REPÚBLICA DEL PERÚ

Resolución Directoral

Expediente N°
009-2017-JUS/DPDP-PS

Resolución N° 791-2017-JUS/DGTAIPD-DPDP

Lima, 09 noviembre de 2017

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

VISTOS: El Informe Nº 066-2016-JUS/DGPDP-DSC del 22 de septiembre de 2016, que se sustenta en las Actas de Fiscalización N° 01-2016 y N° 02-2016 del 18 de mayo de 2016 (Expediente de Fiscalización Nº 021-2016-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;

CONSIDERANDO:

I. Antecedentes

1. Mediante la Orden de Visita de Fiscalización Nº 020-2016-JUS/DGPDP-DSC, la DSC dispuso la realización de una visita de fiscalización a EMPRESA DE GENERACIÓN ELÉCTRICA AREQUIPA S.A., identificada con R.U.C. N° 20216293593, (en adelante, EGASA), con la finalidad de supervisar el tratamiento realizado sobre los datos personales de sus trabajadores.

2. En virtud de la mencionada orden, el 18 de mayo de 2016, el personal de la DSC realizó visitas de fiscalización a los siguientes establecimientos de EGASA:

- Establecimiento ubicado en el pasaje Ripacha N° 101, distrito y provincia de Arequipa, departamento de Arequipa.
- Establecimiento ubicado en la calle Ramón Castilla N° 729, distrito de Cayma, provincia y departamento de Arequipa.

Al finalizar cada visita, se levantaron las actas de Fiscalización N° 01-2016 y 02-2016.

3. Se constató que EGASA realiza a través de medio automatizado (sistema "Sygnus"), tratamiento de los siguientes datos personales: Imagen, código, apellido paterno, apellido materno, nombres, tipo de identificación, número de identificación, e-mail, fecha de nacimiento, estado civil, teléfonos, grupo sanguíneo, compañía, título puesto, lugar de trabajo, tipo trabajador, categoría, fecha de ingreso, fecha último ingreso, fecha de término.

4. Asimismo, se verificó que realizan el tratamiento en soporte no automatizado a través de la ficha de datos del personal y ficha personal del trabajador, los cuales se almacenan en archivadores tipo palanca, junto al contrato de trabajo, el currículum documentado, partidas de nacimiento y matrimonio, así como los antecedentes penales, policiales y judiciales de cada trabajador.

5. El 22 de septiembre de 2016, se puso en conocimiento de la Dirección de Sanciones (en adelante, la DS) el resultado de la fiscalización realizada a dicha entidad por medio del Informe Nº 066-2016-JUS/DGPDP-DSC, adjuntando las actas de fiscalización mencionadas, así como los demás anexos y documentos que conforman el respectivo expediente administrativo.

6. Mediante la Resolución Directoral Nº 272-2016-JUS/DGPDP-DS, la DS resolvió iniciar procedimiento administrativo sancionador a EGASA, por la presunta comisión de la infracción prevista en el literal a. del numeral 2 del artículo 38 de la Ley Nº 29733, Ley de Protección de Datos Personales (en adelante, LPDP).

Se atribuye a EGASA dar tratamiento a los datos personales de sus trabajadores incumpliendo lo dispuesto en el numeral 1 del artículo 39 y en el artículo 42 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."*

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

7. Dicha Resolución Directoral se notificó a EGASA el 17 de febrero de 2017, mediante el Oficio Nº 593-2016-JUS/DGPDP-DS del 30 de diciembre de 2016.

8. Por medio de la comunicación ingresada con la Hoja de Trámite N° 14661 del 13 de marzo de 2017, EGASA presentó sus descargos, exponiendo lo siguiente:

> 8.1 Por medio de la Orden de Servicio N° 286-2016 del 18 de octubre de 2016, contrataron a un proveedor para realizar la actualización normativa para la administración y control de acceso a los recursos TIC, implementando los procedimientos de gestión de accesos y privilegios, así como su revisión periódica. Dicho servicio se cumplió el 30 de diciembre de 2016, con la entrega de los documentos como los denominados "Procedimiento de Creación/Modificación/Baja de Usuarios para Acceder a Redes de Información y Servicios TIC" y "Procedimiento de Acceso a Sistemas de Información y Aplicaciones Software".
>
> 8.2 El departamento de Recursos Humanos implementado dos armarios de madera de cuatro compartimientos cada uno, con puertas corredizas y llaves de seguridad, para almacenar documentos no automatizados que contengan datos personales de los trabajadores, teniendo acceso protegido con puertas que cuentan con llaves de seguridad, como se puede apreciar en las tres fotografías; dichas llaves son debidamente guardadas por el personal de dicho departamento.

9. Por medio de la Resolución Directoral Nº 081-2017-JUS/DGPDP-DS del 16 de mayo de 2017, notificada el 7 de junio de 2017, la DS, 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.

10. Mediante la comunicación ingresada con la Hoja de Trámite N° 35362 del 13 de junio de 2017, EGASA solicitó informe oral, el cual fue concedido por la DS por medio del Oficio N° 198-2017-JUS/DGPDP-DS, para realizarse el 3 de julio de 2017.

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

9. Mediante el Oficio N° 117-2017-JUS/DPDP del 8 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 EGASA ha implementado las medidas de seguridad necesarias para el tratamiento de datos personales, de acuerdo con el contenido de su descargo.

10. A través del Oficio N° 40-2017-JUS/DGTAIPD-DFI del 15 de agosto de 2017, el Director de Fiscalización e Instrucción remitió el Informe N° 011-2017-DFI-VARS, por el cual se dio respuesta a lo solicitado por esta Dirección, indicando lo siguiente:

- Por medio de los documentos presentados en su descargo, EGASA dio cumplimiento a la obligación prevista en el numeral 1 del artículo 39 del Reglamento de la LPDP.
- Respecto a la implementación de medidas de seguridad para el almacenamiento de documentación no automatizada, EGASA ha remitido evidencia fehaciente de haberlas adecuado a lo dispuesto por el artículo 42 del Reglamento de la LPDP.

II. Competencia

11. 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. Normas aplicables y cuestión en discusión

12. 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.

13. Mediante el 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.

14. 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, estaría en vigencia el artículo 132 del Reglamento de la LPDP que tipifica las infracciones; sin embargo, dado que el presente procedimiento sancionador se inició estando vigentes las infracciones señaladas en el artículo 38 de la LPDP, se aplicará la disposición sancionadora más favorable al administrado.

15. En tal sentido, para emitir pronunciamiento se debe determinar si EGASA es responsable por el incumplimiento de la LPDP y su reglamento consistente 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 sus trabajadores a través de su sistema automatizado "Sygnus", ni la verificación periódica de tales privilegios, incumpliendo con el numeral 1 del artículo 39 del Reglamento de la LPDP; y,
(ii) efectuar el almacenamiento de documentación no automatizada que contiene datos personales de sus trabajadores en un área que no cuenta con cerradura o equivalente, incumpliendo lo dispuesto en el artículo 42 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 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"*.

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.
(...)"

IV. Análisis de la cuestión en discusión

Sobre la presunta infracción al numeral 1 del artículo 39 del Reglamento de la LPDP

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

16. Acerca del tratamiento automatizado de datos personales, es necesario tener en cuenta el numeral 1 del artículo 39 del Reglamento de la LPDP, que señala lo siguiente:

> *"**Artículo 39**.- Seguridad para el tratamiento de la información digital.*
> *Los sistemas informáticos que manejen bancos de datos personales deberán incluir en su funcionamiento:*
>
> *1. El control de acceso a la información de datos personales incluyendo la gestión de accesos desde el registro de un usuario, la gestión de los privilegios de dicho usuario, la identificación del usuario ante el sistema, entre los que se encuentran usuario, contraseña, uso de certificados digitales, tokens, entre otros, y realizar una verificación periódica de los privilegios asignados, los cuales deben estar definidos mediante un procedimiento documentado a fin de garantizar su idoneidad."*

17. Durante la fiscalización realizada a EGASA, se verificó que esta entidad administra el banco de datos personales de sus trabajadores en soporte automatizado, por medio del sistema "Sygnus"; por tal motivo 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.

18. En relación a lo mencionado en el considerando 15, se debe indicar que en el Informe Nº 066-2016-JUS/DGPDP-DSC, la DSC concluyó lo siguiente:

> *"2. **Empresa de Generación Eléctrica Arequipa S.A. - EGASA** no cuenta con las medidas de seguridad necesarias para la protección de datos personales, de acuerdo con las exigencias de la LPDP y su reglamento. Dicha omisión constituiría infracción de acuerdo a lo señalado en el literal a) del numeral 2 del artículo 38° de la LPDP."*

19. Al respecto, el mencionado informe de la DSC señala lo siguiente:

> *"19. Se verificó que EGASA no documenta los procedimientos de gestión de accesos, gestión de privilegios y la revisión periódica de privilegios para el acceso a los datos personales de los trabajadores (...)"*

20. Dicha aseveración se sostiene en el Acta de Fiscalización N° 02-2016, dotada de fe pública de acuerdo con el artículo 101 del Reglamento de la LPDP[3], que señala lo siguiente:

> *"Se verificaron las medidas de seguridad en la computadora asignada al asistente de planillas, verificándose lo siguiente: (...) 6) No cuenta con procedimientos documentados referente a gestión de accesos y gestión de privilegios (...)"*

Con esta verificación, la DSC ha evidenciado que EGASA, respecto del banco de datos automatizado de sus trabajadores, no cuenta con la documentación de sus procedimientos de gestión de accesos ni de gestión de privilegios, incumpliendo con la obligación establecida en el numeral 1 del artículo 39 del Reglamento de la LPDP, por lo que la DS le imputó dicho cargo a través de la Resolución Directoral N° 272-2016-JUS/DGPDP-DS.

21. Ahora bien, 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 infractor, si es realizada de forma previa a la notificación de imputación de cargos[4].

22. En el presente caso, como se detalló en el considerando 10 de la presente resolución, EGASA contrató la realización de documentos por los cuales se establezcan los procedimientos de gestión de accesos, gestión de privilegios y verificación periódica de estos. Es así que el 30 de diciembre de 2016, dicha entidad contaba con los documentos denominados "Política de Acceso a la Información" y principalmente, "Procedimiento de Creación/Modificación/Baja de Usuarios para Acceder a Redes de Información y Servicios TIC" y "Procedimiento de Acceso a Sistemas de Información y Aplicaciones Software".

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

23. Cabe señalar que en el segundo de los mencionados documentos, se establecen las responsabilidades que cada área tiene en la creación y asignación de usuarios de los recursos de tecnología de la información en general, así como los permisos con los que cada uno de estos contaría.

24. Más específicamente, el documento denominado "Procedimiento de Acceso a Sistemas de Información y Aplicaciones Software", se desarrolla el proceso por el cual se tramita, dentro de la entidad, las creaciones, modificaciones y asignaciones de permisos a los usuarios de su *software* y aplicaciones.

25. Es preciso reiterar que la implementación de los mencionados documentos por parte de EGASA tuvo lugar en una fecha anterior a la notificación de cargos en su contra (17 de febrero de 2017), por lo que la adopción de tales documentos implica la subsanación del hecho imputado como infractor a través de la Resolución Directoral N° 272-2016-JUS/DGPDP-DS.

---

[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."

[4] **Texto Único Ordenado de la Ley N° 27444, Ley del Procedimiento Administrativo General, aprobado por Decreto Supremo N° 006-2017-JUS.**
*"**Artículo 255.- 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 253."

27. En el presente caso, se entiende que si bien a la fecha de emisión del Informe Nº 066-2016-JUS/DGPDP-DSC se había configurado la infracción tipificada en el literal a. del numeral 2 del artículo 38 de la LPDP, esta situación fue subsanada con la implementación de los documentos mencionados.

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

28. Por consiguiente, respecto de la presente imputación, debe declararse la inexistencia de responsabilidad por parte de EGASA.

Sobre la presunta infracción al artículo 42 del Reglamento de la LPDP

29. Respecto del tratamiento no automatizado de datos personales, el artículo 42 del Reglamento de la LPDP establece 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."*

30. Siguiendo la pauta del artículo transcrito, EGASA tenía la obligación de ubicar los elementos donde almacena los documentos que contengan datos personales de sus trabajadores en áreas protegidas con puertas con sistemas de apertura mediante llave u otro dispositivo equivalente, y que se encuentren cerradas cuando no se necesite acceder a dichos documentos.

31. En relación a lo mencionado en el considerando 15, se debe indicar que en el Informe Nº 066-2017-JUS/DGPDP-DSC, la DSC se indicó lo siguiente:

> *"20. Se verificó que la documentación que contiene el banco de datos no automatizado de trabajadores de EGASA está almacenada en archivadores tipo palanca ordenada por código de trabajador y ubicados en un estante de madera sin llave, incumpliendo con lo dispuesto en el artículo 42 del Reglamento de la LPDP (...)"*

32. Sin embargo, en el Acta de Fiscalización N° 02-2016, se consignó sobre tal factor lo siguiente:

> *"El banco de datos no automatizado se encuentra ubicada en la Oficina del Departamento de Recursos Humanos, se verificó que en esta oficina únicamente se almacenan los expedientes de los trabajadores (cuenta con 128 registros de personas) los cuales son almacenados en archivadores tipo palanca ordenados por código de trabajador y ubicados en un estante de madera sin llave."*

En tal sentido, la DSC ha evidenciado que EGASA no cumple con almacenar la documentación no automatizada de sus trabajadores en un ambiente cuyo acceso se encuentre restringido con llave o sistema equivalente, incumpliendo la obligación establecida en el artículo 42 del Reglamento de la LPDP.

33. Cabe indicar que el 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 infractor, si se efectúa de forma previa a la notificación de imputación de cargos.

34. En sus descargos, EGASA señaló que implementó armarios con puertas corredizas y llaves de seguridad para almacenar los documentos de sus trabajadores, en un ambiente con puertas que cuentan con llaves de seguridad, adjuntando fotografías de los mencionados armarios.

35. Asimismo, es preciso tener en cuenta lo estipulado en el documento "Política de Acceso a la Información" (del 30 de diciembre de 2016) acerca de la seguridad de los ambientes físicos donde se custodian datos personales, en los siguientes términos:

> ***"1. POLÍTICA GENERAL***
>
> *1.1 La Dirección de EGASA está comprometida con la Seguridad de la Información de la empresa, teniendo en cuenta los lineamientos del estándar NTP ISO/IEC 27001:2014 y por otro lado aprobando Políticas, Procedimientos y Normas que sean necesarios para el buen funcionamiento de la empresa.*
> *(...)*
> *1.6 Todas las área de la empresa, están comprometidas en preservar la seguridad de su información, tanto en lo relacionado a accesos lógicos cómo en el cuidado de sus ambientes físicos donde se conserva información sensible o confidencial para la empresa.*
> *(...)*
>
> ***3. POLÍTICAS DE ACCESO FÍSICO A ÁREAS SEGURAS***
>
> *3.1 El Comité de Seguridad de Información de EGASA en coordinación con las áreas de EGASA, identifican todas las áreas o ambientes donde se realiza el procesamiento o almacenamiento de información sensible o confidencial, así como aquellos ambientes donde se encuentren equipos o cualquier infraestructura que brinde soporte a los Sistemas de Información y Comunicaciones. Estas áreas o ambientes se van a considerar como 'Áreas seguras' o de 'Acceso Restringido'.*
> *(...)*
> *3.2 Las situaciones de acceso a las áreas restringidas, son autorizadas por la respectiva Área responsable del ambiente físico a su cargo.*
> *Las personas que van a acceder o visitar dichos ambientes seguros, deben ingresar, previo registro, acompañados por algún funcionario o responsable de dicha área."*

36. De lo expuesto, se desprende que hubo por parte de EGASA una planificación para implementar las medidas de seguridad en el tratamiento no automatizado de los datos personales de sus trabajadores, toda vez que se determinaron restricciones a los accesos a ambientes donde se custodian información sensible, lo cual es

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

complementado con la adecuación de las cerraduras, como se detalló en el considerando 34.

37. En consecuencia, si bien a la fecha de emisión del Informe Nº 066-2016-JUS/DGPDP-DSC se había configurado la infracción tipificada en el literal a. del numeral 2 del artículo 38 de la LPDP, derivada de la inobservancia del artículo 42 del Reglamento de LPDP, debe aplicarse lo dispuesto en el literal f. del artículo 255 de la LPAG debido a las acciones de subsanación demostradas por EGASA, debiendo declararse la inexistencia de responsabilidad de su parte.

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;

SE RESUELVE:

Artículo 1.- Archivar el procedimiento sancionador seguido contra EMPRESA DE GENERACIÓN ELÉCTRICA AREQUIPA S.A.

Artículo 2.- Notificar a EMPRESA DE GENERACIÓN ELÉCTRICA AREQUIPA S.A. la presente resolución.

Regístrese y comuníquese.

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