Consejo Ejecutivo del Poder Judicial

RESOLUCIÓN ADMINISTRATIVA Nº 065-2016-CE-PJ

Lima, 16 de marzo de 2016

VISTO:

El Oficio N° 290-2016-GG, cursado por el Gerente General del Poder Judicial, remitiendo propuesta de "Directiva sobre Tratamiento y Protección de Datos Personales en el Poder Judicial".

CONSIDERANDO:

Primero. Que mediante Ley N° 29733, Ley de Protección de Datos Personales, se garantiza el derecho fundamental a la protección de los datos personales contenidos o destinados a ser contenidos en bancos de datos personales de administración pública o privada.

Segundo. Que el Decreto Supremo N° 003-2013-JUS, aprueba el Reglamento de la Ley N° 29733, Ley de Protección de Datos Personales, que describe las disposiciones a cumplir al implementar dicha Ley en las instituciones tanto públicas como privadas.

Tercero. Que, en dicho contexto, la Resolución Directoral N° 019-2013-JUS/DGPDP aprobó la "Directiva de Seguridad de la Información Administrativa por los Bancos de Datos Personales", la cual contiene información técnica necesaria para formular los documentos claves para la Protección de Datos Personales en el Poder Judicial.

Cuarto. Que, con la finalidad de dar cumplimiento a la normativa antes citada, mediante Resolución Administrativa N° 426-2015-P-PJ la Presidencia del Poder Judicial, aprobó la conformación de la "Comisión de Gestión de Datos Personales en el Poder Judicial", que impulsará la inscripción del Banco de Datos en Registro Nacional de Protección de Datos Personales.

Quinto. Que, en ese sentido, es necesario aprobar la "Directiva sobre Tratamiento y Protección de Datos Personales en el Poder Judicial", para asegurar la adecuada gestión de la información personal en los procesos internos del Poder Judicial y dar cumplimiento a la Ley N° 29733, Ley de Protección de Datos Personales.

Sexto. Que el artículo 82°, inciso 26), del Texto Único Ordenado de la Ley Orgánica del Poder Judicial, determina como función y atribución del Consejo Ejecutivo del Poder Judicial, la adopción de acuerdos y demás medidas necesarias para que las

dependencias de este Poder del Estado funcionen con celeridad y eficiencia; por lo que corresponde aprobar la propuesta remitida por la Gerencia General del Poder judicial.

Por estos fundamentos; en mérito al Acuerdo N° 211-2016 de la décima sesión del Consejo Ejecutivo del Poder Judicial de la fecha, adoptado con la intervención de los señores Ticona Postigo, De Valdivia Cano, Lecaros Cornejo, Ruidías Farfán, Vera Meléndez y Álvarez Díaz; en uso de las atribuciones conferidas por el artículo 82° del Texto Único Ordenado de la Ley Orgánica del Poder Judicial. Por unanimidad,

SE RESUELVE:

Artículo Primero.- Aprobar la Directiva N° 002-2016-CE-PJ, denominada "Directiva sobre el Tratamiento y Protección de Datos Personales en el Poder Judicial", que en documento anexo forma parte de la presente resolución.

Artículo Segundo. Dejar sin efecto las resoluciones administrativas que se opongan a la presente.

Artículo Tercero.- Encargar a la Gerencia de Informática de la Gerencia General del Poder Judicial, la difusión y cumplimiento de la presente Directiva.

Artículo Cuarto.- Disponer la publicación en el Portal Institucional del Poder Judicial la presente resolución administrativa y el documento aprobado, para su debido cumplimiento.

Artículo Quinto.- Transcribir la presente resolución a la Presidencia del Poder Judicial, Oficina de Control de la Magistratura, Cortes Superiores de Justicia de la República; y a la Gerencia General del Poder Judicial, para su conocimiento y fines pertinentes.

Regístrese, publíquese, comuníquese y cúmplase.

S.

CONSEJO EJECUTIVO DEL PODER JUDICIAL

VÍCTOR TICONA POSTIGO
Presidente

LAMC/mlrj

PODER JUDICIAL DEL PERÚ

CONSEJO EJECUTIVO

DIRECTIVA N° 002-2016-CE-PJ

"Directiva sobre el Tratamiento y Protección de Datos Personales en el Poder Judicial"

R.A. N° 065-2016-CE-PJ

MARZO 2016

LIMA – PERU

DIRECTIVA N° 002-2016-CE-PJ

DIRECTIVA SOBRE EL TRATAMIENTO Y PROTECCIÓN DE DATOS PERSONALES EN EL PODER JUDICIAL

I. OBJETIVO

Garantizar el derecho fundamental a la protección de los datos personales contenidos o destinados a ser contenidos en bancos de datos personales del Poder Judicial, a través de su adecuado tratamiento en el marco de respeto a los demás derechos fundamentales previstos en el artículo 2° de la Constitución, mediante medidas de seguridad que protejan a los bancos de datos personales, de conformidad con la Ley N° 29733 y su reglamento.

II. FINALIDAD

Brindar seguridad a las Personas Naturales, respecto al adecuado tratamiento de datos personales, tanto en el ámbito administrativo como el jurisdiccional del Poder Judicial.

III. ALCANCE

La presente Directiva es de aplicación y cumplimiento obligatorio por todas las dependencias administrativas del Poder Judicial, a nivel nacional; y las dependencias jurisdiccionales, que posean bancos de datos personales, independientemente del soporte en el que se encuentren.

IV. BASE LEGAL

4.1 Constitución Política del Perú.

4.2 Texto Único Ordenado de la Ley Orgánica del Poder Judicial.

4.3 Ley N° 29733, Ley de Protección de Datos Personales.

4.4 Decreto Supremo 003-2013-JUS, aprueba el Reglamento de la Ley N° 29733, Ley de Protección de Datos Personales.

4.5 Decreto Supremo 011-2012-JUS, aprueba el Reglamento de Organización y Funciones del Ministerio de Justicia y Derechos Humanos.

4.6 Resolución Ministerial Nº 246-2007-PCM, aprueba la Norma Técnica Peruana "NTP ISO/IEC 17799:2007 EDI, Técnicas de seguridad, Código de Buenas Prácticas para la gestión de seguridad de la información. 2a Edición".

4.7 Resolución de la Comisión de Normalización y de Fiscalización de Barreras Comerciales No Arancelarias 129-2014/CNB-INDECOPI que aprueba la Norma Técnica Peruana 27001:2014, Tecnología de la Información. Técnicas de Seguridad. Sistemas de Gestión de Seguridad de la Información 2° Edición. (Remplaza a la NTP-ISO/IEC 27001:2008 - Revisada el 2013).

4.8 Resolución Administrativa N° 318-2013-P-PJ, que aprueba el Manual para la Formulación de Documentos Normativos de Gestión del Poder Judicial.

V. VIGENCIA

5.1 A partir del día siguiente de la fecha de publicación de la Resolución Administrativa mediante la cual se aprueba la siguiente Directiva.

VI. DISPOSICIONES GENERALES

6.1 El Poder Judicial es responsable de la protección de datos personales bajo su custodio. En tal sentido, se define como datos personales a toda información sobre una persona que la identifique o la hace inidentificable a través de medios que pueden ser razonablemente utilizada. Cuyo tratamiento es todo procedimiento, 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.

6.2 El Titular del Banco de Datos Personales, es quien determina la finalidad y contenido del Banco de Datos Personales, el tratamiento de éstos y las medidas de seguridad a implementar.

6.3 El Encargado del Banco de Datos Personales es quien solo o actuando conjuntamente con otro, realiza el tratamiento de los datos personales por encargo del Titular del Banco de Datos Personales.

6.4 Se asigna los lineamientos a cumplir por el Titular del Banco de Datos Personales en cuanto a medidas organizativas, legales, técnicas, en el tratamiento de datos personales.

6.5 Se asigna lineamientos a cumplir por el Titular del Banco de Datos Personal loses para determinar las medidas de seguridad que resulten apropiadas, en función a las características de cada caso concreto, a partir de considerar criterios de diferenciación basados en las características del tratamiento de datos personales que se vaya a efectuar y en las características de datos personales que se tratan.

6.6 La clasificación de la Información se da en cinco (5) categorías teniendo en consideración lo siguiente: el Volumen de registros, Número de datos, período durante el cual se realiza el tratamiento, finalidad del tratamiento de los datos personales, múltiples localizaciones, tratamientos de datos sensibles.

a. **Básico**, corresponde a la categoría de menor nivel e incluye a bancos de datos personales que:
   - Contengan la información de hasta (50) personas.
   - Número de datos personales no mayor a cinco (05). Por ejemplo: nombres, apellidos, DNI, dirección, teléfono.
   - No incluyen datos sensibles.
   - Tienen como titular a una persona natural.

b. **Simple**, corresponde a bancos de datos personales que:
   - Contengan la información de hasta (100) personas.
   - El periodo de tiempo del tratamiento para cumplir con la finalidad es inferior a un (01) año.
   - No incluyen datos sensibles.
   - Tiene como titular a una persona natural o jurídica.

c. **Intermedio**, corresponde a bancos de datos personales que:
   - Contienen la información de hasta mil (1000) personas.

- Sirven para tratamiento de datos personales cuya finalidad se cumple en un plazo indeterminado o superior a un (01) año.
- Puede incluir datos sensibles.
- Tiene como titular a una persona natural o jurídica.

d. **Complejo**, corresponde a bancos de datos personales que:
- Sirven para el tratamiento de datos personales cuya finalidad se cumple en un plazo indeterminado o superior a un (01) año.
- Sirven para el tratamiento de datos personales que es realizado en múltiples localizaciones
- (Oficinas o dependencias diferentes en la misma ciudad o ciudades diferentes, servicios tercerizados o similares).
- Puede incluir datos sensibles.
- Tiene como titular a una persona jurídica o entidad pública.
- No incluyen datos sensibles.
- Tiene como titular a una persona natural o jurídica.

e. **Crítico**, corresponde la categoría de mayor nivel e incluye a bancos de datos personales que:
- Sirven para el tratamiento de datos personales cuya finalidad está respaldada por una norma legal.
- Sirven para el tratamiento de datos cuya finalidad se cumple en un plazo indeterminado o superior a un (01) año.
- Sirven para el tratamiento de datos personales que es realizado en múltiples localizaciones (Oficinas o dependencias diferentes en la misma ciudad o ciudades diferentes, servicios tercerizados o similares).
- Puede incluir datos sensibles.
- Tiene como titular a una persona jurídica o entidad pública.

6.7 Los Bancos de Datos Personales del Poder Judicial deberán ser inscritos en el Registro Nacional de Protección de Datos Personales – RNPDP, el cual esta a cargo de la Autoridad Nacional de Protección de Datos Personales del Ministerio de Justicia, para lo cual se debe identificar al encargado del tratamiento de dicha información.

6.8 La inscripción de un Banco de Datos Personales en el Registro Nacional de Protección de Datos Personales, tiene por finalidad que los ciudadanos puedan conocer a los titulares de dichos bancos de datos y ejercer los derechos de acceso a la información, rectificación, cancelación, oposición y otros regulados en la Ley y su Reglamento. Para lo cual el Titular del Banco de Datos Personales deberá completar un formulario por cada Banco de Datos Personales que pretenda inscribir.

MATRIZ DE APOYO PARA LA SELECCIÓN DE CATEGORÍA EN EL TRATAMIENTO DE DATOS PERSONALES

ITEM	CRITERIO	BÁSICO	SIMPLE	INTERMEDIO	COMPLEJO	CRÍTICO
1	Volumen de registros, número de titulares de datos personales que consienten el tratamiento de sus datos. (Criterio utilizado para determinar las categorías).	Hasta 50	Hasta 100	Hasta 1000	Indeterminado	Indeterminado
2	Número de datos personales en banco de datos personales que no contienen datos sensibles. (Criterio utilizado para determinar el tipo básico).	Hasta 5	Más de 5	Más de 5	Más de 5	Más de 5
3	Finalidad del tratamiento de datos personales respaldada por ley o similar. (Criterio utilizado para determinar el tipo crítico).	No aplica	No aplica	No aplica	No aplica	Aplica
4	Periodo mayor a un (01) año o indeterminado para cumplir la finalidad (tiempo de tratamiento de los datos personales).	No aplica	No aplica	Aplica	Aplica	Aplica

ITEM	CRITERIO	BÁSICO	SIMPLE	INTERMEDIO	COMPLEJO	CRÍTICO
5	Tipo de Titular del Banco de Datos Personales: persona natural. (Criterio utilizado para determinar el tipo entre básico a intermedio).	Aplica	Aplica	Aplica	No aplica	No aplica
6	Tipo de Titular del Banco de Datos Personales: persona jurídica. (Criterio utilizado para determinar la categoría entre simple a complejo).	No aplica	Aplica	Aplica	Aplica	Aplica
7	Titular del Banco de Datos Personales del tipo persona jurídica o entidad pública con múltiples localizaciones desde las cuales se tiene acceso al banco de datos personales o se realiza tratamiento de los datos personales. (Criterio utilizado para determinar la categoría complejo o crítico).	No aplica	No aplica	No aplica	Aplica	Aplica
8	El banco de datos personales puede incluir datos sensibles. (Criterio utilizado para determinar la categoría entre Intermedio a crítico).	No aplica	No aplica	Aplica	Aplica	Aplica

6.3. Condiciones de Seguridad

6.3.1. Condiciones de Seguridad Externa

a. Marco legal apropiado (leyes, reglamentos, o similares).

b. Conocimiento y conciencia (conocer la importancia de la protección de los datos personales, la Ley N° 29733, Ley de Protección de Datos Personales, y su reglamento).

6.3.2. Condiciones de Seguridad Interna

a. El Titular del Banco de Datos Personales debe estar comprometido con la implementación y operación de la protección de datos personales (para brindar los recursos y dirección en la protección de los datos personales).
b. Determinar claramente las responsabilidades y roles organizacionales apropiados con la suficiente autoridad y recursos para liderar y hacer cumplir la política de seguridad para la protección de datos personales.
c. Enfoque de gestión del riesgo de los datos personales contenidos o destinados a ser contenidos en los bancos de datos personales.

6.4. Requisitos de Seguridad

Todos los Bancos de Datos Personales deben cumplir requisitos de seguridad que varían dependiendo de la categoría de tratamiento de datos que realiza el Titular del Banco de Datos Personales (básico, simple, intermedio, complejo o crítico).

El tal sentido, las categorías de tratamiento deben cumplir (en mayor o menor medida) los siguientes requisitos:

a. Contar con una política de protección de datos personales,
b. Mantener la gobernabilidad completa de los procesos involucrados en el tratamiento de los datos personales, cuando estos sean tercerizados o no.
c. Implementar medidas de seguridad según lo indicado en el numeral 7.1.
d. Mantener procedimientos documentados (procedimientos de seguridad de la información determinados por el SGSI según la ISO/IEC 27001 en su edición vigente).
e. Adoptar un enfoque de riesgos y el plan de tratamiento de riesgos del Banco de Datos Personales que se desprende del mismo, servirá como base para la implementación de controles.

f. Alinear los controles indicados en la NTP-ISO/IEC 27001 o ISO/IEC 27001 en su edición vigente, en caso las categorías de tratamiento sea complejo o crítico.
g. Desarrollar y mantener una lista maestra de registro de los bancos de datos personales de la institución.
h. Desarrollar y mantener actualizado un documento o cláusulas de compromiso de confidencialidad de seguridad en el tratamiento de datos personales.

6.5. Información Complementaria sobre Requisitos de Seguridad

La política de protección de datos que debe mantener el Titular del Banco de Datos Personales es una declaración formal de compromiso y debe considerar:

a. Ser clara y comprensible,
b. Apropiada para los objetivos del Poder Judicial.
c. Constituye un lineamiento de alto nivel organizacional,
d. Debe incluir un compromiso de cumplimiento de los requisitos de seguridad aplicables,
e. Incluir un compromiso de respeto.
f. Comunicarse oportuna y claramente al interior de la organización.

Asimismo, en materia de requisitos de seguridad, las categorías de tratamiento de datos personales, según corresponda, deben implementar los siguientes procedimientos documentados:

a. Control de documentos y registros,
b. Registro de accesos,
c. Registros de personal con acceso autorizado,
d. Registro de incidentes y medidas adoptadas.
e. Registro de auditorías.

VII. DISPOSICIONES ESPECÍFICAS

Se regula disposiciones específicas para las categorías de tratamientos de datos personales *complejos o críticos*, como por ejemplo implementar controles de seguridad de la información según la NTP-ISO/IEC 27001-EDI en su versión vigente. Asimismo, las categorías de tratamientos *intermedios, complejos y críticos* deben designar un responsable de seguridad del Banco de Datos Personales, quien coordinará en la institución la aplicación de la presente Directiva.

Por otro lado, en todas las categorías de tratamiento, los bancos de datos personales deben contener la información estrictamente necesaria para cumplir la finalidad de su recopilación y se debe evaluar la posibilidad de implementar mecanismos de anonimización o separación.

7.1. Medidas de Seguridad

Se implementa (en mayor o menor intensidad) medidas de seguridad organizativa, jurídica y técnicas, en el tratamiento de datos según las distintas categorías.

7.1.1. Medidas de Seguridad Organizativas

- Se debe desarrollar una estructura organizacional con roles y responsabilidades en la institución.
- Compromiso documentado de respeto a la Ley.
- Se debe supervisar y registrar al personal que tenga acceso al banco de datos (trazabilidad).
- La efectividad de las medidas de seguridad adoptadas en la institución deben ser supervisadas periódicamente.
- Los sistemas de gestión de la institución deben ser adecuados para el tratamiento de datos personales.
- Los procesos del negocio del Poder Judicial deben ser adecuados en relación a la protección de datos personales.
- Realizar procedimientos documentados para el tratamiento de datos personales.

- Realizar programas de capacitación orientados a la concientización y entrenamiento en materia de datos personales.
- Elaborar un procedimiento de auditoría en materia de datos personales al menos una vez al año.
- Elaborar un procedimiento de asignación de privilegios de acceso al Banco de Datos Personales

7.1.2. Medidas de Seguridad Jurídicas

- Elaborar y mantener un formato de consentimiento adecuado para el tratamiento de datos personales.
- Adecuación de contratos a la Ley.
- Adecuación de contratos de terceros a la Ley.

7.1.3. Medidas de Seguridad Técnicas

a. Acceso no autorizado

- Gestión y uso de contraseñas para el tratamiento a través de medios informáticos.
- Revisión y registro de privilegios de acceso.
- Protección contra acceso físico no autorizado al banco de datos personales.
- Controlar e identificar las autorizaciones de acceso físico a los bancos de datos personales.

b. Alteración no autorizada del banco de datos personales

- Gestionar autorizaciones para el retiro o traslado de datos personales.
- Adoptar medidas para el traslado de datos personales.
- Adoptar medidas para eliminar la información contenida en medios informáticos removibles.
- Adoptar medidas de seguridad en materia de copias y/o reproducción de documentos.
- Controlar la asignación de privilegios para el tratamiento de datos a usuarios no autorizados.

c. Pérdida del Banco de Datos Personales

- Realizar copias de respaldo de los datos personales para permitir su recuperación en caso de pérdida o destrucción.
- La recuperación de datos personales (desde su copia de respaldo) debe contar con la autorización del encargado del banco de datos personales.
- Se deben realizar pruebas de recuperación de los datos personales respaldados para comprobar su buen funcionamiento.

d. Tratamiento no autorizado del Banco de Datos Personales.

- El banco de datos personales no automatizado debe mantener los datos personales independizados de forma particular, de modo que pueda referirse unívocamente a un Titular de Datos Personales sin exponer información de otro.
- El Titular del Banco de Datos Personales debe informar al Titular de los Datos Personales los incidentes que afecten significativamente sus derechos patrimoniales o morales, tan pronto se confirme el hecho.
- Las computadoras utilizadas para el tratamiento de datos personales deben recibir el mantenimiento que corresponda de acuerdo a las especificaciones del proveedor.
- Las computadoras deben contar con protección contra software malicioso para proteger los datos personales.
- La información electrónica que contiene datos personales debe ser almacenada en forma segura.
- La información de datos personales que se transmite electrónicamente debe ser protegida para preservar su confidencialidad e integridad.
- Adoptar medidas de seguridad en el flujo transfronterizo de datos personales.

- Adoptar medidas de seguridad en servicios de tratamiento de datos personales por medios tecnológicos tercerizados.
- Todo evento identificado que afecte la confidencialidad, integridad y disponibilidad de los datos personales o que indique un posible incumplimiento de las medidas de seguridad establecidas, debe ser reportado inmediatamente al encargado del banco de datos personales.
- Restringir el uso de equipos de fotografía, vídeo, audio u otra forma de registro en el área de tratamiento de datos personales salvo autorización del Titular del Banco de Datos Personales.
- Se debe realizar una auditoría sobre el cumplimiento de la presente directiva, bajo responsabilidad del Titular del Banco de Datos Personales.
- Acciones correctivas y de mejora continua

Se debe considerar el desarrollo de actividades orientadas a la información del personal del Poder Judicial (Titulares de los Datos Personales) en temas de: *"consentimiento", "derechos del titular de los datos personales" y "finalidad".*

Asimismo, los encargados del tratamiento deben asegurar y mantener los mecanismos de auditoría, verificación y toma de decisiones del Titular del Banco de Datos Personales.

VIII. ANEXO

Anexo N° 01.- Formulario de Inscripción de Banco de Datos Personales de la Administración Pública. (F-1).

FORMULARIO DE INSCRIPCIÓN DE BANCO DE DATOS PERSONALES DE ADMINISTRACIÓN PÚBLICA

Dirigido a la Dirección de Registro Nacional de Protección de Datos Personales

I.- REGISTRO DEL TITULAR DEL BANCO DE DATOS PERSONALES

1. Datos de la entidad

Denominación de la institución :

Número de RUC:

Nombre del órgano responsable:

*Adjuntar el documento que acredite la designación del funcionario a cargo de la inscripción del banco de datos personales

2. Marque el tipo de entidad

- Poder Ejecutivo:
  - Presidencia ☐ Consejo de Ministros ☐ Ministerio ☐
- Poder Legislativo ☐
- Poder Judicial:
  - Corte Suprema ☐
  - Corte Superior ☐
  - Otro detallar: ☐
- Organismo autónomo ☐
- Organismo público descentralizado ☐
- Gobierno regional ☐
- Gobierno local ☐

3. Dirección a efectos de la notificación

Calle: Nº Of./ Dpto

Distrito:

Provincia: Región:

Referencia:

Dirección de correo electrónico 1:

Dirección de correo electrónico 2:

4. Ejercicio de los derechos de acceso, rectificación, cancelación y oposición

Señalar el servicio o unidad donde podrán dirigirse los ciudadanos para ejercer los derechos de acceso, rectificación, cancelación y oposición de sus datos personales:

Nombre de la oficina o dependencia:

Calle: N° Of. / Dpto

Distrito: Región:

Provincia: Teléfono:

Referencia:

Dirección de correo electrónico:

II.- REGISTRO DEL BANCO DE DATOS PERSONALES

1. Identificación y finalidad del banco de datos personales

Nombre:

Sistema de Tratamiento:

Automatizado ☐ No automatizado ☐ Automatizado y No automatizado ☐

Fecha de creación del banco de datos de personales: Ingrese fecha dd/mm/aaaa

Detalle la finalidad:

Usos previstos (Marque en el recuadro o recuadros correspondientes)

- ☐ Recursos humanos
- ☐ Prevención de riesgos laborales
- ☐ Administración Tributaria
- ☐ Gestión económica – financiera pública
- ☐ Gestión contable fiscal y administrativa
- ☐ Justicia
- ☐ Fines estadísticos, históricos o científicos
- ☐ Padrón de habitantes
- ☐ Programas sociales
- ☐ Regulación de la inversión privada en los servicios públicos
- ☐ Seguridad y control de acceso a edificios
- ☐ Gestión de listas de miembros de partidos políticos
- ☐ Gestión de listas de miembros de sindicatos.
- ☐ Actividades asociativas, recreativas y deportivas
- ☐ Actividades profesionales
- ☐ Educación y cultura
- ☐ Investigación en temas de salud
- ☐ Historias clínicas
- ☐ Gestión y control sanitario
- ☐ Video vigilancia

☐ Otro tipo de finalidad Detallar:

2. Tipos de datos personales sometidos a tratamiento

Marque en el recuadro o recuadros correspondientes:

Datos de carácter identificativo:

- ☐ Nombres y apellidos
- ☐ N° DNI
- ☐ N° RUC
- ☐ N° Pasaporte
- ☐ Dirección del domicilio
- ☐ Teléfono
- ☐ Voz
- ☐ Dirección de correo electrónico
- ☐ Imagen
- ☐ Firma
- ☐ Firma electrónica
- ☐ Otros Detallar:

Datos de características personales:

- ☐ Estado civil
- ☐ Fecha de nacimiento
- ☐ Nacionalidad
- ☐ Sexo
- ☐ Profesión
- ☐ Edad
- ☐ Otros Detallar:

Datos económicos- financieros y de seguros:

- ☐ Créditos, préstamos, avales
- ☐ Datos bancarios
- ☐ Historial de créditos
- ☐ Información tributaria
- ☐ Seguros
- ☐ Hipotecas
- ☐ Deudas
- ☐ Tarjetas de crédito
- ☐ Bienes patrimoniales
- ☐ Planes de pensiones/ jubilación
- ☐ Beneficios recibidos de programas sociales
- ☐ Otros Detallar:

Datos de carácter social:

- ☐ Pertenencia a clubes o asociaciones
- ☐ Aficiones y hábitos personales
- ☐ Características de vivienda
- ☐ Otros Detallar:

Datos sensibles:

- ☐ Origen étnico
- ☐ Características físicas
- ☐ Información relativa a la salud física o mental
- ☐ Vida sexual
- ☐ Vida afectiva o familiar
- ☐ Convicciones religiosas
- ☐ Convicciones políticas

☐ Convicciones filosóficas o morales ☐ Huella
☐ Ingresos económicos ☐ Afiliación sindical
☐ Otros datos de carácter biométrico Detallar:

3. Origen y procedimiento de obtención de los datos personales

Señale el origen de los datos personales:

☐ El titular del dato personal o su representante legal
☐ Fuentes de acceso al público
☐ Entidad privada
☐ Entidad pública
☐ Otros detallar:

Señale el soporte utilizado para la obtención:

☐ Papel
☐ Soporte informático/ magnético
☐ Vía telemática
☐ Otros detallar:

Señale el procedimiento de obtención de los datos personales:

☐ Formularios
☐ Transmisión electrónica
☐ Encuestas
☐ Telemarketing
☐ Entrevistas personales
☐ Referencias comerciales
☐ Otros detallar:

4. Ubicación física del banco de datos personales

Calle: Nº: Of. / Dpto

Distrito: Región:

Provincia: País

Referencia:

Teléfono:

Persona de contacto:

¿La ubicación corresponde a un tercero? Sí ☐ No ☐

¿Existen ubicaciones alternativas o secundarias? Sí ☐ No ☐

En caso de que la respuesta sea afirmativa, detallar:

Calle/ Nº / Of. / Dpto.	Distrito	Provincia	Región

III.- TRANSFERENCIAS DE DATOS PERSONALES

La entrega de datos personales por parte del titular del banco de datos personales al encargado no se considera transferencia de datos personales.

1. Transferencia de datos personales a nivel nacional

¿Realiza comunicaciones de datos personales a nivel nacional? Sí ☐ No ☐

En caso que la respuesta sea afirmativa indique si la comunicación es:

- Onerosa ☐
- Gratuita ☐

Marque las categorías de receptores:

- ☐ Organizaciones o personas directamente relacionadas
- ☐ Entidades aseguradoras
- ☐ Entidades Prestadoras de Salud (EPS)
- ☐ Centros de salud (clínicas, hospitales y postas médicas)
- ☐ Asociaciones Administradoras de Fondo de Pensiones (AFP)
- ☐ Oficina de Normalización Previsional (ONP)
- ☐ Entidades financieras
- ☐ Centrales de riesgo
- ☐ Entidades religiosas
- ☐ Colegios profesionales
- ☐ Administración tributaria
- ☐ Programas sociales
- ☐ Instituciones educativas
- ☐ Organizaciones no gubernamentales (ONG)
- ☐ Sindicatos
- ☐ Partidos políticos
- ☐ Registros Públicos
- ☐ Organismos reguladores de la inversión privada en los servicios públicos
- ☐ Seguro social
- ☐ Fuerzas Armadas y Policía Nacional
- ☐ Órganos judiciales
- ☐ Organismos autónomos
- ☐ Ministerios
- ☐ Instituto Nacional de Estadística e Informática (INEI)
- ☐ Gobiernos regionales
- ☐ Gobiernos locales

☐ Otras entidades públicas detallar:

☐ Otros detallar:

2. Transferencia de datos personales a nivel internacional (flujo transfronterizo)

¿Realiza comunicaciones de datos personales a nivel internacional? Sí ☐ No ☐

En caso que la respuesta sea afirmativa indique si la comunicación es:

- Onerosa ☐
- Gratuita ☐

Indique los países y las categorías de receptores:

Países destinatarios	Categoría de receptores (Ver categorías de receptores del numeral 1 del punto III)

En caso de que el país destinatario no cuente con un nivel de protección adecuado, el emisor del flujo transfronterizo de datos personales asume la responsabilidad de garantizar que el tratamiento de los datos personales se realice conforme a lo dispuesto en la Ley N° 29733 y su reglamento.

IV.- MEDIDAS DE SEGURIDAD

¿Dispone de un documento de seguridad?

Sí ☐ No ☐

¿Tiene documentado los procedimientos relacionados con el acceso y el tratamiento de la información?

Sí ☐ No ☐

¿Existe un responsable de seguridad?

Sí ☐ No ☐

¿Realiza un control periódico del cumplimiento de las políticas de seguridad?

Sí ☐ No ☐

En caso la respuesta sea afirmativa, indicar cada cuánto tiempo se realiza el control:

En virtud de lo señalado, SOLICITO la inscripción del banco de datos personales a la Dirección de Registro Nacional de Protección de Datos Personales al amparo de lo establecido en el artículo 34 de la Ley N° 29733- Ley de Protección de Datos Personales- y de los artículos 76, 77, 78, 79 y 81 del Reglamento de la Ley de Protección de Datos Personales, aprobado por Decreto Supremo N° 003-2013-JUS.

Adjunto en un CD el archivo del formulario llenado en PDF, previamente descargado desde el Portal Institucional del Ministerio de Justicia y de Derechos Humanos.

Declaro que los datos que anteceden son ciertos, siendo responsable quien los proporciona de su corrección y calidad.

Fecha: Ingrese fecha dd/mm/aaaa

Firma: _____

Nombre:
DNI: