



PROCEDIMIENTO

Protección de datos personales

Código: LE-MN-001

Versión: 01

Fecha: 28/08/2023

Elaborado por:	Asistente Legal
Revisado por:	Gerente Legal
Aprobado por:	Gerente General



Código:	LE-MN-001	MANUAL	
Versión	01		
Fecha:	28/08/2023	PROTECCIÓN DE DATOS PERSONALES	
Página:	2 de 42		

TABLA DE CONTENIDO

1.OBJETIVO	3
2. ALCANCE	3
2.1 ÁMBITO DE APLICACIÓN	3
3. RESPONSABILIDADES.....	3
3.1 ORGANIGRAMA.....	3
3.2. DESCRIPCIÓN DE RESPONSABILIDADES	4
4 DEFINICIONES	6
5 DOCUMENTOS DE REFERENCIA	9
6 ACTIVIDADES	9
6.1 Principios de Protección de Datos Personales	9
6.2 Derechos de los Titulares de Datos Personales	11
6.3 Comunicación de los Datos Personales.....	12
6.4 Gestión de las Bancos de Datos.....	14
6.5 Medidas de Seguridad	15
6.6 Del personal de P.A. PERU S.A.C.....	16
6.7 Disposiciones adicionales	18
6.8 Condiciones internas y externas de la seguridad.....	18
6.9 Requisitos de seguridad	19
6.10 Disposiciones específicas de seguridad	22
6.11 Medidas de seguridad organizativas.....	22
6.12 Medidas de seguridad jurídicas	26
6.13 Medidas de seguridad técnicas	27
6.14 Medios validos de obtención del consentimiento	36
6.15 Confidencialidad de datos personales	37
6.16 Limitaciones al consentimiento para el tratamiento de datos personales.....	37
6.17 Tratamiento de datos personales	38
7. RECURSOS UTILIZADOS	38
8. REGISTROS	38
9. ANEXOS	38
10. CONTROL DE CAMBIOS	42

Código:	LE-MN-001	MANUAL	
Versión	01		
Fecha:	28/08/2023	PROTECCIÓN DE DATOS PERSONALES	
Página:	3 de 42		

1. OBJETIVO

El presente documento garantiza la protección de los datos contenidos o destinados a ser contenidos en los bancos de datos personales de P.A. PERU S.A.C. respecto a los clientes, potenciales clientes, usuarios de la página web y redes sociales, libro de reclamaciones, trabajadores, practicantes, postulantes, proveedores, visitantes, video vigilancia y demás sujetos interesados que participen en sus actividades de negocio, estableciendo la organización de la protección de los datos personales en P.A. PERU S.A.C. y las responsabilidades de todos sus actores en la cual se traten con datos personales. Asimismo, definiendo los mecanismos para obtener el consentimiento por parte del Titular de Datos Personales para el tratamiento adecuado de éstos.

2. ALCANCE

El presente documento se emite en cumplimiento de las disposiciones legales vigentes, con el objeto de gestionar adecuadamente la protección de datos personales; su aplicación alcanza a todo el personal, así como a terceros que, previo acuerdo de confidencialidad, tengan acceso a la información de P.A. PERU S.A.C. para el cumplimiento del servicio contratado.

2.1 ÁMBITO DE APLICACIÓN

El presente Manual de P.A. PERU S.A.C. que será de aplicación tanto para los datos personales de las personas naturales indicadas en la Ley, sea que estén registrados en soportes físicos o digitales, tanto para los susceptibles de tratamiento inmediato o para cualquier modalidad de uso posterior de los mismos.

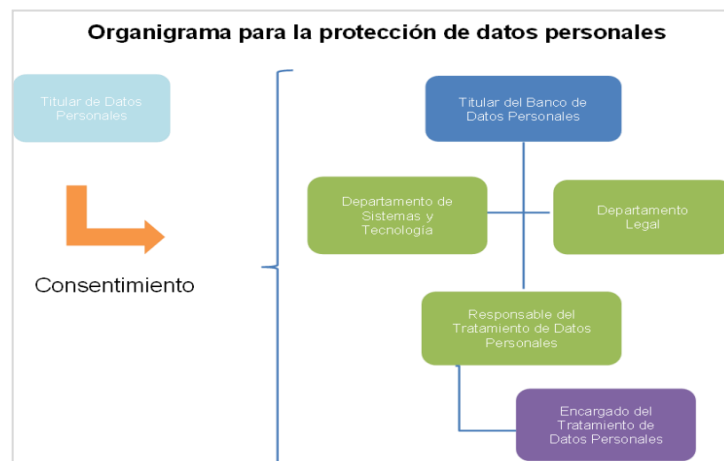
La adopción del presente Manual implica la inscripción de los nuevos bancos de datos identificados ante la Dirección de Protección de Datos Personales del Ministerio de Justicia y Derechos Humanos.


Este Manual aplica a todas las tiendas, oficinas, instalaciones y trabajadores de P.A. PERU S.A.C. Sin perjuicio de lo indicado, su aplicación podrá ser ampliado al grupo económico del cual forma parte P.A. PERU S.A.C., de considerarlo conveniente.

3. RESPONSABILIDADES

3.1 ORGANIGRAMA

P.A. PERU S.A.C. ha implementado una estructura organizacional de protección de datos personales sobre la base de las unidades organizativas existentes y los roles que son descritos en la Ley y su reglamento:



Código:	LE-MN-001	MANUAL	
Versión	01		
Fecha:	28/08/2023	PROTECCIÓN DE DATOS PERSONALES	
Página:	4 de 42		

3.2. DESCRIPCIÓN DE RESPONSABILIDADES

3.2.1 Titular del Banco de Datos Personales

La titularidad de los bancos de datos personales es asumida por P.A. PERU S.A.C. como persona jurídica de derecho privado, representado por el Gerente General y asume las responsabilidades de garantizar el cumplimiento de la Ley 29733, Ley de Protección de Datos Personales en la empresa a través de su liderazgo y apoyo mediante los recursos que sean necesarios.

El Gerente General como representante del titular del Banco de Datos Personales de P.A. PERU S.A.C. asignará las siguientes responsabilidades al Gerente Legal:

Quien actuará dentro del marco de la Ley y de las responsabilidades otorgadas, no deberá eximir al Gerente General de situaciones que deba participar o tomarse una decisión respecto al Banco de Datos Personales de P.A. PERU S.A.C.

El Gerente Legal, informará mensualmente de los acontecimientos ocurrido referente al Banco de Datos Personales de P.A. PERU S.A.C.

El Gerente Legal tendrá el soporte del Departamento de Tecnología y Departamento Legal cuando sea requerido sobre el Banco de Datos Personales.

3.2.2 Departamento de Tecnología

3.2.2.1 Seguridad de la Información: Tiene la responsabilidad de velar y monitorear el cumplimiento de las medidas de seguridad a nivel organizativo, jurídico y técnico en toda la organización.

3.2.2.2 Gerente de TI: Es responsable de dar proveer y gestionar todas las facilidades técnicas para la implementación de las medidas de seguridad técnicas que ayuden a mantener la privacidad de los datos personales.


3.2.3 Departamento Legal

Dar soporte en la implementación de las medidas jurídicas, realizar todos los trámites administrativos ante la Autoridad Nacional de Protección de Datos Personales (inscripción de bancos de datos, modificación, cancelación) y dar mantenimiento a las cláusulas contractuales y formularios de consentimiento referidos al cumplimiento de la Ley 29733, Ley de Protección de Datos Personales.

3.2.4 Responsable del Tratamiento de Datos Personales

Está representado por todos los responsables del más alto nivel de cada uno de los procesos de P.A. PERU S.A.C., en los que se realice el tratamiento de Banco de Datos Personales y sus responsabilidades son:

- a. Tomar decisiones acerca del tratamiento del banco de datos personales.
- b. Determinar el contenido de los bancos de datos personales.
- c. Determinar la finalidad del tratamiento de los bancos de datos personales.
- d. Determinar el tratamiento y el tiempo de tratamiento de los bancos de datos personales de los cuales es titular.
- e. Asegurar la aplicación de la finalidad de tratamiento del banco de datos personales definida por la organización.
- f. Gestionar operativamente el consentimiento por parte de los titulares de datos personales para el tratamiento en coordinación con el Departamento Legal y de Tecnología.
- g. Comunicar a las terceras partes, cuando fuera el caso, las condiciones de tratamiento de

Código:	LE-MN-001	MANUAL	
Versión	01		
Fecha:	28/08/2023	PROTECCIÓN DE DATOS PERSONALES	
Página:	5 de 42		

datos que le sea encargado.

- h.** Implementar las medidas administrativas que garanticen el cumplimiento de los derechos de los titulares de datos personales de acuerdo con lo estipulado en la Ley 29733, Título III – Derechos del Titular de Datos Personales, Artículos del 18 al 27.
- i.** Gestionar el registro de los bancos de datos personales ante la Dirección de Protección de Datos Personales, en coordinación con el Departamento Legal.
- j.** Identificar los bancos de datos personales, así como las necesidades de registrar la creación, modificación o cancelación de los bancos de datos personales a su cargo.
- k.** Aplicar el secreto profesional a los datos personales a los que estén asignados a acceder.
- l.** Velar por el cumplimiento dentro de su ámbito de los principios rectores indicados en el Título I - Artículos del 4 al 11, de la Ley 29733, Ley de Protección de Datos Personales: (i) Principio de legalidad; (ii) Principio de consentimiento; (iii) Principio de finalidad; (iv) Principio de proporcionalidad; (v) principio de calidad; (vi) Principio de seguridad; (vii) Principio de disposición de recurso; (viii) Principio de nivel de protección.

3.2.5 Encargado del Tratamiento de Datos Personales

Está representado por cada uno de los trabajadores de P.A. PERU S.A.C. Nivel operativo en todos los procesos en los que se realiza el tratamiento de bancos de datos personales, cuyas responsabilidades son las siguientes:


- a.** Velar en todo momento por la seguridad de los datos personales.
- b.** Aplicar el secreto profesional a los datos personales a los que estén asignados a acceder.
- c.** Cumplir con los principios rectores de la Ley 29733, Ley de Protección de Datos Personales.
- d.** Obtener el consentimiento desde los medios no automatizados que sean puestos a su disposición para tal fin.
- e.** Velar por el cumplimiento y otorgamiento de los derechos de los titulares de datos personales de acuerdo con lo estipulado en la Ley 29733, Título III – Derechos del Titular de Datos Personales, Artículos del 18 al 27 y a las medidas administrativas que por motivo de ello sea implementado por la organización.

3.2.6 Titular de Datos Personales

- a.** Es responsable de sus propios datos personales, debe tomar en cuenta que su consentimiento para el tratamiento de sus datos personales debe ser libre, previo e informado y verificar que su consentimiento sea registrado en los términos en que expresa e inequívocamente lo ha dado.
- b.** Es responsable de conocer y ejercer los derechos conferidos por la Ley 29733, Ley de Protección de Datos Personales.


Todos los actores que componen la organización de la protección de datos personales son pasibles de las sanciones que la organización defina de acuerdo con la gravedad del incumplimiento del que sean protagonistas y en función de los resultados de las investigaciones y/o pericias pertinentes.

Por su parte, el Titular de Datos Personales tiene responsabilidades de acuerdo con lo indicado en la Ley 29733; estas responsabilidades deben ser de observancia obligatoria y general por parte de los actores de la Organización de la Protección de Datos Personales de P.A. PERU S.A.C.


Código:	LE-MN-001	MANUAL	
Versión	01		
Fecha:	28/08/2023	PROTECCIÓN DE DATOS PERSONALES	
Página:	6 de 42		

4. DEFINICIONES


- a) Anonimización:** Es el proceso de ocultar o eliminar cualquier aspecto que vincula un conjunto de datos con el propietario de estos. Es decir, es un proceso de alteración de los datos – codificando (o encriptando) los identificadores clave – para complicar la identificación y fomentar un movimiento de datos más seguro entre sistemas.
- b) Autoridad Nacional de Protección de Datos Personales (APDP):** La Dirección General de Transparencia, Acceso a la Información Pública y Protección de Datos Personales, del Ministerio de Justicia y Derechos Humanos, es la Autoridad Nacional de Protección de Datos Personales. Corresponde a esta institución realizar todas las acciones necesarias para el cumplimiento del objeto y demás disposiciones de la Ley 29733 y de su reglamento (en adelante, “La ley y su reglamento”). Para tal efecto, goza de potestad sancionadora, de conformidad con la Ley 27444, Ley del Procedimiento Administrativo General, o la que haga sus veces, así como de potestad coactiva, de conformidad con la Ley 26979, Ley de Procedimiento de Ejecución Coactiva, o la que haga sus veces.
- c) Banco de datos personales:** Conjunto organizado de datos personales, automatizado o no, independientemente del soporte, sea este físico, magnético, digital, óptico u otros que se creen, cualquiera fuere la forma o modalidad de su creación, formación, almacenamiento, organización y acceso.
- d) Banco de datos personales de administración privada:** Banco de datos personales cuya titularidad corresponde a una persona natural o a una persona jurídica de derecho privado, en cuanto el banco no se encuentre estrictamente vinculado al ejercicio de potestades de derecho público.
- e) Banco de datos personales de administración pública:** Banco de datos personales cuya titularidad corresponde a una entidad pública.
- f) Banco de datos personales no automatizado:** Conjunto de datos de personas naturales no computarizado y estructurado conforme a criterios específicos, que permita acceder sin esfuerzos desproporcionados a los datos personales, ya sea aquel centralizado, descentralizado o repartido de forma funcional o geográfica.
- g) Bloqueo:** Es la medida por la que el encargado de tratamiento de datos personales impide el acceso de terceros a los datos y éstos no pueden ser objeto de tratamiento, durante el periodo en que se esté procesando alguna solicitud de actualización, inclusión, rectificación o supresión, en concordancia con lo que dispone el tercer párrafo del artículo 20 de la Ley. Se dispone también como paso previo a la cancelación por el tiempo necesario para determinar posibles responsabilidades en relación a los tratamientos, durante el plazo de prescripción legal o prevista contractualmente.
- h) Cancelación:** Es la acción o medida que en la Ley se describe como supresión, cuando se refiere a datos personales, que consiste en eliminar o suprimir los datos personales de un banco de datos.
- i) Consentimiento Libre:** Sin que medie error, mala fe, violencia o dolo que puedan afectar la manifestación de voluntad del titular de los datos personales. La entrega de obsequios o el otorgamiento de beneficios al titular de los datos personales con ocasión de su consentimiento no afectan la condición de libertad que tiene para otorgarlo, salvo en el caso de menores de edad, en los supuestos en que se admite su consentimiento, en que no se considerará libre el consentimiento otorgado mediando obsequios o beneficios. El condicionamiento de la prestación de un servicio, o la advertencia o amenaza de denegar el acceso a beneficios o servicios que normalmente son de acceso no restringido, sí afecta la libertad de quien otorga consentimiento para el tratamiento de sus datos personales, si los datos solicitados no son indispensables para la prestación de los beneficios o servicios.

Código:	LE-MN-001	MANUAL	
Versión	01		
Fecha:	28/08/2023	PROTECCIÓN DE DATOS PERSONALES	
Página:	7 de 42		

- j) Consentimiento Previo:** Con anterioridad a la recopilación de los datos o en su caso, anterioral tratamiento distinto a aquel por el cual ya se recopilaron.
- k) Consentimiento Expreso e Inequívoco:** Cuando el consentimiento haya sido manifestado en condiciones que no admitan dudas de su otorgamiento. Se considera que el consentimiento expreso se otorgó verbalmente cuando el titular lo exterioriza oralmente de manera presencial o mediante el uso de cualquier tecnología que permita la interlocución oral.
- l) Consentimiento Informado:** Cuando al titular de los datos personales se le comunique clara, expresa e indubitablemente, con lenguaje sencillo, cuando menos de lo siguiente:
- I. La identidad y domicilio o dirección del titular del banco de datos personales o del responsable del tratamiento al que puede dirigirse para revocar el consentimiento o ejercer sus derechos.
 - II. La finalidad o finalidades del tratamiento a las que sus datos serán sometidos.
 - III. La identidad de los que son o pueden ser sus destinatarios, de ser el caso, la existenciadel banco de datos personales en que se almacenarán, cuando corresponda.
 - IV. El carácter obligatorio o facultativo de sus respuestas al cuestionario que se le proponga, cuando sea el caso.
 - V. Las consecuencias de proporcionar sus datos personales y de su negativa a hacerlo.
 - VI. En su caso, la transferencia nacional e internacional de datos que se efectúen
- m) Datos personales:** Es aquella información numérica, alfabética, gráfica, fotográfica, acústica, sobre hábitos personales, o de cualquier otro tipo concerniente a las personas naturales que las identifica o las hace identificables a través de medios que puedan ser razonablemente utilizados.
- n) Datos personales relacionados con la salud:** Es aquella información concerniente a la salud pasada, presente o pronosticada, física o mental, de una persona, incluyendo el grado de discapacidad y su información genética.
- o) Datos sensibles:** Datos personales constituidos por los datos biométricos que por sí mismos pueden identificar al titular; datos referidos al origen racial y étnico; imágenes, fotos, ingresos económicos, opiniones o convicciones políticas, religiosas, filosóficas o morales; afiliación sindical, características físicas, hechos o circunstancias de su vida afectiva o familiar, los hábitos personales que corresponden a la esfera más íntima, la información relativa a la salud física o mental u otras análogas que afecten su intimidad.
- p) Dirección General de Transparencia, Acceso a la Información Pública y Protección de Datos Personales:** Es el órgano encargado de ejercer la Autoridad Nacional de Protección de Datos Personales.
- q) Emisor o exportador de datos personales:** Es el titular del banco de datos personales o aquél que resulte responsable del tratamiento situado en el Perú que realice, conforme a lo dispuesto en el presente reglamento, una transferencia de datos personales a otro país.
- r) Encargado del tratamiento de datos personales:** Toda persona natural, persona jurídica de derecho privado o entidad pública que sola o actuando conjuntamente con otra realiza el tratamiento de los datos personales por encargo del titular del banco de datos personales en virtud de una relación jurídica que le vincula con el mismo y delimita el ámbito de su actuación. Incluye a quien realice el tratamiento sin la existencia de un banco de datos personales. Esta función lo asumirán directores, Gerentes, jefes, analistas, asistentes que sean designados por los responsables del tratamiento de datos.
- s) Encargo de tratamiento:** Entrega por parte del titular del banco de datos personales a un encargado de tratamiento de datos personales en virtud de una relación jurídica que los vincula. Dicha relación jurídica delimita el ámbito de actuación del encargado de tratamiento de los datos personales.

Código:	LE-MN-001	MANUAL	
Versión	01		
Fecha:	28/08/2023	PROTECCIÓN DE DATOS PERSONALES	
Página:	8 de 42		

- t) 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.
- u) Fuentes accesibles para el público:** Bancos de datos personales de administración pública o privada, que pueden ser consultados por cualquier persona, previo abono de la contraprestación correspondiente, de ser el caso.
- v) Nivel suficiente de protección para los datos personales:** Nivel de protección que abarca por lo menos la consignación y el respeto de los principios rectores de la Ley, así como medidas técnicas de seguridad y confidencialidad, apropiadas según la categoría de datos de que se trate.
- w) Procedimiento de anonimización:** Tratamiento de datos personales que impide la identificación o que no hace identificable al titular de estos. El procedimiento es irreversible.
- x) Procedimiento de disociación:** Tratamiento de datos personales que impide la identificación que no hace identificable al titular de estos. El procedimiento es reversible.
- y) Receptor o importador de datos personales:** Es toda persona natural o jurídica de derecho privado, incluyendo las sucursales, filiales, vinculadas o similares; o entidades públicas, que recibe los datos en caso de transferencia internacional, ya sea como titular o encargado de tratamiento de datos personales, o como tercero.
- z) Rectificación:** Es aquella acción genérica destinada que afectar o modificar un banco de datos personales ya sea para actualizarlo, incluir información en él o específicamente rectificarse su contenido con datos exactos.
- aa) Registro Nacional de Protección de Datos Personales:** Es la unidad de almacenamiento destinada a contener principalmente la información sobre los bancos de datos personales de titularidad pública o privada y tiene por finalidad dar publicidad de la inscripción de dichos bancos de tal forma que sea posible ejercer los derechos de acceso a la información, rectificación, cancelación, oposición y otros regulados en la Ley y el presente reglamento. El Registro Nacional se encuentra bajo responsabilidad de la Dirección de Protección de Datos Personales, que es una unidad orgánica de la Dirección General de Transparencia, Acceso a la Información Pública y Protección de Datos Personales (APDP) del Ministerio de Justicia y Derechos Humanos.
- bb) Repertorio de jurisprudencia:** Es el banco de resoluciones judiciales o administrativas que se organizan como fuente de consulta y destinadas al conocimiento público.
- cc) Responsable del tratamiento:** Es aquél que decide sobre el tratamiento de datos personales, aun cuando no se encuentren en un banco de datos personales. El responsable del tratamiento de datos personales representada para P.A. PERU S.A.C. (titular del banco de datos personales). Esta función será asumida por Accionistas, Gerentes, directores y jefes de cada área del negocio.
- dd) Tercero:** Es toda persona natural, persona jurídica de derecho privado o entidad pública, distinta del titular de datos personales, del titular o encargado de tratamiento de datos personales y del responsable del tratamiento, incluyendo a quienes tratan los datos bajo autoridad directa de aquellos, como empresas proveedoras de servicios, contratistas o consultores, que brinden servicios o productos a la institución.
- ee) Titular de datos personales:** Persona natural a quien corresponde los datos personales.
- ff) Titular del banco de datos personales:** Persona natural, persona jurídica de derecho privado o entidad pública que determina la finalidad y contenido del banco de datos personales, el tratamiento de estos y las medidas de seguridad. Para efectos de esta norma P.A. PERU S.A.C. es el titular de sus bancos de datos personales.
- gg) Transferencia de datos personales:** Toda transmisión, suministro o manifestación de datos

Código:	LE-MN-001	MANUAL	
Versión	01		
Fecha:	28/08/2023	PROTECCIÓN DE DATOS PERSONALES	
Página:	9 de 42		

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.

hh) 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.

5. DOCUMENTOS DE REFERENCIA

- Constitución Política del Perú.
- Ley 29733 – Ley de Protección de Datos Personales.
- Decreto Supremo 003-2013-JUS – Reglamento de la Ley 29733.
- Directiva de Seguridad de la Ley 29733.
- Decreto Legislativo 1353 - Creación de 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.

6. ACTIVIDADES

6.1 Principios de Protección de Datos Personales

6.1.1 Legalidad del tratamiento de datos personales

Cualquier forma de tratamiento de datos personales se encuentra amparada en las disposiciones legales vigentes entre ellas la Ley 29733 – Ley de Protección de Datos Personales y su Reglamento. En tal sentido, el trabajador de P.A PERU S.A.C. deberá tener especial cuidado que la recopilación, registro, organización, almacenamiento, utilización, transferencia o cualquier otra forma de procesamiento, no haya sido utilizada por medios fraudulentos, desleales o ilícitos.


Está prohibido gestionar los datos personales bajo los supuestos indicados en el párrafo anterior, con cargo a dejarse constancia en el expediente personal del trabajador reportarse al Departamento de Recursos Humanos para las acciones legales correspondientes.

6.1.2 Consentimiento del titular de los datos personales

El trabajador de P.A. PERU S.A.C. que realice el tratamiento de los datos personales tiene el deber de asegurarse que éstos hayan sido otorgados de manera consentida por el titular de los datos personales, salvo los supuestos de excepción previstos en la Ley de Protección de Datos Personales.

Dicho consentimiento debe ser libre, previo, expreso e inequívoco. La forma prevista para acreditarlo puede ser escrita, digital u otro mecanismo válido que garantice la identidad de su titular. Cuando se trate de datos sensibles, el consentimiento deberá ser por escrito necesariamente.

En el caso que, los datos personales correspondan a los trabajadores de P.A. PERU S.A.C., dicho consentimiento no será válido si como consecuencia de ello, deriva o pudiera derivar en algún perjuicio relevante para el trabajador.

Código:	LE-MN-001	MANUAL	
Versión	01		
Fecha:	28/08/2023	PROTECCIÓN DE DATOS PERSONALES	
Página:	10 de 42		

6.1.3 Finalidad de los datos personales

Los datos personales objeto de tratamiento no deberán ser usados para fines distintos para los que los hubieran sido consignados.

El trabajador de P.A. PERU S.A.C., que realice el tratamiento de los datos personales deberá eliminarlos cuando estos hayan dejado de ser necesarios o pertinentes para los fines para los cuales hubieren sido recabados.

6.1.4 Proporcionalidad de los datos personales

El tratamiento de los datos personales que realice el trabajador de P.A. PERU S.A.C., debe guardar proporcionalidad con los fines para los que fueron recopilados. Por tanto, se considerará solo a aquellos datos personales que sean adecuados, relevantes y no excesivos a la finalidad señalada.

6.1.5 Calidad y exactitud de los datos personales

En la medida de lo posible, el tratamiento que el colaborador de P.A. PERU S.A.C. brinde a los datos personales, será actualizado y veraz. Procurará que dichos datos sean lo más exactos posibles y buscará que este deber de veracidad no solo sea en la recopilación de éstos, sino que, ante la falta de calidad de éstos (o se determine un trato inadecuado respecto de su finalidad), comunique inmediatamente a su jefe inmediato a fin de coordinar con el área encargada interna del tratamiento, para su actualización o supresión definitivos.

6.1.6 Seguridad y Deber de Secreto

Sin perjuicio de cualquier otra disposición o medida implementada por P.A. PERU S.A.C., para con sus trabajadores que intervengan en cualquier fase del tratamiento de los datos personales, se encuentran obligados a cumplir con el deber de confidencialidad, no pudiendo divulgarlos, salvo expresa autorización del titular de estos.

P.A. PERU S.A.C. y/o cualquiera de los encargados del tratamiento de datos personales adoptarán las medidas técnicas, organizativas y legales necesarias para garantizar la seguridad de los datos personales que gestione su personal.


6.1.7 Disposición de recurso

Todos los trabajadores de P.A. PERU S.A.C., que realicen el tratamiento de datos personales deberán orientar a los titulares de estos para hacer efectiva cualquier solicitud sobre sus derechos, de ser el caso. Para tal efecto, informarán que existen vías administrativas o judiciales para hacer efectivos sus derechos.

6.1.8 Nivel de Protección Adecuado

Cuando el tratamiento de datos personales involucre una transferencia internacional o flujo transfronterizo, el personal de P.A. PERU S.A.C. deberá verificar que, el país receptor de los datos personales cuente con un nivel de protección adecuado; caso contrario, informará a su jefe inmediato para tomar las previsiones correspondientes con el titular de los datos personales y evitar cualquier contingencia legal contra P.A. PERU S.A.C.

La transferencia deberá formalizarse mediante mecanismos que permitan demostrar que el titular del banco de datos personales o el responsable del tratamiento comunicó al responsable receptor las condiciones en las que el titular de los datos personales consintió el tratamiento de estos.

Código:	LE-MN-001	MANUAL	
Versión	01		
Fecha:	28/08/2023	PROTECCIÓN DE DATOS PERSONALES	
Página:	11 de 42		

6.2 Derechos de los Titulares de Datos Personales

6.2.1 Información en la Recopilación de los Datos

El trabajador de P.A. PERU S.A.C. deberá considerar no develar información que el Titular de Datos Personales entregue, garantizando la confidencialidad de la información; debe cumplir con los plazos establecidos por ley para dar respuesta a las solicitudes presentadas por los titulares de datos personales y considerar los flujos del proceso, no acceder a entregar información a persona distinta del titular salvo que medie autorización expresa y por escrito, a no proporcionar información reservada del titular por actos de soborno o ventaja económica, entre otros.

El trabajador de P.A. PERU S.A.C. deberá considerar que los titulares de los datos personales sean debidamente informados que dichos datos serán utilizados para los fines previstos por la empresa. Dicha información será expresa, precisa e inequívoca.

Asimismo, informará el destino que tendrán los datos personales y, de ser el caso, el Banco de Datos en el cual serán almacenados. Asimismo, informará de la posibilidad de ejercitar los derechos de acceso, rectificación, cancelación y oposición (ARCO).

De otro lado, con mayor énfasis, el encargado del tratamiento de los datos personales de trabajadores de P.A. PERU S.A.C. deberá informar con total transparencia sobre el uso y finalidad que se darán a sus datos personales. El tratamiento no solo debe ser efectuado de manera proporcional, sino que no debe restringir injustificadamente los derechos y libertades de los interesados.

6.2.2 Derecho de Acceso

Cualquier persona titular de datos personales que sean tratados por P.A. PERU S.A.C., tiene derecho a obtener de la institución, la información que corresponda con relación a los datos que sobre sí mismos fueron objeto de tratamiento, así como la forma en que sus datos fueron recopilados, las razones que motivaron dicha recopilación, a solicitud de quién se realizó la recopilación, así como las transferencias realizadas o que se prevén hacer de ellos.

Este derecho se hará efectivo cuando el titular de los datos personales, o su representante legal, requiera a P.A. PERU S.A.C. mediante medio escrito o cualquier otro que permita dejar constancia de la identidad del solicitante y la atención de la solicitud, y en un plazo de veinte (20) días desde la fecha de presentación de la solicitud.

En el caso de que P.A. PERU S.A.C. no trate o haya tratado los datos personales solicitados, lo comunicará oportunamente a los titulares de dichos datos.


6.2.3 Derecho de Rectificación

Por el derecho de rectificación el titular de datos personales o su representante legal, puede solicitar la corrección, actualización e inclusión de éstos, cuando estos sean total o parcialmente inexactos o errados.

A solicitud del titular de los datos personales, P.A. PERU S.A.C. hará efectivo el derecho de rectificación cuando sea oportunamente requerido por medio escrito o cualquier otro que permita dejar constancia de la identidad del solicitante y la atención de la solicitud, siempre que se determine que corresponde la rectificación del contenido por la actualización o corrección de los datos personales.

Durante el plazo que la solicitud de rectificación efectuada por el titular de datos personales se encuentre en proceso de atención, el encargado del banco de datos personales o el Departamento de Tecnología efectuará el bloqueo de dichos datos, con el fin de impedir que terceros accedan a los mismos mientras se mantiene la solicitud en curso.

El personal encargado de dar cumplimiento a la solicitud efectuada por el titular de los

Código:	LE-MN-001	MANUAL	
Versión	01		
Fecha:	28/08/2023	PROTECCIÓN DE DATOS PERSONALES	
Página:	12 de 42		

datos personales cuenta con un plazo de diez (10) días hábiles desde la fecha de presentación de la solicitud.

6.2.4 Derecho de Cancelación

Por el derecho de cancelación, cesa el tratamiento de los datos personales, cuando media solicitud justificada del titular de éstos.

El responsable de P.A. PERU S.A.C., procederá con la cancelación o supresión de los datos personales cuando determine que corresponde dicha cancelación o supresión, debido a que ha transcurrido el plazo para el cual los mismos fueron recopilados, o bien se ha cumplido la finalidad que motivó su recopilación y tratamiento.

Durante el plazo que la solicitud de cancelación o supresión efectuada por el titular de datos personales se encuentre en proceso de atención, el encargado del banco de datos personales o Departamento de Tecnología efectuará el bloqueo de dichos datos, con el fin de impedir que terceros accedan a los mismos mientras se mantiene la solicitud en curso.

El personal encargado de dar cumplimiento a la solicitud efectuada por el titular de los datos personales cuenta con un plazo de diez (10) días hábiles desde la fecha de presentación de la solicitud.

6.2.5 Derecho de Oposición

El titular de los datos personales puede oponerse al tratamiento de uno, varios o todos los datos que cuyo tratamiento decida realizar P.A. PERU S.A.C. Dicha solicitud debe contar con la debida justificación, y procederá siempre que el tratamiento no estuviera amparado en una norma legal o en el consentimiento del titular de datos personales, luego de lo cual, el colaborador encargado del tratamiento de los datos personales procederá a suprimirlos de sus bancos de datos, sean físicos o digitales.

El personal encargado de dar cumplimiento a la solicitud efectuada por el titular de los datos personales cuenta con un plazo de diez (10) días hábiles desde la fecha de presentación de la solicitud.

6.2.6 Acceso, Rectificación, Cancelación u Oposición

Los derechos de acceso, rectificación, cancelación u oposición (ARCO) de los datos personales se ejercerán siempre ante P.A. PERU S.A.C., quien implementará los canales de atención adecuados para que los titulares de datos personales puedan hacer valer sus derechos.


La solicitud debe hacerse por medio escrito y estará dirigida a las áreas definidas por la institución, Departamento Legal y Departamento de Tecnología, cuyo personal tendrá especial cuidado en cumplir con los plazos señalados en los literales precedentes.

En aquellos casos que el personal de P.A. PERU S.A.C., determine que no existen datos personales del solicitante que sean materia de tratamiento, la solicitud no podrá ser atendida, ante lo cual le informará de la improcedencia.

6.3 Comunicación de los Datos Personales

6.3.1 Uso Inaceptable de la Información referida a Datos Personales

El trabajador de P.A. PERU S.A.C. se encuentra prohibido de realizar las actividades indicadas en el presente párrafo, sin que esta enumeración sea limitativa. No se aceptará por ningún motivo el uso de la información referida a datos personales en los siguientes supuestos:

Código:	LE-MN-001	MANUAL	
Versión	01		
Fecha:	28/08/2023	PROTECCIÓN DE DATOS PERSONALES	
Página:	13 de 42		

- a. Realizar el tratamiento sin el previo consentimiento del titular del dato personal, cuando este sea obligatorio.
- b. Realizar el tratamiento para beneficio propio.
- c. Realizar el tratamiento para realizar actividades contrarias a la Ley.

6.3.2 Comunicación de los Datos Personales a Terceros y al Público

El personal de P.A. PERU S.A.C. solo podrá transferir los datos personales respecto de los cuales es responsable del tratamiento, en los siguientes supuestos:

- a. Cuando el destinatario sea un tercero legitimado y sea en cumplimiento de fines directamente relacionados con las funciones legítimas del tercero destinatario
- b. En aplicación de la Ley N.º 27806, Ley de Transparencia y Acceso a la Información Pública, cuando sea solicitado por cualquier sujeto interesado respecto de la información pública accesible, previa determinación por P.A. PERU S.A.C. de la situación en concreto.
- c. Para cumplimiento de una relación contractual y/o profesional.
- d. En los casos en que exista un consentimiento previo del titular de los datos, salvo disposición contraria de la Ley y el Reglamento.

No se considera transferencia, el acceso de un tercero a los mismos, cuando dicho acceso sea necesario para la prestación de un servicio específico a P.A. PERU S.A.C. y cuando se trate de un supuesto de tratamiento por encargo.

6.3.3 Acceso o tratamiento de datos por cuenta de terceros a causa de servicios

La realización de tratamiento de datos personales por cuenta de terceros debe estar regulada por medio escrito, es decir, mediante un contrato formal, estableciéndose expresamente que el encargado del tratamiento solo podrá tratar los datos personales conforme a las instrucciones y lineamientos establecidos.


En caso de incumplimiento de las estipulaciones establecidas en el contrato, el trabajador de P.A. PERU S.A.C., encargado del tratamiento será considerado, también responsable del tratamiento, respondiendo de las infracciones en que hubiera incurrido personalmente.

En el contrato se estipularán, asimismo, las medidas de seguridad que el encargado del tratamiento está obligado a implementar.

Una vez cumplida la prestación contractual, los datos personales serán destruidos, devueltos o custodiados bajo los términos vigentes que establezca el Departamento de Tecnología de P.A. PERU S.A.C.

El tratamiento de datos personales por cuenta de terceros puede configurarse en dos supuestos:

- a. Cuando, en virtud de una relación jurídica que vincula a P.A. PERU S.A.C. con un tercero, P.A. PERU S.A.C. debe tratar datos personales de los cuales dicho tercero es encargado o responsable del tratamiento, con el fin de cumplir con las obligaciones a su cargo.
- b. Cuando, en virtud de una relación jurídica que vincula a P.A. PERU S.A.C., con un tercero, P.A. PERU S.A.C. otorga acceso o encarga todo o parte del tratamiento de datos personales a un tercero.

Código:	LE-MN-001	MANUAL	
Versión	01		
Fecha:	28/08/2023	PROTECCIÓN DE DATOS PERSONALES	
Página:	14 de 42		

6.3.4 Comunicación de Datos con Fines de Investigación y/o Estadísticos

La comunicación de datos o su uso interno con fines de investigación y/o estadísticos sólo se producirá con la autorización del titular de los datos o cuando se haya aplicado respectivamente de estos un procedimiento de disociación o anonimización.

6.3.5 Flujo transfronterizo de datos personales

La transferencia internacional de datos personales o flujo transfronterizo solamente será posible si el destinatario ofrece una garantía igual o mayor de protección a lo establecido en la legislación peruana. De ser el caso, y de presentarse una situación de flujo transfronterizo de información, en la cual el personal de P.A. PERU S.A.C. no tenga claro si el tratamiento involucra un flujo transfronterizo, deberá informar de inmediato a su jefe directivo, de corresponder, coordinar cualquier consulta sobre dicha transferencia a la Dirección de Protección de Datos Personales del Ministerio de Justicia y Derechos Humanos.

6.4 Gestión de las Bancos de Datos

6.4.1 Creación, modificación o supresión de Bancos de Datos Personales

El tratamiento de los datos personales que realiza los trabajadores de P.A. PERU S.A.C. puede dar lugar a la creación de Bancos de Datos, los cuales serán creados, modificados o eliminados por el Departamento de Tecnología en coordinación con el Área/Departamento responsable del Banco de Datos Personales y Departamento Legal, este último comunicará dicho acto a la Dirección de Protección de Datos Personales del Ministerio de Justicia y Derechos Humanos, mediante la debida inscripción en el Registro de Protección de Datos Personales.


Cada uno de los Bancos de Datos registrados por P.A. PERU S.A.C. ante la Dirección de Protección de Datos Personales estará a cargo del Área/Departamento interno que tendrá la responsabilidad de comunicar al Departamento de Tecnología sobre cualquier modificación que se deba realizar en los correspondientes Bancos de Datos a su cargo.

A fin de solicitar la inscripción ante el Registro Nacional de Protección de Datos Personales antes mencionado, las áreas internas de P.A. PERU S.A.C. encargadas de los Bancos de Datos deberán proporcionar la siguiente información:

- a. Denominación del Banco de Datos
- b. Finalidad
- c. Usos previstos
- d. Sistema/s de Tratamiento
- e. Tipos de datos personales
- f. Procedimientos de obtención
- g. Ubicación física del banco de datos
- h. Receptores de los datos a nivel nacional
- i. Receptores de los datos a nivel internacional
- j. Medidas de Seguridad

6.4.2 Seguridad en Tratamiento de Datos Personales en Menores

El personal de P.A. PERU S.A.C. es consciente de la importancia y especial cuidado que debe tenerse respecto de los datos personales de menores de edad. Por tal motivo, cada vez que se tome conocimiento del tratamiento de este tipo de datos en la empresa, se deberá contar con el consentimiento expreso de los padres o tutores,

Código:	LE-MN-001	MANUAL	
Versión	01		
Fecha:	28/08/2023	PROTECCIÓN DE DATOS PERSONALES	
Página:	15 de 42		

quienes ejercen la representación de los menores. Esta representación constará debidamente acreditada con el documento de sustento legal, bajo los requisitos que establezca el Departamento Legal.

6.4.3 Gestión de la Seguridad de la Información de Banco de Datos

Cada uno de los datos de carácter personal recopilados por P.A. PERU S.A.C. y/o por encargo de este son considerados como un activo valioso y el trabajador responsable los clasificará como "Información Confidencial", previendo que los documentos que sirvan como soporte cuenten con un indicativo que dicho documento físico o digital, contiene datos personales.

La protección de los datos personales está prevista en el Sistema de Gestión de Seguridad de la Información de P.A. PERU S.A.C. a cargo del Departamento de Tecnología, quien velará el cumplimiento de las medidas necesarias para salvaguardar su integridad, confidencialidad y disponibilidad.

6.5 Medidas de Seguridad

6.5.1 Aplicación de los Niveles de Seguridad

Los trabajadores de P.A. PERU S.A.C. encargados del tratamiento de datos personales deberán adoptar un conjunto de medidas legales, técnicas y organizativas a fin de garantizar la seguridad de los datos personales; estas medidas serán implementadas previa identificación de las categorías de los datos personales (ver Anexo 2), de acuerdo con su nivel de criticidad tanto en la recolección como en su propio tratamiento, de acuerdo con lo dispuesto por el principio de seguridad.

Para todos los efectos, el tratamiento de los datos personales realizados por P.A. PERU S.A.C. y los Bancos de Datos de los cuales es titular, tendrán un nivel alto de protección, entendiéndose éste como aquel que permite establecer medidas de seguridad integral para garantizar su integridad, confidencialidad y disponibilidad. Asimismo, se protegerá ante el acceso o filtración por parte de terceros no autorizados y el no repudio de los mismos por parte de su titular.


6.5.2 Responsable de seguridad

La protección de los datos personales está prevista en el Sistema de Gestión de Seguridad de la Información de P.A. PERU S.A.C., cuyo objetivo es velar por el cumplimiento de las medidas necesarias para salvaguardar su integridad, confidencialidad y disponibilidad.

El Departamento de Tecnología de P.A. PERU S.A.C. y el Departamento Legal, en forma conjunta, coordinan la seguridad en el tratamiento de los datos personales, así como de cada uno de los Bancos de Datos físicos y/o digitales que existieren; y responderá ante la Dirección de Protección de Datos Personales del Ministerio de Justicia y Derechos Humanos.

6.5.3 Bases de Datos temporales o copias de trabajo de documentos

Al igual que las bases de datos permanentes, el personal de P.A. PERU S.A.C., deberá considerar que las bases de datos temporales serán tratadas con las medidas de seguridad de nivel alto y, una vez que se haya culminado el objeto para el cual fueron recogidos los datos personales, el personal de P.A. PERU S.A.C. procederá con su eliminación física y digital.

Código:	LE-MN-001	MANUAL	
Versión	01		
Fecha:	28/08/2023	PROTECCIÓN DE DATOS PERSONALES	
Página:	16 de 42		

6.5.4 Documento Maestro de Protección de Datos Personales

P.A. PERU S.A.C., implementará una normativa de seguridad mediante un documento de obligatorio cumplimiento para el personal con acceso a los datos personales y a los sistemas de información que los contengan. Dicho documento formará parte del marco de Privacidad de Datos Personales y estará a cargo del Departamento de Tecnología y Departamento Legal.

El documento de seguridad deberá incluir los siguientes temas:

- a. Ámbito de aplicación del documento con especificación detallada de los recursos protegidos.
- b. Medidas y procedimientos de actuación destinados a garantizar el nivel de seguridad exigido en la normatividad vigente y del presente Capítulo.
- c. Funciones y responsabilidades del personal correspondientes a la protección de datos personales.
- d. Descripción de los sistemas de información que los tratan.
- e. Lineamientos sobre notificación, gestión y respuesta ante las incidencias.
- f. Los procedimientos de realización de copias de respaldo y de recuperación de los datos.
- g. Controles periódicos que se deban realizar para verificar el cumplimiento de lo dispuesto en el propio documento de seguridad.
- h. Medidas a adoptar para el transporte de soportes y documentos.
- i. Medidas a adoptar para la destrucción o reutilización de los documentos y soportes.

6.5.5 Fiscalización Administrativa

El personal de P.A. PERU S.A.C., debe conocer las obligaciones y responsabilidades que tiene para con las entidades administrativas que fiscalizan la información confidencial y protección de datos personales, en especial la Dirección de Protección de Datos Personales del Ministerio de Justicia y Derechos Humanos.


Para ello, los responsables de cada Área/Departamento que realicen el tratamiento de datos personales recomendarán a su personal que, ante cualquier duda sobre las consecuencias de un mal uso de los datos personales por parte de los trabajadores, ingresen a la página web de la Dirección de Datos Personales (<https://www.minjus.gob.pe/proteccion-de-datos-personales/>) o directamente con el Departamento Tecnología.

6.6 Del personal de P.A. PERU S.A.C.

6.6.1 Funciones y Obligaciones del Personal

El Departamento de Tecnología contará con un documento maestro de Seguridad el cual marcará las pautas sobre las funciones y responsabilidades de los trabajadores de P.A. PERU S.A.C., con acceso a los datos personales materia del presente Capítulo, así como definirá sus perfiles.

Cada Área/Departamento responsable interna de cada Banco de Datos Personales informará al Departamento de Tecnología y Departamento Legal sobre las medidas de seguridad que ha adoptado su personal y les recordará sobre las consecuencias a las que P.A. PERU S.A.C. se encuentra expuesto en caso de incumplimiento.

Código:	LE-MN-001	MANUAL	
Versión	01		
Fecha:	28/08/2023	PROTECCIÓN DE DATOS PERSONALES	
Página:	17 de 42		

6.6.2 Identificación y autenticación

Las contraseñas proporcionadas a los responsables de los Bancos de Datos Personales, así como al personal a su cargo, se deberá cambiar con la periodicidad que determine el Departamento de Tecnología, que en ningún caso será superior a seis (06) meses, y mientras estén vigentes se almacenarán de forma indescifrable. El tratamiento de datos personales fuera de los locales donde se encuentran los Bancos de Datos Personales deberá ser autorizado expresamente por área interna encargada de cada Banco de Datos de titularidad de P.A. PERU S.A.C. y garantizarse el nivel de seguridad alto.

6.6.3 Gestión y Control de Acceso Digital

Como parte de las medidas de seguridad técnicas, P.A. PERU S.A.C. asegurará que los trabajadores, usuarios de los sistemas de la información de la empresa, cuenten con un usuario y contraseña y estén debidamente controlados. Para ello, se realizarán periódicamente revisiones a los privilegios de acceso a los datos personales y deberá permitirse el registro y trazabilidad de la revisión.

6.6.4 Control de Acceso Físico

Para el caso en que los datos personales sean custodiados mediante documentos en físico, el personal autorizado solo podrá acceder a los ambientes que estén protegidos por una cerradura o similar mecanismo. Dicho mecanismo estará a cargo del Área/Departamento interna encargada del banco de datos personales pertinente.

6.6.5 Copias de respaldo y recuperación

El Departamento de Tecnología de P.A. PERU S.A.C. establecerá procedimientos de actuación para la realización de copias de respaldo, salvo que en dicho período no se hubiera producido ninguna actualización de los datos. Asimismo, se establecerán procedimientos para la recuperación de los datos que garanticen en todo momento su reconstrucción y devolverlos al estado en que se encontraban al tiempo de producirse la pérdida o destrucción.


Deberá conservarse una copia de respaldo de los Bancos de Datos que se encontrará en un lugar diferente de aquél en que se encuentren los equipos informáticos que los tratan cumpliendo en todo caso las medidas de seguridad establecidas.

6.6.6 Auditoría

P.A. PERU S.A.C. deberá incorporar en su programa de Auditoría del Sistema de Gestión de Seguridad de la Información, un acápite especial relacionado a las medidas de seguridad implementadas para asegurar la mitigación de los riesgos relacionados a la protección de datos personales.

6.6.7 Capacitación

En el proceso de ingreso de cada trabajador, P.A. PERU S.A.C. incluirá una sección especial para el desarrollo de una capacitación de creación de conciencia y entrenamiento en materia de protección de datos personales, la cual constará en documento de aceptación del conocimiento y respeto a los principios de la Ley de Protección de Datos Personales y su Reglamento.

Código:	LE-MN-001	MANUAL	
Versión	01		
Fecha:	28/08/2023	PROTECCIÓN DE DATOS PERSONALES	
Página:	18 de 42		

6.7 Disposiciones adicionales

6.7.1 Excepciones y Sanciones

Cualquier excepción al cumplimiento del presente Capítulo debe ser registrada y aprobada por el Departamento de Tecnología con informe del Departamento Legal. El incumplimiento del presente documento se considerará como falta grave y será sancionado como tal, según lo estipulado en el Reglamento Interno de Trabajo (RIT) y en este manual.

6.7.2 Obligatoriedad

El presente Capítulo es de obligatorio cumplimiento para todos los trabajadores de P.A. PERU S.A.C. Aquellos que incumplan con las conductas descritas en el presente Capítulo serán pasibles de sanciones, según corresponda.


6.8 Condiciones internas y externas de la seguridad

6.8.1 Condiciones de seguridad externas

- a. Como marco legal para la protección de datos personales, se tiene la Ley 29733, Ley de Protección de Datos Personales, y su reglamento; aplicable a P.A. PERU S.A.C. como persona jurídica de derecho privado, que provee servicios a sus clientes.
- b. El conocimiento y conciencia acerca de la importancia de la protección de datos personales, la Ley 29733, Ley de Protección de Datos Personales, y su reglamento, son realizados por medio de Capacitación y Concientización de Protección de Datos Personales que tiene implementado P.A. PERU S.A.C., los mismos que están bajo la responsabilidad del Departamento Legal a través del Departamento de Recursos Humanos.

6.8.2 Condiciones de seguridad interna

- a. La Gerencia General de P.A. PERU S.A.C. se compromete a brindar todos los recursos necesarios y la dirección activa en la protección de los datos personales contenidos y destinados a ser contenidos en los bancos de datos personales de los que P.A. PERU S.A.C. como persona jurídica de derecho privado, es titular.
- b. Así mismo, en la Política Corporativa de Protección de Datos Personales, se expresa el compromiso de la Gerencia General de P.A. PERU S.A.C. con el cumplimiento de la Ley 29733, Ley de Protección de Datos Personales, y su reglamento mediante las acciones de mejora continua y el respeto a sus principios rectores.
- c. P.A. PERU S.A.C. trata datos personales en sus diferentes procesos administrativos y de negocio, los mismos que son protegidos bajo el marco de privacidad.
- d. La organización y responsabilidades están establecidos en la presente Manual, Capítulo Segundo; en el que se enuncia la responsabilidad de cada actor dentro del marco de privacidad y en especial del Departamento Legal, quien tiene todas las facultades, recursos y autoridad para liderar y hacer cumplir la Política Corporativa de Protección de Datos Personales en todos los estratos


Código:	LE-MN-001	MANUAL	
Versión	01		
Fecha:	28/08/2023	PROTECCIÓN DE DATOS PERSONALES	
Página:	19 de 42		

organizativos.

- e. Los datos personales contenidos o destinados a ser contenidos en los bancos de datos personales de P.A. PERU S.A.C. se gestionan y protegen bajo el enfoque de riesgos de la protección de datos personales estableciendo requisitos de seguridad.


6.9 Requisitos de seguridad

- a. La Política Corporativa de Protección de Datos Personales, constituye el compromiso e involucramiento de la Gerencia General de P.A. PERU S.A.C. con la protección de datos personales que se tratan en la empresa.
- b. La gobernabilidad de los procesos involucrados en el tratamiento de los datos personales se da mediante las siguientes actividades preliminares, básicas para el entendimiento, que deben ser lideradas por el Departamento Legal (a través del Departamento de Recursos Humanos) de forma conjunta con el Departamento de Tecnología, responsable de la seguridad de los bancos de datos personales:
 - Identificación de los flujos de datos personales.
 - Identificación de los procesos en los que se tratan datos personales.
 - Identificación de los responsables y encargados de tratamiento.
 - Identificación de los encargados de tratamiento de datos personales externos o terceras partes que acceden a los bancos de datos personales de titularidad de P.A. PERU S.A.C.
 - Aplicar, por parte de la Gerencia General, el manual de Protección de Datos Personales con la finalidad que se cumplan sus lineamientos en toda la organización.
 - Aplicar lo establecido en el Capítulo Segundo del presente Manual a fin de empoderar al Departamento de Tecnología en sus funciones como voz autorizada sobre la seguridad de los bancos de datos personales.
 - Aplicar lo establecido en el Capítulo Segundo del presente Manual, a fin de asignar las responsabilidades allí detalladas a todos los actores de los procesos involucrados en el tratamiento de datos personales, con la finalidad que las asuman y tengan la potestad de decidir en forma controlada sobre los bancos de datos personales que les corresponda.
- c. P.A. PERU S.A.C. aplica las medidas de seguridad para la protección de datos personales correspondiente al nivel de clasificación "Crítico" en conformidad con lo establecido en la Directiva de Seguridad de la Información de la Autoridad de Protección de Datos Personales (en adelante, "APDP") y por ser la clasificación más alta identificada entre los bancos de datos personales de la empresa.
- d. Las medidas de seguridad para la protección de datos personales a ser implementadas y mantenidas se detallan en los incisos k, l y m del numeral 6.9 del presente Manual.
- e. P.A. PERU S.A.C. controla la información documentada del marco de Privacidad, para ello se contará con un listado maestro de información documentada, en el que se gestionan las versiones de los documentos y la conservación y disposición final de

Código:	LE-MN-001	MANUAL	
Versión	01		
Fecha:	28/08/2023	PROTECCIÓN DE DATOS PERSONALES	
Página:	20 de 42		


los registros.

- f. El Departamento de Tecnología establece los lineamientos de seguridad relacionados con los accesos autorizados a los datos mediante procedimientos de identificación y autenticación que garantizan la seguridad del tratamiento de los datos personales.
- g. El Departamento de Tecnología de P.A. PERU S.A.C. deberá establecer un procedimiento formal de gestión de accesos de usuarios a los sistemas informáticos que soporten los bancos de datos personales.
- h. El Departamento de Tecnología debe activar, mantener y monitorear los registros de auditoría de sistemas informáticos que soporten bancos de datos personales.
- i. El Departamento de Tecnología alineará la atención incidentes y problemas en privacidad de datos personales.
 - El Departamento de Tecnología debe generar y mantener registros de incidentes y problemas que afecten a los datos personales que administra la empresa.
- j. El Departamento de Tecnología, debe mantener un Registro de Control de Acceso que se encuentre debidamente documentado y que contemple lo siguiente:
 - La gestión de acceso desde el registro de un usuario.
 - La identificación de un usuario.
 - La gestión de los privilegios del usuario.
 - La identificación del usuario ante el sistema.
 - Registro de la revisión periódica de los privilegios asignados.
 - Para fines de trazabilidad, el Departamento de Tecnología, debe contar con el Registro de Acceso a Bancos de Datos Personales, que provea evidencias sobre las interacciones de los encargados de tratamiento con los datos lógicos.
 - En el punto 6.13 Medidas de seguridad técnica, numeral 6.13.1 Relacionadas al acceso no autorizado al banco de datos personales, inciso f. Identificación de los accesos realizados a los datos personales para su tratamiento, se detalla los campos mínimos que debe contener el Registro de Accesos a Bancos de Datos Personales.
 - Los 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 que puedan realizarse.
- k. P.A. PERU S.A.C. debe incluir en los planes de Auditoría Interna aplicable al marco de Privacidad en que se revise semestralmente su idoneidad respecto del cumplimiento de la Ley 29733; los hallazgos de las auditorías internas deben ser registrados en el Plan de Acciones Correctivas y de Mejora.

Código:	LE-MN-001	MANUAL	
Versión	01		
Fecha:	28/08/2023	PROTECCIÓN DE DATOS PERSONALES	
Página:	21 de 42		

- I.** El Plan de Auditoría Interna del marco de Privacidad de P.A. PERU S.A.C., debe estar bajo la responsabilidad del Departamento de Tecnología, quien se encargará de todas las gestiones necesarias para que se ejecute.
- m.** Dadas las condiciones internas en el que se cuenta con un enfoque de riesgos de privacidad de datos personales del marco de Privacidad de P.A. PERU S.A.C., se debe incluir lo siguiente para alinear los criterios de evaluación de riesgo de los datos personales:
- Los datos personales se mantienen dentro de medios específicos, que son los bancos de datos personales, los mismos que a su vez son considerados activos de información dentro del marco de Privacidad, y son procesados por sistemas cuando son automatizados o procesados en forma manual cuando son no automatizados, conforme a ello, los bancos de datos personales de P.A. PERU S.A.C. se categorizan de acuerdo con los criterios indicados por la APDP.
 - Se establece que debe considerarse en la evaluación de riesgo de datos personales el análisis de impacto en la privacidad, por lo tanto, deben definirse los criterios correspondientes para su aplicación en todos los casos en que se evalúen riesgos a los bancos de datos personales, estos criterios están dados por la Metodología de Gestión de Riesgos de Privacidad de Datos Personales.
 - El valor de riesgo de privacidad de datos personales, que comprometa a los bancos de datos personales, que se obtenga y que resulten no aceptables, deben ser tratados de acuerdo con lo que establezca el Departamento de Tecnología de P.A. PERU S.A.C., basado en la Metodología de Gestión de Riesgos de Privacidad de Datos Personales en función de las decisiones sobre acciones a tomar que corresponda a cada tipo de riesgo identificado.
- n.** El presente Capítulo del Manual debe ser revisado anualmente y modificado de acuerdo con los resultados específicos de manera que se mantenga su idoneidad con el contexto, las directrices organizacionales y en cumplimiento de la normativa vigente.
- o.** El presente Manual es de responsabilidad del Departamento Legal con soporte del Departamento de Tecnología, y debe ser asimilada en la organización en calidad de guía para la implementación, mantenimiento y mejora del marco de Privacidad para la protección de los datos personales.
- p.** Todo personal de P.A. PERU S.A.C. y terceros que estén relacionados con el tratamiento de datos personales debe firmar un compromiso de confidencialidad en el tratamiento de datos personales en señal de conformidad y aceptación con las condiciones de privacidad con las que se rige la organización. Este acuerdo obliga al personal firmante a guardar la confidencialidad de los datos personales y de sus antecedentes, esta obligación debe subsistir aun después de finalizadas las relaciones con P.A. PERU S.A.C.

El obligado puede ser relevado de la obligación de confidencialidad si se da

Código:	LE-MN-001	MANUAL	
Versión	01		
Fecha:	28/08/2023	PROTECCIÓN DE DATOS PERSONALES	
Página:	22 de 42		

cualquiera de los casos que indica el segundo párrafo del artículo 17 de la Ley N° 29733, Ley de Protección de Datos Personales.

6.10 Disposiciones específicas de seguridad

- a. Para el tratamiento de los bancos de datos personales el Departamento de Tecnología de P.A. PERU S.A.C. se implementará los controles adecuados.
- b. P.A. PERU S.A.C., como titular de banco de datos ha designado en el Capítulo Segundo del presente manual como responsable de seguridad de los bancos de datos personales al Departamento de Tecnología, quien coordinará en la empresa la aplicación de las medidas de seguridad para preservar la privacidad de los bancos de datos personales.
- c. Los registros y documentos que evidencian el cumplimiento o que forman parte de las medidas de seguridad de datos personales que sean implementadas, pueden estar en cualquier formato o tipo de medio de información; siempre de acuerdo con las facilidades técnicas y operativas que se tengan en P.A. PERU S.A.C.
- d. Todos los bancos de datos personales existentes deben ser limitados a los datos que sean estrictamente necesarios para cumplir con la finalidad para la cual fueron recabados.
- e. En todos los casos en los que sea pertinente y no se requiera del detalle de los datos personales, se deben aplicar mecanismos de anonimización o disociación de acuerdo con las facilidades técnicas existentes.


6.11 Medidas de seguridad organizativas

La implementación de las medidas organizativas es de responsabilidad de la Gerencia General que debe aprobar y apoyar la estructura organizacional de la protección de datos personales y en forma operativa es responsabilidad del Departamento Legal que debe disponer de los recursos necesarios para llevar a cabo la implementación y operación del marco de Privacidad.

- a. La estructura organizacional, los roles y responsabilidades respecto de la protección de datos personales, se encuentra establecido en el Capítulo Segundo del presente Manual.

En la estructura organizacional establecida se distinguen los siguientes roles:

- Titular de Datos Personales.
 - Titular del Banco de Datos Personales.
 - Responsable de Tratamiento.
 - Encargado de Tratamiento.
 - Departamento de Tecnología.
 - Departamento de Legal.
- b. En la Política Corporativa de Protección de Datos Personales se establece el compromiso de la Gerencia General y de toda la organización de P.A. PERU S.A.C. con el respeto a los principios rectores de la Ley 29733, Ley de Protección de Datos


Código:	LE-MN-001	MANUAL	
Versión	01		
Fecha:	28/08/2023	PROTECCIÓN DE DATOS PERSONALES	
Página:	23 de 42		

Personales.

La Política Corporativa de Protección de Datos Personales debe estar debidamente entendida y aceptada por todos los trabajadores de P.A. PERU S.A.C.

El Departamento de Recursos Humanos, debe llevar el registro de la entrega y de la aceptación de la Política Corporativa de Protección de Datos Personales y deberá informarlo al Departamento Legal.

- c. El Departamento Legal realizará todos los trámites ante la APDP que correspondan a los bancos de datos de titularidad de P.A. PERU S.A.C. y de atender todas las denuncias que puedan emitir los titulares de datos personales.
- d. Todo banco de datos personales que sea creado en P.A. PERU S.A.C. debe ser autorizado por el Departamento Legal previo visto bueno del Departamento de Tecnología e inscrito ante la Autoridad Nacional de Protección de Datos Personales de manera previa a su puesta en producción y a la recopilación de datos personales.
- e. El Departamento de Tecnología, debe realizar la revisión de los formularios de inscripción de bancos de datos provistos por las Áreas/Departamento de P.A. PERU S.A.C.
- f. Es responsabilidad de cada Área/División, proporcionar al Departamento Legal el formulario de inscripción de bancos de datos personales (Formulario TUPA N° 34 C: Formulario para entidades Privadas) debidamente llenado para su validación, firmado por el Gerente General y la posterior inscripción por parte del Departamento Legal ante la APDP.
- g. La descripción del llenado del formulario de inscripción se encuentra en el Título IV ¿Cómo completar el formulario? de la Guía de Inscripción de Bancos de Datos Personales que se encuentra publicada en la página web del MINJUS:
- h. Los procesos de modificación y cancelación de bancos de datos personales que hayan sido inscritos ante la APDP deben ser reportados por cada Área/Departamento al Departamento Legal a través del llenado de los siguientes formularios publicados en la página web del MINJUS:
 - Formulario de modificación de banco de datos personales:
 - Formulario TUPA N°35: Formulario de modificación del banco de datos.
 - Formulario de cancelación de banco de datos personales:
 - Formulario TUPA N°36: Formulario de cancelación del banco de datos.
- i. El Departamento de TI, debe llevar un control y registro de los trabajadores con acceso a cada banco de datos personales con el objetivo de poder identificarlos ante sucesos que requieran realizar la trazabilidad de las acciones. Este control deberá ser compartido con el Departamento legal a través de una ruta compartida u otra forma segura que considere el Departamento de Tecnología. Dicho control tendrá el siguiente modelo:


Código:	LE-MN-001	MANUAL	
Versión	01		
Fecha:	28/08/2023	PROTECCIÓN DE DATOS PERSONALES	
Página:	24 de 42		

Ítem	Nombre del Colaborador	BDP Autorizado

- j. El Departamento de Tecnología, debe revisar periódicamente la efectividad de las medidas de seguridad adoptadas y registrar los resultados de la verificación en un documento adjunto al banco de datos personales (si es lógico en el servidor y si es físico en el contenedor de documentos). El registro de las revisiones deberá ser compartido con el del registro de resultados.
- k. Se puede adoptar el siguiente modelo para el documento a ser adjuntado al banco de datos personales:


Ítem	BDP	Medida de Seguridad	Fecha de revisión	Nivel de efectividad	Observaciones

- La medida de seguridad debe ser identificada de acuerdo con una bitácora que debemantener y administrar el Departamento de Tecnología.
 - El nivel de efectividad puede ser bajo, medio y alto.
- l. Toda aplicación de tratamiento de datos personales debe ser adaptada mediante la configuración de accesos y perfiles acordes a los cargos, el desarrollo de mecanismos de seguridad en el acceso y en la transferencia de datos personales, esta actividad es responsabilidad del Departamento de Tecnología en conjunto con las Áreas/Departamentos y el responsable de Recursos Humanos de P.A. PERU S.A.C.
- m. Todos los procesos de negocio involucrados en el tratamiento de datos personales deben adecuarse al cumplimiento de la Ley y su reglamento contemplando:
- Implementación de procesos administrativos suficientes, en todas las Áreas/Departamento, para brindar acceso a los derechos ARCO y al derecho de acceso a la información a los titulares de datos personales. En la implementación y operación deben intervenir todas las Áreas/Departamentos de P.A. PERU S.A.C. que procesen solicitudes de los clientes, usuarios de la página web y redes sociales, libro de reclamaciones, trabajadores, practicantes, postulantes, proveedores, clientes, visitantes y video vigilancia.
 - Las siguientes Áreas/Departamento, Responsables de Bancos de Datos Personales, son responsables de adecuar los procesos administrativos de P.A. PERU S.A.C. con la finalidad de atender requerimientos de los titulares de datos personales relacionados a los derechos ARCO (Acceso, Rectificación, Cancelación y Oposición) dicha atención será apoyado por el Departamento Legal:
 - La Dirección Comercial, es el responsable de adecuar los procesos administrativos para el banco de datos de socios y libro de reclamaciones, de ser el caso;
 - El Departamento de Recursos Humanos, es responsable de adecuar los

Código:	LE-MN-001	MANUAL	
Versión	01		
Fecha:	28/08/2023	PROTECCIÓN DE DATOS PERSONALES	
Página:	25 de 42		

procesos administrativos para los bancos de datos personales de trabajadores, practicantes, y postulantes.

- El Departamento de Finanzas, es responsable de adecuar los procesos administrativos para los bancos de datos proveedores y clientes, visitantes y videovigilancia;
 - El Departamento de Marketing, es el responsable de adecuar los procesos administrativos para el banco de datos de usuarios de la página web y redes sociales.
- El Departamento Legal es el responsable de poner a disposición toda la información necesaria, en donde corresponda, para que los titulares de datos personales conozcan el contexto de aplicación de la Ley y su reglamento en P.A. PERU S.A.C.
 - El Departamento de Tecnología, es responsable de adecuar los aplicativos y sistemas de negocio, para que tengan la capacidad de proporcionar las facilidades necesarias en la atención de los derechos ARCO.
 - En complemento al párrafo anterior, se deben establecer los tiempos de atención de los procesos que estén comprendidos en el acceso a los derechos ARCO y el derecho de información por parte de los titulares de datos personales de acuerdo al Procedimiento de Atención de Derechos ARCO, que está alineado con lo estipulado en el Reglamento de la Ley 29733.
 - Es responsabilidad del Departamento de Tecnología, velar por la publicación, en los medios telemáticos de recopilación de datos personales, la Política de Privacidad de forma complementaria, la adopción de un mecanismo de obtención de consentimiento que reúna todas las características establecidas en el reglamento de la Ley.
 - Se debe implementar un canal de autorización de creación de nuevos bancos de datos personales; estos deben ser autorizados por el Departamento Legal, previo a su lanzamiento y a la recopilación de datos personales, este paso previo debe ser conocido por todas las Áreas/Departamentos de PA PERU SAC
 - Todos los trabajadores identificados como responsables de tratamiento y encargados de tratamiento de datos personales, de todos los niveles de la organización y externos que traten datos personales, deben asumir sus responsabilidades respecto de la protección de datos personales, para ello, deben participar activamente en las actividades de capacitación y concienciación de la Ley y su reglamento.
 - Todas las Áreas/Departamentos de P.A. PERU S.A.C. deben tener definidos los procesos de obtención de consentimiento de datos personales al momento de recabarlos en cualquiera de los procesos de P.A. PERU S.A.C., según sea el caso y siempre con la observancia de las características de consentimiento indicadas en el Reglamento de la Ley.
 - Si los datos personales son recogidos en línea a través de redes de

Código:	LE-MN-001	MANUAL	
Versión	01		
Fecha:	28/08/2023	PROTECCIÓN DE DATOS PERSONALES	
Página:	26 de 42		


comunicaciones electrónicas, se debe publicar la Política de Privacidad, que debe ser fácilmente accesible e identificable por los usuarios, esto sin perjuicio de la obtención obligatoria del consentimiento de tratamiento de datos personales.

- n. Todas las áreas/departamentos de P.A. PERU S.A.C. tendrán a disposición el procedimiento para el tratamiento de datos personales.
- o. El Departamento de Tecnología con apoyo del Departamento de Recursos Humanos, son responsables de elaborar el programa de creación de conciencia y entrenamiento en materia de protección de datos personales.
- p. P.A. PERU S.A.C. ejecutará auditorías internas con una periodicidad semestral, contemplando en su alcance a los bancos de datos personales y las medidas de seguridad de la Directiva de Seguridad de la Información de la Ley y su reglamento.
- q. El Departamento de TI a tiene un procedimiento para la atención de incidentes y problemas que debe ser aplicable a todo incidente que afecte la confidencialidad, integridad y disponibilidad de los bancos de datos personales, este procedimiento interno debe ser de aplicación permanente por parte de todos los trabajadores de P.A. PERU S.A.C. y del propio Departamento de Tecnología. Este tipo de atención serán prioritarias las cuales se registrarán en el reporte de incidentes de seguridad.
- r. La asignación de privilegios de acceso a los aplicativos de P.A. PERU S.A.C., en los que se tratan datos personales lo administra el Departamento de Tecnología.

6.12 Medidas de seguridad jurídicas

La implementación de las medidas Jurídicas, son de responsabilidad exclusiva del Departamento Legal, por lo que ésta última, debe disponer de los recursos necesarios para su cumplimiento.

- a. Todas las Áreas/Departamentos tendrán los formatos de consentimiento por cada banco de datos personales que se tenga en P.A. PERU S.A.C. y que estén de acuerdo con la finalidad de la recopilación de los datos personales, estos formatos deben contener desarrolladas las características de consentimiento de ser libre, previo, expreso, inequívoco e informado que pide la Ley y su reglamento.
- b. Las Gerencias/jefes de las Áreas/Departamento como responsable de tratamiento de datos personales deben valerse del apoyo del Departamento Legal para elaborar y mantener sus formatos de consentimiento adecuados de manera específica para los bancos de datos que tratan en sus procesos de recopilación de datos personales.
- c. El Departamento Legal, debe asistir al Departamento de Recursos Humanos, en la elaboración de los contratos de colaboradores, en especial para aquellos que estén destinados a ocupar cargos relacionados con el tratamiento de datos personales, que contemple cláusulas de compromiso y/o acuerdo con la protección de datos personales y las medidas disciplinarias que correspondan y a los que se rige todo trabajador, a través de la comprensión y aceptación del Reglamento Interno de Trabajo (RIT) de P.A. PERU S.A.C.

Código:	LE-MN-001	MANUAL	
Versión	01		
Fecha:	28/08/2023	PROTECCIÓN DE DATOS PERSONALES	
Página:	27 de 42		

- d. En forma seguida, el Departamento de Recursos Humanos, debe recabar la firma del acuerdo de confidencialidad en el tratamiento de datos personales cuyo tenor debe estar acorde a la obligación de guardar confidencialidad respecto de los bancos de datos personales y de sus antecedentes. El documento debe dejar en claro que la obligación subsiste aún después de finalizada la relación contractual con P.A. PERU S.A.C. avalado por el Artículo 17 de la Ley.
- e. Al igual que con los contratos de los trabajadores, el Departamento Legal, debe asistir a las distintas Áreas/Departamentos en la elaboración de los contratos para la contratación de proveedores y/o terceros que contemple cláusulas de compromiso con la protección de datos personales, con la confidencialidad de los datos personales, sus antecedentes y las medidas correctivas que correspondan de acuerdo con las leyes vigentes.
- f. Debe regir así mismo en los contratos con proveedores y/o terceros que la obligación de mantener la confidencialidad sobre los datos personales subsiste aún después de finalizada la relación contractual con P.A. PERU S.A.C. avalado por el Artículo 17 de la Ley.

6.13 Medidas de seguridad técnicas


6.13.1 Relacionadas al acceso no autorizado al banco de datos personales

a. Gestión y uso de contraseñas cuando el tratamiento se realice con medios informáticos

Mediante los lineamientos dado por el Departamento de Tecnología referida seguridad de la información y administración de cuentas de usuario se controla la asignación y el uso de las contraseñas de los usuarios de los sistemas de información incluyendo aquellos que realizan tratamiento de datos personales y las responsabilidades de los usuarios respecto de sus contraseñas.

En forma complementaria se deben considerar los siguientes lineamientos para la protección de los datos personales que se tratan en los sistemas:

- Las contraseñas de acceso a los sistemas operativos y aplicaciones de negocio deben ser creadas contemplando las condiciones dadas por el Departamento de Tecnología referida a la seguridad de la información (autenticación de usuarios).
- Las sesiones de usuario del sistema operativo y de los aplicativos de negocio deben estar configurados para que se bloqueen luego de tres (03) intentos fallidos de autenticación consecutivos.
- Complementariamente a estas medidas mínimas referidas a la gestión de accesos, se deben aplicar, a la protección de datos personales, las medidas en control de acceso implementadas por el Departamento de Tecnología referida a seguridad de la información.

Código:	LE-MN-001	MANUAL	
Versión	01		
Fecha:	28/08/2023	PROTECCIÓN DE DATOS PERSONALES	
Página:	28 de 42		

b. Revisión y registro de los perfiles de acceso:

El Departamento de Tecnología es responsable de efectuar la revisión de perfiles de acceso a los aplicativos que procesan datos personales que correspondan al personal autorizado; esta revisión debe ser realizada con una periodicidad semestral programada y en forma aleatoria.

Producto de la revisión de los perfiles de acceso a los aplicativos se debe generar un registro de revisión que evidencie su realización, este registro debe ser mantenido por el Departamento de TI e informado al Departamento Legal.

El registro tendrá el siguiente modelo:


Ítem	Usuario	Privilegios de acceso	Observaciones	Fecha de revisión

La revisión de los privilegios de acceso de los usuarios debe ser realizada versus una base de referencia, para lo cual maneja una Matriz de Perfiles y Privilegios de Acceso a los Sistemas y Servicios de TI que debe estar alineada a las funciones del cargo del usuario en concordancia con la versión vigente del Manual de Organización y Funciones (MOF) de P.A. PERU S.A.C.

El Departamento de Tecnología, debe mantener plenamente identificados a los responsables y encargados de tratamiento y los privilegios de acceso asignados.

c. Protección del banco de datos personales contra acceso físico no autorizado

- Las medidas de acceso físico a la información y en particular a los bancos de datos personales se rigen conforme a los lineamientos dado por el Departamento de Tecnología referido a seguridad de la información.
- Departamento de Tecnología, debe velar por que cada una de las Divisiones conserve los bancos de datos personales físicos en ambientes seguros a los que sólo personal autorizado pueda acceder.
- La responsabilidad de mantener el mecanismo de seguridad del ambiente es de cada responsable de tratamiento de datos personales de acuerdo con el Área/Departamento y la ubicación en la que el banco de datos físico se encuentre.
- Los ambientes aislados en los que se encuentren los bancos de datos físicos deben ser solo de acceso estricto y autorizado del responsable de tratamiento y de los encargados de tratamiento, quienes además deben encontrarse debidamente identificados.
- Si por tareas de revisión o auditoría, sea requerido el acceso de personal ajeno a los procesos y al tratamiento de los datos personales en bancos de datos físicos, el responsable de tratamiento o a quien este designe debe autorizarlo y debe mantenerse vigilante del accionar de los visitantes, asimismo, deberá poner en conocimiento al Departamento Legal.
- El responsable de tratamiento debe llevar el correspondiente registro de acceso autorizado a los bancos de datos personales que se encuentren en forma física.

Código:	LE-MN-001	MANUAL	
Versión	01		
Fecha:	28/08/2023	PROTECCIÓN DE DATOS PERSONALES	
Página:	29 de 42		

d. Protección del banco de datos personales contra acceso lógico no autorizado

- El Departamento de TI, debe velar, mantener protegido y limitado el acceso a los sistemas informáticos, solo a los involucrados en el tratamiento de datos personales debidamente autorizados.
- La Departamento de TI, debe garantizar el cumplimiento de las políticas de control de accesos referidas seguridad de la información y en forma particular a aquellos lineamientos referidos que garanticen:
 - Que todos los usuarios de los sistemas informáticos tengan un identificador único de acceso asociado a perfiles de usuarios y los accesos autorizados para cada uno de estos perfiles.
 - Que los sistemas informáticos cuenten con mecanismos de restricción de acceso a recursos del sistema no autorizados.
 - Que se establezcan el acceso a través de cuentas de usuario y contraseñas a todos los aplicativos.

e. Autorización de acceso a los bancos de datos personales

Los responsables de tratamiento de los bancos de datos personales son los designados por P.A. PERU S.A.C. como titular del banco de datos personales, para autorizar o retirar el acceso, de los encargados de tratamiento, a los bancos de datos personales de los procesos en los que sean partícipes.

El Departamento de TI, debe mantener el registro de las autorizaciones de acceso a los bancos de datos personales, contenidos en los sistemas informáticos, brindados por los responsables de tratamiento a los encargados de tratamiento.

Es obligatorio que como mínimo este registro contenga:


- Identificador de usuario.
- Fecha y hora de asignación y/o retiro de autorización del usuario.
- Responsable de tratamiento que autoriza.
- Responsable de atención de requerimientos de acceso.

Toda autorización de acceso a los sistemas debe ser dada en función del cargo que ocupe cada encargado de tratamiento de datos personales.

f. Identificación de los accesos realizados a los datos personales para su tratamiento

El Departamento de TI, debe implementar y mantener el registro de accesos a Bancos de Datos Personales, el cual debe contener al menos los siguientes campos:

- Cuenta de usuario con acceso al sistema.

Código:	LE-MN-001	MANUAL	
Versión	01		
Fecha:	28/08/2023	PROTECCIÓN DE DATOS PERSONALES	
Página:	30 de 42		

- Fecha y hora de inicio y cierre de sesión.
- Nombres y apellidos de la persona o personas quienes realizan el acceso.
- Identificador del titular de los datos personales a tratar (mediante mecanismo dedisociación aplicado).
- Motivo del acceso.
- Acciones relevantes (consulta, registro, modificación, supresión, transacciones).

6.13.2 Relacionadas a la alteración no autorizada del banco de datos personales

a. Autorización para el retiro o traslado de datos personales

Todo traslado de datos personales contenidos en soportes físicos o lógicos hacia lugares fuera de los ambientes en donde se ubica el banco de datos personales debe contar con la autorización del Departamento Legal previa validación del Departamento de Tecnología.

Es obligación de los responsables de tratamiento informar al Departamento Legal sobre el traslado de datos personales fuera de los ambientes donde se ubica el banco de datos personales, contemplando como mínimo la siguiente información:

- Origen.
- Motivo del traslado.
- Finalidad del traslado.
- Responsable del traslado.
- Destino.
- Así mismo, el responsable de tratamiento debe mantener un registro trazable del traslado, que contenga como mínimo:
 - Banco de datos al que pertenecen los datos personales.
 - Responsable del traslado.
 - Fecha y hora de traslado.


Si el retiro del medio informático es definitivo por obsolescencia o renovación de equipos, se debe ejecutar el borrado seguro, previo respaldo, de la información y de los datos personales que pudiera tener almacenado.

b. Traslado de datos personales

- Las medidas de seguridad para los datos personales que son trasladados en soporte físico deben realizarse de acuerdo con las directivas dadas por el Departamento de Tecnología referida a retiro o traslado de Datos Personales.
- Se restringe el traslado de información personal en soportes informático, siendo posible únicamente si se realiza el encriptamiento de la información y se utiliza un mecanismo de verificación de la integridad.

c. Eliminación de la información contenida en medios informáticos removibles

- Cuando se requiera eliminar la información contenida en un medio informático removible (USB, disco duro externo, CD) se deben utilizar mecanismos seguros de eliminación que incluyan el borrado total de la información y/o la destrucción del medio; de forma tal que, no sea posible la recuperación de los datos; para ello las Áreas/Departamentos de P.A. PERU S.A.C. se deben valer del apoyo del


Código:	LE-MN-001	MANUAL	
Versión	01		
Fecha:	28/08/2023	PROTECCIÓN DE DATOS PERSONALES	
Página:	31 de 42		

Departamento de TI.

- La eliminación o borrado de datos personales contenidos en medios informáticos removibles de almacenamiento de P.A. PERU S.A.C., debe ser realizada con autorización de los responsables de Tratamiento del banco de datos personales a los Encargados de Tratamiento. El responsable de Tratamiento se apoyará con del Departamento Legal contará con un listado de encargados de tratamiento autorizados a realizar la eliminación segura de la información.
- El responsable de Tratamiento, debe mantener un registro de eliminación de datos personales contenidos en medios removibles de almacenamiento, este registro debe contener en forma mínima.
 - Banco de datos al que corresponde la información a eliminar.
 - Nombres y apellidos de la persona que autoriza la eliminación.
 - Nombres y apellidos de la persona que elimina la información.
 - Registro de la serie/descripción del medio removible del cual es borrada la información.
 - Fecha y hora de la eliminación.
 - Motivo de la eliminación.
- Cuando se proceda a eliminar información personal de medios removibles de almacenamiento, los encargados de tratamiento deben notificar al Departamento Legal y Departamento de Tecnología, quien a su vez deben garantizar que la información sea eliminada en forma segura.
- Ningún medio removible de almacenamiento que contenga datos personales debe salir de las instalaciones de P.A. PERU S.A.C. sin autorización del Departamento Legal y Departamento de Tecnología, y sin haber sido autorizado su traslado ni empleados mecanismos de encriptación y validación de integridad.

d. Seguridad en la copia o reproducción de documentos

- Todas las Áreas/Departamentos de P.A. PERU S.A.C., deben contar con Encargados de Tratamiento autorizados a generar y/o eliminar las copias o reproducciones de los datos personales; por lo que el responsable de Tratamiento debe designarlos y mantener un listado de ellos.
- Se deben implementar las siguientes medidas para preservar la confidencialidad de los datos personales que van a ser reproducidos.
- Utilizar impresoras, fotocopiadoras, scanner u otros equipos de reproducción autorizados que incluyan mecanismos de seguridad y control que permitan trazar las actividades de reproducción.
 - Todo Encargado de Tratamiento, es responsable de supervisar el procesode copia o reproducción de los documentos. No se debe dejar desatendidoel equipo.
 - Los Encargados de Tratamiento deben retirar los documentos originales y las copias del equipo inmediatamente después de finalizada la copia o reproducción.
 - El Departamento de Tecnología con apoyo del Departamento Legal

Código:	LE-MN-001	MANUAL	
Versión	01		
Fecha:	28/08/2023	PROTECCIÓN DE DATOS PERSONALES	
Página:	32 de 42		

debe promover campañas de concientización respecto a la seguridad en las actividades de copia y reproducción de medios que contengan datos personales.

e. Autorización de Perfiles de Acceso a bancos de datos personales


El responsable de Tratamiento, debe asignar o retirar perfiles a los usuarios con acceso a los datos personales contenidos en el banco de datos personales. Dicha operación debe ser registrada. Los datos para registrar deben incluir como mínimo:

- Usuario (en sistemas informáticos el identificador de usuario)
- Privilegio asignado o retirado al perfil.
- Fecha y hora de asignación y/o retiro de perfiles del usuario.
- Usuario que realiza la asignación y/o retiro de privilegios (en sistemas informáticos el identificador de usuario).

6.13.3 Relacionadas a la pérdida del banco de datos personales

a. Copias de Respaldo

- El proceso de realización de copias de respaldo se rige de acuerdo con los lineamientos dados por el Departamento de Tecnología referido a seguridad de la información.
- Se deben realizar copias de respaldo de los datos personales para permitir su recuperación en caso de pérdida o destrucción.
- Toda copia de respaldo de los datos personales debe estar protegida mediante técnicas de cifrado y almacenada en un local seguro y distante al ambiente principal de tratamiento de datos, para garantizar su disponibilidad frente a un desastre en el ambiente principal.
- La frecuencia de realización de las copias de respaldo y su periodo de conservación deben ser acordes con la finalidad del tratamiento a realizar y el impacto de la pérdida en los derechos del titular de los datos personales; la finalidad de tratamiento es definida por el responsable de Tratamiento, por lo tanto, es a su vez, responsable de brindar estos parámetros al Departamento de Tecnología.
- El Departamento de Tecnología es responsable de establecer lineamientos de la mano con mecanismos de seguridad que garanticen la continuidad del tratamiento de los datos personales.
- Toda recuperación de datos personales, desde su copia de respaldo, debe contar con la autorización del responsable de Tratamiento de datos personales y el Departamento de Tecnología.
- El Departamento de Tecnología debe realizar pruebas de integridad y de recuperación de los datos personales respaldados para comprobar que las copias de respaldo pueden ser utilizadas en caso de ser requerido.
- Estas pruebas deben realizarse en forma trimestral y se debe mantener el registro de los resultados incluyendo:
 - Fecha y hora de la prueba.
 - Nombre de la persona que realizó la prueba.
 - Banco de datos personales recuperado.
 - Archivo recuperado y fecha de los datos recuperados.
 - Tiempo de recuperación.

Código:	LE-MN-001	MANUAL	
Versión	01		
Fecha:	28/08/2023	PROTECCIÓN DE DATOS PERSONALES	
Página:	33 de 42		

- Resultados de las pruebas.
- Acciones tomadas en caso de pruebas insatisfactorias.

Este registro debe ser mantenido por el Departamento de Tecnología e informado al Departamento Legal.

6.13.4 Relacionadas al tratamiento no autorizado del banco de datos personales

a. Medidas Generales

- Todas las Áreas/Departamentos de P.A. PERU S.A.C., en la que se traten datos personales y que cuenten con bancos de datos físicos, deben tenerlos independizados e individualizados por cada titular de datos personales sin exponer información de otro; es responsabilidad del Departamento de Tecnología y Departamento Legal implementar estas medidas en sus procesos.
- El Departamento de Tecnología, es responsable de adecuar los procesos administrativos en los que se de atención a los socios con la finalidad de comunicarles de manera oportuna, como titulares de datos personales, sobre los incidentes que afecten significativamente sus derechos patrimoniales o morales.

b. El informe de incidentes al titular de datos personales debe contener en forma mínima la siguiente información:

- Naturaleza del incidente.
- Datos personales comprometidos.
- Recomendaciones al titular de datos personales.
- Medidas correctivas implementadas.

c. Medidas Específicas

I. Mantenimiento de equipos utilizados para el tratamiento de datos personales


Es responsabilidad de cada Área/Departamento en la que se traten datos personales, reportar al Departamento de Tecnología, la identificación de equipos en los que se tratan datos personales.

El Departamento de Tecnología es responsable de gestionar con los proveedores el mantenimiento preventivo y correctivo de los equipos utilizados para el tratamiento de los datos personales.

Los proveedores de los equipos de cómputo y periféricos deben realizar el mantenimiento preventivo y correctivo de los equipos en forma acorde a las recomendaciones y especificaciones del fabricante para asegurar su disponibilidad e integridad.

El Departamento de Tecnología es responsable de desarrollar el plan de mantenimiento anual de equipos en forma coordinada con los proveedores.

El Departamento de Tecnología es responsable de generar y mantener

Código:	LE-MN-001	MANUAL	
Versión	01		
Fecha:	28/08/2023	PROTECCIÓN DE DATOS PERSONALES	
Página:	34 de 42		

el registro de la realización del mantenimiento preventivo y/o correctivo. Dichas rutinas de mantenimiento de equipos son autorizadas por el mismo Departamento.

II. Protección contra software malicioso

Los equipos utilizados para el tratamiento de los datos personales deben contar con software de protección contra software malicioso (virus, troyanos, spyware, etc.), para proteger la integridad de los datos personales. El software de protección debe ser actualizado frecuentemente de acuerdo con las recomendaciones y especificaciones del proveedor.

III. Almacenamiento seguro de la información personal

Toda información electrónica que contenga datos personales debe ser almacenada en forma segura empleando mecanismos de control de acceso y cifrada para preservar su confidencialidad.

En el caso de los sistemas informáticos, el Departamento de Tecnología, debe aplicar las medidas de control de acceso y cifrado a las bases de datos que contengan datos personales.

Para el caso de archivos de ofimática que contengan datos personales, los encargados de tratamiento son responsables de cifrar la información mediante una contraseña de apertura.

IV. Seguridad en la transmisión electrónica de datos personales


La información de datos personales que se transmite electrónicamente debe ser protegida para preservar su confidencialidad e integridad.

Es imprescindible que se valide la identidad de quien emita datos personales hacia P.A. PERU S.A.C., para lo cual se deben implementar los mecanismos de autenticación correspondientes.

V. Seguridad en servicios de tratamiento de datos personales por medios tecnológicos tercerizados

Para que sea posible que P.A. PERU S.A.C. contrate servicios de tratamiento de datos personales por medios tecnológicos tercerizados, el Departamento de Tecnología debe velar por el cumplimiento tajante de las siguientes condiciones:

- Que el proveedor no tenga acceso a la información de datos personales que utilicen su infraestructura.
- Que el proveedor no brinde acceso a terceros a los datos personales que utilicen su infraestructura.
- La destrucción o imposibilidad de recuperación de los datos alojados en el servicio una vez concluida la relación con el proveedor.
- Uso de canales seguros para la transferencia de datos personales.
- Garantizar el cumplimiento de las medidas de seguridad en todos los lugares en donde se encuentre distribuida la infraestructura del proveedor.

Código:	LE-MN-001	MANUAL	
Versión	01		
Fecha:	28/08/2023	PROTECCIÓN DE DATOS PERSONALES	
Página:	35 de 42		

Todos estos aspectos técnicos, deben estar debidamente incorporados en los términos y condiciones contractuales, en la que se debe incluir además la potestad de realizar revisiones de cumplimiento en forma inopinada de cada aspecto cubierto por el servicio.

VI. Gestión de incidentes de seguridad de los datos personales

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 responsable de Tratamiento.

El responsable de Tratamiento o quien sea designado debe coordinar las acciones requeridas para analizar y responder en forma rápida y efectiva a los incidentes de seguridad presentados.

Se deben registrar los incidentes de seguridad relacionados con los bancos de datos personales, incluyendo como mínimo:


- Fecha y hora del incidente.
- Nombre de la persona que lo reporta.
- Naturaleza del incidente.
- Datos personales comprometidos.
- Nombres de las personas involucradas en la resolución del incidente.
- Consecuencias del incidente.
- Medidas correctivas implementadas.
- Recomendaciones para el titular de datos personales. (Si aplica).
- Recuperación de datos.
- En caso de haber realizado recuperación de datos, se debe registrar:
 - Nombre de la persona que realizó la recuperación.
 - Descripción y fecha de los datos restaurados.
 - Descripción de los datos restaurados en forma manual. (Si aplica).

VII. Restricción uso de equipos de video, fotografía y audio

P.A. PERU S.A.C., como titular de banco de datos personales, restringe el uso de equipos de fotografía, video, audio u otra forma de registro en todas aquellas Áreas/Departamentos en las que se realice el tratamiento de datos personales salvo aviso expreso del Departamento Legal vía correo electrónico incluyendo la autorización del Gerente General.

Las solicitudes de autorización deben ser canalizadas por correo electrónico por el responsable de Tratamiento al Departamento Legal y con copia al Departamento de Tecnología; así mismo, las autorizaciones deben ser canalizadas por el mismo medio por el Gerente General.

De darse el caso de ser autorizado por el Titular del Banco de Datos Personales (Gerente General de P.A. PERU S.A.C.,) se debe mantener como registro de su realización, los correos electrónicos de solicitud

Código:	LE-MN-001	MANUAL	
Versión	01		
Fecha:	28/08/2023	PROTECCIÓN DE DATOS PERSONALES	
Página:	36 de 42		

y autorización, los cuales quedan bajo responsabilidad del Departamento Legal quien debe recopilarlos.

VIII. Auditoría de seguridad de datos personales

Las auditorías internas y externas de seguridad de datos personales, se rige por los lineamientos y actividades establecidas por la Norma ISO/IEC 27001.

Es responsabilidad del Titular del Banco de Datos Personales, realizar una auditoría externa para la verificación del cumplimiento de la Directiva de Seguridad de la Información de la Ley y su reglamento, a fin de asegurar imparcialidad en los resultados.

Para el caso de la auditoría al marco de Privacidad, se tomará como referencia el cumplimiento de las medidas de seguridad indicados en la Directiva de Seguridad de la Información de la Ley 29733.

Las competencias exigibles a los auditores es la de tener certificación de haber participado en auditorías a sistemas de gestión de seguridad de la información basados en la Norma ISO/IEC 27001.

IX. Acciones correctivas y mejora continua

Es responsabilidad de los Departamentos de Tecnología y Legal asegurar que la protección de datos personales siga el orden del cumplimiento de la Ley 29733, Ley de Protección de Datos Personales por medio de mantenimiento del marco de Privacidad dentro un ciclo de mejora continua.

Toda desviación al cumplimiento de la Ley y su reglamento debe ser corregida mediante acciones correctivas emprendidas por los mismos responsables y encargados de tratamiento y con el apoyo de los Departamentos de Tecnología y Legal, éste último tiene la obligación de brindar soporte permanente.

d. Disposiciones complementarias a las medidas de seguridad.


P.A. PERU S.A.C., a través del Departamento de Legal y con el apoyo del Departamento de Recursos Humanos debe desarrollar programas informativos dirigido a titulares de datos personales sobre "consentimiento", "derechos del titular de datos personales" y "finalidad"

Estos programas de difusión en información, debe ser realizado dentro del ámbito que le corresponde a P.A. PERU S.A.C.

P.A. PERU S.A.C., a través del Departamento de Tecnología, debe asegurar y mantener los mecanismos de auditoría, verificación y toma de decisiones de cumplimiento con el tratamiento de datos personales realizados en bancos de datos de terceros que sean contratados, los sistemas de identidad de personas, entre otros.

6.14 Medios validos de obtención del consentimiento

Entre los mecanismos válidos para la obtención del consentimiento conforme con establecido en la Ley y el Reglamento, P.A. PERU S.A.C., podrá utilizar los siguientes:

Código:	LE-MN-001	MANUAL	
Versión	01		
Fecha:	28/08/2023	PROTECCIÓN DE DATOS PERSONALES	
Página:	37 de 42		

- a. **Consentimiento Escrito:** Se considera consentimiento escrito a aquél que otorga el titular mediante un documento con su firma autógrafa, huella dactilar o cualquier otro mecanismo autorizado por el ordenamiento jurídico que queda o pueda ser impreso en una superficie de papel o similar. La condición de expreso no se limita a la manifestación verbal o escrita.
- b. **Consentimiento Oral:** Se considera que el consentimiento expreso se otorgó verbalmente cuando el titular lo exterioriza oralmente de manera presencial o mediante el uso de cualquier tecnología que permita la interlocución oral.
- c. **Consentimiento por Acción Propia:** Se considerará consentimiento expreso a aquel que se manifieste mediante la conducta del titular que evidencie que ha consentido inequívocamente, dado que de lo contrario su conducta, necesariamente, hubiera sido otra.
- d. **Consentimiento en Entorno Digital:** Se considera expresa la manifestación consistente en “hacer clic”, “clickear” o “pinchar”, “dar un toque”, “touch” o “pad” u otros similares. En este contexto el consentimiento escrito podrá otorgarse mediante firma electrónica, mediante escritura que quede grabada, de forma tal que pueda ser leída e impresa, o que por cualquier otro mecanismo o procedimiento establecido permita identificar al titular y recabar su consentimiento, a través de texto escrito.
- e. **Consentimiento mediante Texto Preestablecido:** El cual deberá ser fácilmente visible, legible y en lenguaje sencillo, que el titular pueda hacer suyo, o no, mediante una respuesta escrita, gráfica o mediante clic o pinchado.

6.15 Confidencialidad de datos personales


El responsable del banco de datos personales, el encargado del tratamiento de datos personales y quienes intervengan en cualquier parte de su tratamiento están obligados a guardar confidencialidad respecto de estos y de sus antecedentes.

Esta obligación subsiste aun después de finalizadas las relaciones con el Titular del Banco de Datos Personales.

6.16 Limitaciones al consentimiento para el tratamiento de datos personales

Se establece como limitaciones al consentimiento para el tratamiento de datos personales, las siguientes situaciones:

- a. Cuando se trate de datos personales contenidos o destinados a ser contenidos en fuentes accesibles para el público.
- b. Cuando se trate de datos personales relativos a la solvencia patrimonial y de crédito, conforme a ley.
- c. Cuando los datos personales sean necesarios para la ejecución de una relación contractual en la que el titular de datos personales sea parte, o cuando se trate de datos personales que deriven de una relación científica o profesional del titular y sean necesarios para su desarrollo o cumplimiento.
- d. Cuando se hubiera aplicado un procedimiento de anonimización o disociación.

Código:	LE-MN-001	MANUAL	
Versión	01		
Fecha:	28/08/2023	PROTECCIÓN DE DATOS PERSONALES	
Página:	38 de 42		

- e. Cuando el tratamiento de los datos personales sea necesario para salvaguardar intereses legítimos del titular de datos personales por parte del titular de datos personales o por el encargado de datos personales.
- f. Otros establecidos por ley, o por el reglamento otorgado de conformidad con la presente Ley.

6.17 Tratamiento de datos personales

El consentimiento otorgado por el Titular de Datos Personales autoriza a P.A. PERU S.A.C., a realizar cualquier operación o procedimiento técnico, automatizado o no automatizado, 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.

7. RECURSOS UTILIZADOS

7.1. HUMANO-COMPETENCIAS

- Gerente General de la empresa
- Área de Recursos Humanos
- Área Legal
- Área de T.I

7.2. FÍSICOS

- Oficina dotada de dispositivos electrónico entre computadoras, laptops, teléfonos y elementos de oficina.
- Archiveros físicos para el correspondiente almacenamiento de los registros.

7.3. SOFTWARE

- Medios de comunicación: correo electrónico, redes sociales, plataformas de videollamadas, entre otros.
- Acceso a Internet.


8. REGISTROS

No aplica

9. ANEXOS


ANEXO N° 1: BANCO DE DATOS DECLARADOS A LA AUTORIDAD NACIONAL DE PROTECCIÓN DE DATOS PERSONALES

Nombre de Banco de Datos Personales	Tipos de Datos Personales	Finalidad	Área Responsable de Tratamiento de Datos Personales
Banco de datos Videovigilancia	Datos de carácter identificativo: Imagen Datos sensibles: características físicas	Identificar clientes, no clientes y transacciones realizadas en las instalaciones de P.A.	Gerente de TI.

Código:	LE-MN-001	MANUAL	
Versión	01		
Fecha:	28/08/2023	PROTECCIÓN DE DATOS PERSONALES	
Página:	39 de 42		


		PERU S.A.C. relacionados a temas básicos de la seguridad de la empresa.	
Banco de Datos de Quejas - Reclamos	Datos de carácter identificativo: Nombres y apellidos, N° DNI, N° RUC, dirección de domicilio, teléfono, dirección de correo electrónico, N° de Pasaporte, N° de carné de extranjería. Datos de características personales: Fecha de nacimiento, nacionalidad. Datos económicos – financieros y de seguros: Créditos, préstamos, avales, datos bancarios, historial de créditos, deudas.	Recopilar información de los clientes para el registro, seguimiento y respuesta de reclamos presentados y reportarlos a los órganos reguladores como la SBS, INDECOPI, etc.	Gerencia Legal.
Banco de Datos de Clientes	Datos de carácter identificativo: Nombres y apellidos, N° DNI, N° RUC, dirección de domicilio, teléfono, dirección de correo electrónico. Datos de características personales: Fecha de nacimiento, nacionalidad.	Recopilar información de clientes para enviarles publicidad o propuestas de productos.	Gerente de Marketing

Nombre de Banco de Datos Personales	Tipos de Datos Personales	Finalidad	Área Responsable de Tratamiento de Datos Personales
Banco de Datos- Proveedores	Datos de carácter identificativo: Nombres y apellidos, N° DNI, dirección del domicilio, teléfono, imagen, firma. Datos de características personales: Estado civil, fecha de nacimiento, nacionalidad, sexo, profesión, edad, antecedentes penales y policiales. Datos económicos – financieros y de seguros: Créditos, préstamos, avales, datos bancarios, historial de créditos, bienes patrimoniales, beneficios recibidos de programas sociales, deudas.	Recopilar información de los clientes para el registro correspondiente	Gerente TI.

Código:	LE-MN-001	MANUAL	
Versión	01		
Fecha:	28/08/2023	PROTECCIÓN DE DATOS PERSONALES	
Página:	40 de 42		

Banco de Datos - Trabajadores	<p>Datos de carácter identificativo: Nombres y Apellidos, N° DNI, N° Pasaporte, dirección de domicilio, teléfono, dirección de correo electrónico, imagen.</p> <p>Datos de características personales: Estado civil, fecha de nacimiento, nacionalidad, sexo, profesión, edad.</p> <p>Datos económicos – financieros y de seguros: Datos bancarios, seguros, planes de pensiones/jubilación.</p> <p>Datos Sensibles: Origenético, ingresos económicos, convicciones religiosas. Datos de exámenes médicos.</p>	<p>Mantenimiento y actualización de datos de los trabajadores, generación de planilla y liquidaciones, generación de reportes a nivel interno y externo, generación del T-Registro y PLAME, control de contratos y convenios, controles de posiciones en el organigrama, generación de reportes.</p>	Departamento de Recursos Humanos
--	--	--	----------------------------------


Nombre de Banco de Datos Personales	Tipos de Datos Personales	Finalidad	Área Responsable de Tratamiento de Datos Personales
Banco de Datos Clientes - Persona Natural	<p>Datos de carácter identificativo: Nombres y apellidos, N° DNI, N° RUC, N° Pasaporte, dirección de domicilio, teléfono, dirección de correo electrónico, voz, firma, firma electrónica. Datos de características personales: Estado civil, fecha de nacimiento, nacionalidad, sexo, profesión, edad.</p> <p>Datos económicos – financieros y de seguros: Créditos, préstamos, avales, datos bancarios, historial de créditos, tarjetas de crédito, bienes patrimoniales, hipotecas, deudas.</p> <p>Datos de carácter social: Características de vivienda.</p> <p>Datos sensibles: Ingresos económicos, huella digital.</p>	<p>Administra la información de las personas naturales que son clientes de P.A. PERU S.A.C</p> <p>Utilizar los datos para las operaciones que demanden los productos que han contratado el cliente.</p>	Gerente de DN, Marketing y Comunicaciones
	<p>Datos de carácter identificativo: Nombres y apellidos, N° DNI, N° RUC, N° de Pasaporte, dirección de domicilio, teléfono, dirección de correo electrónico, imagen, voz, firma.</p> <p>Datos de características personales: Estado civil, fecha de nacimiento, nacionalidad, sexo,</p>	<p>Identificar a los prospectos a clientes interesados en contratar los servicios de P.A. PERU S.A.C. Generar base de datos con información de</p>	

Código:	LE-MN-001	MANUAL	
Versión	01		
Fecha:	28/08/2023	PROTECCIÓN DE DATOS PERSONALES	
Página:	41 de 42		

Prospectos de Clientes	<p>profesión, edad.</p> <p>Datos económicos – financieros y de seguros: Créditos, préstamos, avales, datos bancarios, historial de créditos, información tributaria, seguros, tarjetas de crédito, bienes patrimoniales, hipotecas, deudas.</p> <p>Datos de carácter social: Pertenencia a clubes o asociaciones, aficiones y hábitos personales, características de vivienda.</p> <p>Datos sensibles: Ingresos económicos.</p>	<p>prospectos a clientes para ofrecer servicios de P.A. PERU S.A.C.</p> <p>Administrar la información de las personas naturales que son prospectos de P.A. PERU S.A.C.</p> <p>Ofrecer productos y/o servicios de empresas terceras o vinculadas.</p>	Gerente TI.
-------------------------------	---	--	-------------

ANEXO N° 2: MATRIZ DE CATEGORÍAS DE LOS DATOS PERSONALES

Criterio	Básico	Simple	Intermedio	Complejo	Critico
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 100	Indeterminado	Indeterminado
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
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
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
Tipo de Titular de banco de datos personales: persona natural. (Criterio utilizado para determinar el tipo entre básico e intermedio).	Aplica	Aplica	Aplica	No aplica	No aplica
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

Código:	LE-MN-001	MANUAL	
Versión	01		
Fecha:	28/08/2023	PROTECCIÓN DE DATOS PERSONALES	
Página:	42 de 42		

Criterio	Básico	Simple	Intermedio	Complejo	Crítico
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
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

10. CONTROL DE CAMBIOS

Versión	Fecha	Descripción del cambio
01	28/08/2023	Creación del documento