccionar la enmienda

En lo concerniente a la inscripción de los bancos de datos personales y a la omisión de inscripción del flujo transfronterizo de los datos personales recopilados a través de la mencionada página web, se debe señalar que la administrada, a pesar de su

desconocimiento respecto de esta modalidad de tratamiento y las obligaciones que conlleva, demostró su intención de no seguir infringiendo la normativa, al emprender los trámites correspondientes, perfeccionando la enmienda.

En lo que refiere al incumplimiento de las disposiciones sobre medidas de seguridad contempladas en el Reglamento de la LPDP, es preciso señalar que la administrada demostró la intención de enmendar los incumplimientos, con las acciones encaminadas a su enmienda.

103. Es pertinente indicar que para imponer la sanción se tendrá en cuenta la suma de todos los criterios que permiten graduar la sanción conforme a los argumentos desarrollados en el considerando 102 de la presente resolución directoral.

104. De otro lado, respecto de las sanciones recomendadas por la DFI por medio de su Informe N° 102-2018-JUS/DGTAIPD-DFI, debe señalarse que el mismo se emite para el cierre de la instrucción, siguiendo las disposiciones del artículo 255 de la LPAG que se citan a continuación:

"Artículo 255.- Procedimiento sancionador

Las entidades en el ejercicio de su potestad sancionadora se ciñen a las siguientes disposiciones:

(...)

5. Concluida, de ser el caso, la recolección de pruebas, la autoridad instructora del procedimiento concluye determinando la existencia de una infracción y, por ende, la imposición de una sanción; o la no existencia de infracción. La autoridad instructora formula un informe final de instrucción en el que se determina, de manera motivada, las conductas que se consideren probadas constitutivas de infracción, la norma que prevé la imposición de sanción; y, la sanción propuesta o la declaración de no existencia de infracción, según corresponda."

105. De dicha norma citada, se desprende que la sanción que propone la DFI no es vinculante para esta dirección, siendo solo una propuesta a evaluar por la autoridad resolutora, cuyo criterio es independiente de la autoridad que llevó a cabo la instrucción.

106. Ahora bien, es necesario tomar en cuenta que de acuerdo con lo informado por la administrada, el 10% del resultado bruto de sus ventas, que constituye el límite máximo del monto de la multa, asciende a S/ [redacted]

Por las consideraciones expuestas y de conformidad con lo dispuesto por la LPDP y su reglamento, la LPAG, y el Reglamento del Decreto Legislativo N° 1353 que crea la Autoridad Nacional de Transparencia y Acceso a la Información Pública, fortalece el Régimen de Protección de Datos Personales y la regulación de la gestión de intereses aprobado por Decreto Supremo N° 019-2017-JUS;

SE RESUELVE:

Artículo 1.- Sancionar a Clínica Monte Horeb S.A. con la multa ascendente a siete unidades impositivas tributarias (7 UIT), por haber recopilado datos personales a través de los formularios "Contáctanos" y "Quejas y Reclamos" de la página web www.clinicamontehoreb.com.pe sin facilitar a los usuarios algún enlace a la política de privacidad que informe sobre lo requerido en el artículo 18 de la LPDP; conducta prevista como infracción grave en el literal a) del numeral 2 del artículo 132 del Reglamento de la LPDP, esto es, *"no atender, impedir u obstaculizar el ejercicio de los derechos del titular de datos personales de acuerdo a lo establecido en el título III de la Ley N° 29733 y su Reglamento"*.

Artículo 2.- Sancionar a Clínica Monte Horeb S.A. con la multa ascendente a cero coma cinco unidades impositivas tributarias (0,5 UIT) por no haber inscrito en el RNPDP los bancos de datos personales de la información recopilada por medio de los formularios "Contáctanos" y "Quejas y Reclamos" de la página web www.clinicamontehoreb.com.pe, conducta que configura la infracción leve prevista 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"*.

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

Artículo 3.- Sancionar a Clínica Monte Horeb S.A. con la multa ascendente a cero coma cinco unidades impositivas tributarias (0,5 UIT) por no haber comunicado al RNPDP la realización de flujo transfronterizo de los datos personales recopilados a través de los formularios de la mencionada página web, conducta que configura la infracción leve prevista 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"*.

Artículo 4.- Sancionar a Clínica Monte Horeb S.A. con la multa ascendente a cinco coma cinco unidades impositivas tributarias (5,5 UIT) por el incumplimiento de las disposiciones de los artículos 39, 40 y 42 del Reglamento de la LPDP; conducta tipificada como infracción grave en el literal c) del numeral 2 del artículo 132 del Reglamento de la LPDP, esto es, *"realizar tratamiento de datos personales sensibles incumpliendo las medidas de seguridad establecidas en la normativa sobre la materia"*.

Artículo 5.- Imponer como medidas correctivas a Clínica Monte Horeb S.A., las siguientes:

- Presentar en su página web, la política de privacidad que incluya información sobre todos los factores cuya indicación se exige (indicación de existencia del banco de datos personales donde se almacenan los datos recopilados, el tiempo durante el cual se conservarán tales datos, lo referente a su transferencia

nacional e internacional, identidades de los destinatarios, posibilidad del titular de ejercer sus derechos y la forma de hacerlo).
- Remitir la documentación de su procedimiento de verificación periódica de los privilegios asignados para el sistema automatizado con el que se efectúa el tratamiento de los datos personales de pacientes.
- Remitir documentación que sustente la generación y mantenimiento de registro de interacción lógica con el banco de datos personales automatizado de pacientes.

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

Artículo 6.- Informar a Clínica Monte Horeb 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[28].

Artículo 7.- Informar a Clínica Monte Horeb 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 entiende que se cumple con pagar la multa impuesta, si antes de que venza el plazo establecido en el requerimiento de pago, se cancela el 60% de la multa impuesta, de conformidad con lo dispuesto en el artículo 128 del Reglamento de la LPDP[29].

---

[28] **Texto Único Ordenado de la Ley N° 27444, Ley del Procedimiento Administrativo General, aprobado por Decreto Supremo N° 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."

[29] **Reglamento de la Ley de Protección de Datos Personales, aprobado por Decreto Supremo N° 003-2013-JUS**
"Artículo 128.- Incentivos para el pago de la sanción de multa.
Se considerará que el sancionado ha cumplido con pagar la sanción de multa si, antes de vencer el plazo otorgado para pagar la multa, deposita en la cuenta bancaria determinada por la Dirección General de Protección de Datos Personales el sesenta por ciento (60%) de su monto. Para que surta efecto dicho beneficio deberá comunicar tal hecho a la Dirección General de Protección de Datos Personales, adjuntando el comprobante del depósito bancario correspondiente. Luego de dicho plazo, el pago sólo será admitido por el íntegro de la multa impuesta."

Artículo 8.- Notificar a Clínica Monte Horeb S.A. la presente resolución directoral.

Regístrese y comuníquese.

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