- ***Tecnisegur Uruguay S.A. comprometida con la seguridad de la información personal de sus partes interesadas, Clientes, Proveedores, Empleados, y con la finalidad de dar estricto cumplimiento a la normativa vigente sobre la protección de Datos Personales, en especial por lo establecido en la Ley 18.331 de Protección de Datos Personales, y Acción de Habeas Data, de 11 de agosto de 2008 (LPDP), y decreto reglamentario 414/2009 de 31 de agosto de 2009 y demás disposiciones que las modifiquen, adicionen o complementen; se permiten presentar la Política de Tratamiento en materia de protección de Datos Personales (en adelante la "Política") en relación con la recolección, uso, y transferencia de los mismos, en virtud de la autorización que ha sido otorgada por los Titulares de la información. Es obligación por parte de Tecnisegur Uruguay S.A. la inscripción de las bases de datos que haya conformado o de los códigos de conducta con que se rijan las actividades que desarrolla.***

1. POLITICAS RELACIONADAS.

- Política de uso informático para funcionarios operativos.
- Política de seguridad de la información.
- Política antifraude.
- FP 09C-062 Gestión vulnerabilidades.
- IT 02-021 Codigo de ética y conducta Tecnisegur Uruguay S.A.
- IT 10-001 Plan de continuidad del negocio
- FP 09C-047 Proceso de ejercicio de los derechos de rectificación, actualización, inclusión, supresión de datos personales.
- FP 09C-049 Proceso de notificación en escenarios de brecha de seguridad.
- FP 09C-063 Almacenamiento y conservación de registros.

2. LOS PRINCIPIOS PARA EL TRATAMIENTO DE LOS DATOS PERSONALES DE TECNISEGUR URUGUAY S.A. SERAN:

- **Principio de legalidad**: La formación de bases de datos es lícita cuando se encuentren debidamente inscriptas, observando en su operación los principios que establecen la Ley 18.331 y sus reglamentaciones. La base de datos de Tecnisegur se encuentra inscriptos en el registro a cargo de la Unidad Reguladora y de control de datos personales (URCDP) Resolución 2019-01-103 Aprobación de Datos Tecnisegur SA.

- **Principio de finalidad**: Los datos utilizados por Tecnisegur Uruguay S.A. son de uso en el fin para el cual fue solicitado. Una vez que cese la necesidad de tratamiento de los datos, los mismos podrán ser eliminados de las bases de datos, o archivados en términos seguros a efectos de que solamente sean divulgados cuando a ello hubiere lugar de acuerdo con la ley. Algunos datos no serán eliminados a pesar de la solicitud del Titular, cuando la conservación de estos sea necesaria para el cumplimiento de una obligación o contrato.

Para Tecnisegur Uruguay S.A.es indispensable recolectar, almacenar y utilizar los datos empresariales de los clientes: Número de RUT; Razón social, Nombre de fantasía; Dirección de la empresa; Localidad, Departamento; Teléfonos de contacto, Persona de contacto, Celular; Dirección de correo electrónico; Cuenta bancarias, Banco, Tipo de

cuenta, Número de cuenta para conocer la naturaleza del servicio que se les prestará, y también para remitir las facturas

Para el caso de los empleados, es indispensable conocer los sus datos personales a fin de tomar conocimiento de las personas que trabajan para Tecnisegur Uruguay S.A como ser : Número de documento de identidad; Género; Nombres y Apellidos; Fecha de nacimiento; Estado civil, Datos del cónyuge e hijos ,Dirección de domicilio; Barrio; Localidad; Departamento; Teléfonos de contacto; Celular; Dirección de correo electrónico; Cuenta bancaria para los depósitos : Banco; Tipo de cuenta; Número de cuenta , Datos de BPS experiencia laboral , formación y estudios, Certificados de buena conducta, Carnet de Salud (Dato Sensible según Articulo 18),Libreta de conducir para determinados cargos. credencial cívica, y constancias de voto.

Tecnisegur tiene bajo su responsabilidad los datos personales de todos sus empleados con el fin de poder desarrollar de forma adecuada su objeto social. También es necesario contar con los datos de personas que sean potenciales empleados, para así agilizar los procesos de selección, y obtener resultados más eficientes en los mismos. Estas Bases de datos tienen como finalidad cumplir con las obligaciones contractuales con sus empleados, y también facilita las obligaciones de Tecnisegur Uruguay S.A. para con sus Clientes, Proveedores, y/o Contratistas.

Respecto a los potenciales empleados la Base de datos tiene como finalidad poder realizar procesos de selección más eficientes, y cortos, clasificando a los potenciales candidatos, o conservando sus datos para una posterior convocatoria, dichos datos podrán ser utilizados a su vez para otros procesos de selección dentro Tecnisegur.

Si dentro de la información recolectada se encuentran datos sensibles, Tecnisegur le informará de la calidad de dicho dato sensible, y sólo serán tratados con su consentimiento previo, expreso e informado.

Para el caso de Proveedores Tecnisegur Uruguay S.A. requiere de diversos Proveedores de productos, y/o servicios para así cumplir con sus obligaciones contractuales, y para brindar las herramientas a sus empleados. En esa medida para la contratación de proveedores, y para que se cumpla con sus obligaciones legales, contractuales, y estatutarias se deben recopilar ciertos datos personales de: Nombre, RUT y Razón, Datos generales y específicos de identificación de los contactos de cada uno, Datos personales y profesionales de los contactos de cada uno., Información financiera, (cuentas bancarias).

El Titular al aceptar esta Política, autoriza que los Datos Personales serán utilizados sólo para los propósitos señalados, y entiende que Tecnisegur Uruguay S.A. no procederá a vender, licenciar, transmitir o divulgar la misma, fuera de Tecnisegur salvo que:

(i) El Titular autorice expresamente a hacerlo.
(ii) Sea necesario para permitir a nuestros servicios tercerizados a prestar los servicios que les fueron encomendado, con el fin de proporcionarle nuestros productos o servicios.
(iii) Sea divulgada a las entidades que prestan servicios de marketing en nuestro nombre o a otras entidades con las cuales tenemos acuerdos de mercadeo conjunto.
(iv) Según sea requerido o permitido por la ley.

A fin de poner en práctica los propósitos descritos anteriormente, los datos personales del Titular podrán ser divulgados con los fines dispuestos en esta Política al personal de recursos humanos, encargados, consultores, asesores y a otras personas y empresas según corresponda.

Tecnisegur recolecta los datos para los siguientes fines:

a) Prestar los servicios de traslado de activos.
b) Acreditar dinero a las cuentas de los clientes.
c) Realizar campañas de publicidad, y mercadeo para ofrecer servicios.
d) Informar sobre cambios de nuestros productos, o servicios.
e) Implementar programas de fidelización.
f) Evaluar la calidad de nuestros productos, y servicios.
g) Proveer nuestros productos, y servicios requeridos directamente, o a través de terceros, y recibir retroalimentación.
h) Informar sobre nuevos productos o servicios que estén relacionados o no con el contrato suscrito.
i) Enviar información sobre actividades desarrolladas o envío de información que se considere de interés a través de diferentes medios.
j) Dar cumplimiento a las obligaciones legales de información a los entes administrativos, así como a las autoridades competentes que así lo requieran.
k) Realizar encuestas de satisfacción.
l) Cualquier otra finalidad que llegara a resultar en desarrollo del contrato, o la relación comercial entre Tecnisegur Uruguay S.A., y los Clientes
m) Informar al personal de disposiciones internas, y comunicados fuera del horario de trabajo.
n) Poder trasmitir información requerida por organismos del estado: BPS, MTSS, DIGEFE, DGI, u otros
o) Seguridad interna, y controles en el recuento por medio de filmación requerimiento necesario.
p) Seguridad externa, en las unidades blindadas y controles por medio de filmación requerimiento necesario.

- **Principio de previo consentimiento informado**: Tecnisegur obtiene los datos con el consentimiento libre, dicho consentimiento debe ser:
  - **Informado**: Al titular de los datos hay que informarle para que se usaran y donde pueden ejercer sus derechos.
  - **Documentado**: Registrado en algún tipo de soporte o documento que permita verificar su existencia.
  - **Expreso**: Debe ser dado de forma explícita, no debe darse por sobre entendido.
  - **Previo:** Debe ser pedido antes de los datos.
  - **Libre:** Lo debe dar en forma voluntaria.

Para tratar los datos personales siempre es necesario contar con el consentimiento del titular salvo en los siguientes casos: Fuentes públicas, funciones del Estado, obligación legal, relacion contractual científica o profesional, uso personal individual o doméstico.

Tecnisegur Uruguay S.A. A través de su **Cláusula de Consentimiento** (en su página web institucional, o bien en el documento físico, Acuerdo de confidencialidad, Contratos con funcionarios, y Clientes), recolectará informacion que será reservada y con previa autorización del titular del dato..

Excepciones legales a la obtención de una autorización: el previo consentimiento no será necesario cuando:

a) Así lo disponga una ley de interés general.

b) En los supuestos del artículo 9° de la presente ley.

- **Principio de veracidad**: El tratamiento de la información será veraz, adecuada, ecuánime, (imparcial), y no excesiva en relación con la finalidad para la que se han obtenido. La recolección de datos no podrá hacerse por medios desleales, fraudulentos, abusivos, extorsivos o en forma contraria a las disposiciones a la presente ley 18331.
  Los datos deberán ser exactos y actualizarse en el caso en que ello fuere necesario.

  Cuando se constate la inexactitud o falsedad de los datos, el responsable del tratamiento, en cuanto tenga conocimiento de dichas circunstancias, deberá suprimirlos, sustituirlos o completarlos por datos exactos, veraces y actualizados. Asimismo, deberán ser eliminados aquellos datos que haya caducado de acuerdo a lo previsto en la presente ley.

- **Principio de reserva:** Tecnisegur Uruguay S.A. tratara los datos personales de forma reservada, y los utilizara únicamente para la finalidad para la que se obtuvieron. El personal de Tecnisegur Uruguay S.A., está obligado a guardar estricto secreto profesional sobre los datos (artículo 302 del Código Penal, Articulo 25 Ley 15322 y Articulo 54 Ley 18627). Tecnisegur Uruguay S.A. no podrá facilitar noticia alguna sobre fondos o valores que tengan en cuenta corriente, depósitos o cualquier otro concepto perteneciente a persona física o jurídica. Tampoco se podrá dar a conocer informacion confidencial que reciba de sus clientes o sobre sus clientes. Cuando hayan sido recogidos de fuentes no accesibles al público. Los responsables y/o personal de las diferentes áreas serán instruidos en el conocimiento de dicho artículo.
  Solo se podrá relevar el secreto profesional en dos ocasiones:
  - Con existencia de una orden judicial.
  - Consentimiento del titular

  Tecnisegur Uruguay S.A. podrá subcontratar a terceros para realizar determinadas funciones. Cuando ello ocurra el procesamiento de información personal, o comparta información personal a terceros prestadores de servicios; en ambos casos Tecnisegur Uruguay S.A advierte a los mismos, a través de su **Contrato de prestación de servicios**, y de su **Acuerdo con proveedor**, sobre la necesidad de proteger dicha información confidencial y reservada con medidas de seguridad apropiadas, les prohíbe el uso de información personal para fines propios, y les impide que divulguen su información personal a otros.

  De igual forma Tecnisegur Uruguay S.A podrá transferir, o transmitir (según corresponda) datos personales a otras compañías en el extranjero por razones de seguridad, eficiencia administrativa y mejor servicio, lo cual se autoriza mediante la

aceptación de esta Política. En materia de transferencias internacionales de datos, Uruguay cuenta con una regulación específica dispuesta en el art. 23 de la Ley 18.331 de Protección de Datos Personales.

Esta norma indica la prohibición de realizar transferencias internacionales de datos a países u organismos internacionales que no proporcionen niveles de protección de datos adecuados, de acuerdo con los estándares de derecho nacionales e internacionales en la materia, salvo excepciones.

Entre estas excepciones se encuentra la autorización por parte de la Unidad Reguladora y de Control de Datos Personales, para una o varias transferencias.

- **Principio de responsabilidad:** Es el que establece que el responsable de la base de datos es responsable de las violaciones de las disposiciones de la ley.

- **Principio de seguridad de los datos:** Tecnisegur Uruguay S.A. protege y almacena los datos en sus servidores Primarios y Secundarios como contingencia en sitio alternativo pertenecientes a Tecnisegur Uruguay S.A.
  Los servidores en que se almacenan los datos estan emplazados en lugares seguros y protegidos por medidas de seguridad físicas ; el perímetro de la infraestructura de IT estará protegido por cortafuegos de red, y se reforzará la seguridad en el almacenaje de dichos datos.
  Todo personal interno o externo firmara acuerdos de confidencialidad.
  A los usuarios se les garantizaran derechos de acceso exclusivamente a aquellos recursos que sean estrictamente necesarios para desempeñar sus tareas.
  Solo el administrador del sistema (Responsable IT) estará facultado para conceder, modificar, o anular los derechos de acceso de acuerdo a criterios estrictos.

  En ella se regulan diversos principios en sus artículos 5 al 12 de la propia Ley 18.331, a los que se deben ceñir los responsables, y encargados de tratamiento de datos personales. Dentro de estos principios se encuentra el que es el objeto central, el de seguridad de los datos (Articulo 10 de la Ley 18.331). Este principio refiere a las medidas de seguridad que deben ser adoptadas , además de establecer obligaciones vinculadas a la forma de almacenar los datos de forma de permitir el ejercicio del derecho de acceso, y a condiciones técnicas de integridad, y seguridad que de no existir prohíben el registro de dichos datos.

- **Principios en materia de medidas de seguridad.** Las medidas recomendadas para el responsable como el, o los encargados del tratamiento de los datos son:
  a) Usar los sistemas, y softwares necesarios para tener el nivel de seguridad adecuado.
  b) Determinar en forma correcta, eficaz, y eficiente quienes son las personas que tienen los permisos para la gestión de los datos personales que contienen las bases, y su acceso.
  c) Utilizar contraseñas seguras, difíciles de ser cifradas por terceros
  d) Instalar programas conocidos o que se puedan identificar el origen.
  e) Publicar solo los datos personales necesarios.
  f) Realizar copias de seguridad de los datos personales que se posee, las que deberán almacenarse al menos con los mismos criterios de seguridad habituales.

g) Usar servicios de nube de proveedores conocidos y con criterios seguros para los datos.

- **Tratamiento del ciclo de vida de los datos**. Es necesario mapear las distintas etapas del ciclo de vida de los datos con respecto a las actividades habituales de TECNISEGUR URUGUAY S.A.

  Es fundamental que se describan como recolectan , almacenan, utilizan y finalmente eliminan la información en su poder. En términos generales pueden identificarse las siguientes etapas en el ciclo de vida de los datos:

  - **Recolección:** Obtención de datos de persona determinada o determinable para destinar a actividades de tratamiento.
  - **Categorización:** Implica toda actividad de clasificación de la información , incorporándola en distintas categorías definidas por el tipo de dato y su finalidad. Distintas categorías de datos pueden ser objeto de distintas medidas de seguridad de acuerdo a su naturaleza. En cuanto a los datos sensibles, estos deben ser tratados con estricta reserva.
  - **Tratamiento:** Hace referencia a todo tipo de gestión sobre los datos, incluyendo su almacenamiento, conservación y aplicación en sistemas de la empresa, además de incluir las actividades de actualización, rectificación y disociación de la información.
  - **Comunicación:** Refiere a toda revelación o envió de datos personales a personas distintas del titular previstas por las normas.
  - **Eliminación:** Una vez cumplida la finalidad para la que se obtuvo la información, corresponde proceder a su supresión. Asimismo, ante la eliminación supone algo más que la mera eliminación del archivo, pues también requieres de una constatación de dicha eliminación, comprobando que no haya quedado rastros de los datos en el sistema.

- **Gestión del riesgo:** Para realizar una adecuada gestión de riesgos si la organización entiende como procesa, o procesara datos personales. Ignorar que información se tiene y para que se usa en sí, puede entrañar un riesgo significativo a los derechos de las personas.
  TECNISEGUR URUGUAY S.A. realiza su gestión de riesgos mediante el cual se identifica , analiza y valor la probabilidad, y la evaluación del impacto de las ocurrencias de amenazas que, mediante la explotación de alguna vulnerabilidad puedan materializar un riesgo para los derechos de las personas (Una Evaluación de Impacto en la Protección de Datos (EIPD) es un proceso que las organizaciones deben efectuar para identificar y tratar los riesgos que puedan producir sus actividades habituales, sus nuevos proyectos o sus políticas corporativas cuando involucran el tratamiento de datos personales).
  El objetivo es establecer cuáles son las hipótesis de riesgo para luego en una etapa posterior definir el plan de tratamiento necesario para minimizar aquellos riesgos que no se consideren aceptables para mantener protegido los derechos de las personas.

- **Los Datos Personales** que son incluidos en la Base de Datos de Tecnisegur Uruguay S.A. provienen de la información recopilada en ejercicio de las actividades desarrolladas debido a los vínculos comerciales, contractuales, laborales.

- **Los datos videovigilancia** al igual que los anteriores son incluidos en la base de datos de Tecnisegur Uruguay S.A, siendo respaldados a través de sistema de filmación durante 60 días (según Circular 2404- Articulo 30 Instituciones financieras BCU)

  Los canales donde se obtienen los datos son: Sitio Web, Redes Sociales, Contratos Comerciales, y Laborales, Encuestas de Satisfacción y de Servicio, son los medios a través de los cuales Tecnisegur Uruguay S.A., obtiene los Datos Personales a que hace referencia la presente Política.

- Las Bases de Datos, cuya administración tiene Tecnisegur Uruguay S.A., están sujetas a estrictas medidas de seguridad, cuyo cumplimiento debe ser garantizado por cada uno de los empleados de Tecnisegur Uruguay S.A., que tengan acceso a estás. Las Bases de Datos que constan en archivos electrónicos bien sea en los computadores de los funcionarios, están protegidas por contraseñas, las cuales sólo pueden conocer los empleados que requieran acceder a éstas. Las Bases de Datos que consten en medios físicos, son responsabilidad de cada funcionario de Tecnisegur Uruguay S.A., quien las deberá mantener bajo llave, o cualquier mecanismo equivalente, que permita en todo momento garantizar el acceso restringido a esta. Cualquier clase de vulneración o amenaza a las bases de datos debe ser informada inmediatamente al Comité de Seguridad de la informacion.

- **Los datos biométricos** como datos personales obtenidos a partir de un tratamiento técnico especifico, relativos a las características físicas, fisiológicas o conductuales de una persona física que permitan o confirmen la identificación única de dicha persona tales como datos dactiloscópicos, reconocimiento de imagen o voz (artículo 4 Literal Ñ de la Ley 18331). Dicho datos considerados datos especialmente sensible impulsa a la obligación de los responsables de realizar evaluaciones de impacto previas a su tratamiento.

3. GARANTIAS SOBRE LOS DERECHOS.

La ley creo la Unidad Reguladora y de Control de Datos Personales como un órgano desconcentrado de la Agencia de Gobierno electrónico y sociedad de la informacion y del conocimiento.(URCDP).

Los cometidos de dicha Unidad:

a) Accesoria sobre el dictado de normas.
b) Recomendar políticas en el tratamiento seguridad y manipulación de los datos personales.
c) Controlar que se cumpla la Ley.
d) Realizar un censo de las bases de datos alcanzadas por la Ley y llevar un registro de las mismas.

- **Derecho de acceso**: Cuando el titular de datos personales acredite su identificación con el documento de identidad, o poder respectivo, tendrá el derecho a obtener toda la información que sobre sí mismo se halle en bases de datos de Tecnisegur Uruguay S.A. Podrá ser ejercidos sus derechos a intervalo de 6 meses, y si el titular lo prefiere podrá suministrar por escrito, y en forma clara a través de medios electrónicos, telefónicos, de imagen, u otro idóneo a tal fin

- **Derecho de rectificación, actualización, inclusión o supresión**: Las personas físicas o jurídicas tendrán derecho a solicitar la rectificación, actualización, inclusión o supresión de los datos personales que le corresponda incluidos en una base de datos, al constatarse error, o falsedad, o exclusión en la información de la que es titular. Podrá solicitarla la rectificación, actualización, inclusión, y/o supresión al correo contacto@tecnisegur.com.uy; dicha casilla de correo va redireccionada al sector IT responsable del tratamiento de los datos personales.

  Dispondrá de 5 días hábiles (según Articulo 15 Ley 18.331), para realizar la acción e informar al solicitante de lo efectivamente realizado o, en su caso, informar de las razones por las que estime no corresponde.

  TECNISEGUR URUGUAY S.A durante el proceso de rectificación, actualización, inclusión o supresión de datos personales y ante el requerimiento de terceros por acceder a informes sobre los mismos, deberá dejar constancia que dicha información se encuentra sometida a revisión.

  El ejercicio de los derechos de los Titulares conforme a la Ley 18.331 serán recibidas en:

  Domicilio: Uruguay N.º 2054 - Montevideo

  Mediante el formulario "Contáctenos" de la página web.

  Correo electrónico a la siguiente dirección: contacto@tecnisegur.com.uy

  En todos los casos, la solicitud deberá ir acompañada de la cédula de identidad del titular, poder en caso de comparecer mediante apoderado y/o documentación que acredite la calidad de sucesor, en caso de solicitar información respecto de personas fallecidas.

4. RESPONSABLES DEL TRATAMIENTO DE DATOS PERSONALES

TECNISEGUR URUGUAY S.A.

Razón social: TVTUSA

RUT: 215437010016

Domicilio: Avenida Uruguay 2054- Montevideo.

Teléfono: +598 24012565

Correo electrónico: contacto@tecnisegur.com.uy // canal de denuncias RRHH

Página Web: https://www.tecnisegur.com.uy

- **ÁREA RESPONSABLE DEL TRATAMIENTO DE DATOS PERSONALES**

Obligaciones del responsable:

a) Cumplir con la Ley y todos los principios que en ella se enumeran.
b) Informar a los titulares cuando les pide sus datos, ¿Dónde?, ¿Para qué?, ¿Cómo puede acceder?, ¿Cuánto tiempo?, ¿Cómo ejercer sus derechos?.
c) Obtener el consentimiento de los titulares.

d) Inscribir la base de datos.
e) Responder en un plazo máximo de cinco días hábiles.

- **El Departamento IT** a través de su Jefe de área, será encargado de recibir las peticiones, actualizaciones, eliminación, quejas, o reclamos de los Titulares de los Datos Personales, informado por los responsables lideres según departamentos que manejan dicha informacion:

- **DELEGADO ANTE LA UNIDAD REGULADORA ARGESIC.**

De acuerdo con lo dispuesto en el artículo 40 de la Ley N° 19670 de 15 de octubre de 2018, deberán designar un delegado de protección de datos personales. Dicha responsabilidad es cumplida por el Responsable del sistema de gestión integral cuyas funciones principales como delegado de protección de datos serán:

a) Asesorar en la formulación, diseño y aplicación de políticas de protección de datos personales.

b) Supervisar el cumplimiento de la normativa sobre dicha protección en la entidad o entidades para las que preste servicios.

c) Proponer todas las medidas que entienda pertinentes para adecuarse a la normativa y a los estándares internacionales en materia de protección de datos personales y verificar su realización.

d) Actuar como nexo entre su entidad y la Unidad Reguladora y de Control de Datos Personales.

e) Estrecha comunicación con los diferentes responsables por área.

5. PODER JUDICIAL

Consagra el derecho de HABEAS DATA determinando que toda persona puede reclamar ante la Justicia conocer los datos que existen en Bases de Datos publica y privadas referidos a su persona, su finalidad y uso. Cuando cualquier de sus derechos no son respetados, puede recurrir a la Justicia para reclamar el cumplimiento de la ley.

Procedencia y competencia (ley 18.331 Articulo 38).- El titular de datos personales podrá establecer la acción de protección de datos personales o habeas data, contra todo responsable de una base de datos pública o privada, en los siguientes supuestos:

A) Cuando quiera conocer sus datos personales que se encuentran registrados en una base de datos o similar y dicha información le haya sido denegada, o no le hubiese sido proporcionada por el responsable de la base de datos, en las oportunidades y plazos previstos por la ley.

B) Cuando haya solicitado al responsable de la base de datos o tratamiento su rectificación, actualización, eliminación, inclusión o supresión y éste no hubiese procedido a ello o dado razones suficientes por las que no corresponde lo solicitado, en el plazo previsto al efecto en la ley.

Si el reclamo es aceptado , el Juez convoca a una audiencia pública dentro del plazo de 3 días.(Articulo 40-45 de ley)

Terminología de la Ley 18.331:

Los conceptos introducidos en esta ley son claves para determinar su alcance e

implicancias. Se detallan algunas de las definiciones descritas en el artículo

❖ Dato personal:

Información de cualquier tipo referida a personas físicas o jurídicas determinadas o determinables. Se consideran datos públicos, los cuales no requieren consentimiento informado a:

• Para personas físicas: Nombres y apellidos, documento de identidad, nacionalidad, domicilio y fecha de nacimiento.

• Para personas jurídicas: Razón social, nombre de fantasía, registro único de contribuyentes, domicilio, teléfono e identidad de las personas a cargo de esta.

❖ Dato sensible:

Datos personales que revelen origen racial y étnico, preferencias políticas, convicciones religiosas o morales, afiliación sindical e informaciones referentes a la salud o a la vida sexual.

❖ Base de datos:

Conjunto organizado de datos personales que sean objeto de tratamiento o procesamiento electrónico o no, cualquiera que fuere la modalidad de su formación almacenamiento, organización o acceso.

❖ Tratamiento de datos:

Operaciones y procedimientos sistemáticos, de carácter automatizado o no, que permitan el procesamiento de datos personales, así como también su cesión a terceros a través de comunicaciones, consultas, interconexiones o transferencias.

❖ Titular de los datos:

Persona cuyos datos sean objeto de un tratamiento incluido dentro del ámbito de acción de la ley.

❖ Responsable de la base de datos o del tratamiento:

Persona física o jurídica, pública o privada, propietaria de la base de datos o que decida sobre la finalidad, contenido y uso del tratamiento.

❖ Encargado del tratamiento:

Persona física o jurídica, pública o privada, que sola o en conjunto con otros trate datos personales por cuenta del responsable de la base de datos o del tratamiento.

❖ Usuario de datos:

Toda persona, pública o privada, trate datos, ya sea en una base de datos propia o a través de conexión con los mismos.

❖ Derechos de los interesados:

a) Recibir información previa acerca de para que se solicitan los datos.
b) Conocer que datos poseen sobre cada uno.
c) Rectificar o cancelarlos cuando sean inexactos o incompletos.
d) Que nuestros datos no sean comunicados sin nuestro consentimiento, salvo las excepciones que la ley prevé.
e) Las personas tienen derecho a ser informadas sobre el criterio de

valoración y el programa utilizado para ello.

f) No recibir publicidad no deseada.

g) Consultar o Denunciar ante la Unidad reguladora y de Control de datos Personales

❖ Nivel de los datos:

- INTIMIDAD: Protege la esfera de reserva de la vida personal.
- PRIVACIDAD: Relacionamiento con los demás, apertura al mundo.

❖ Principios fundamentales en la protección de datos:

- FINALIDAD: Para el cual son utilizados los datos.
- CONSENTIMIENTO EXPRESO Y REVOCABLE: Aprobación de la persona para el tratamiento de sus datos:

22 de Octubre del 2020

Numero de revisión: 01 Fecha: 12/2020
Numero de revisión: 02 Fecha: 03/2021
Numero de revisión: 03 Fecha: 09/2021
Numero de revisión: 04 Fecha: 03/2022
Numero de revisión: 05 Fecha: 08/2022
Numero de revisión: 06 Fecha: 06/2023
Numero de revisión: 07 Fecha: 01/2024
Numero de revisión: 08 Fecha: 07/2024
Numero de revisión: 09 Fecha: 08/2025
Numero de revisión: 10 Fecha: 10/2025

Aprobada

Miguel Alvez

Director

Registro de revisiones	Revisión	Fecha	Observaciones
	00	Octubre 2020	Documento original
	01	Diciembre 2020	Se define los registros de inscripción por la Unidad Reguladora y de control de Datos Personales. Se define la forma de destrucción de los datos personales al momento del cese en sus funciones.
	02	Marzo 2021	Se ajusto la política de acuerdo con las necesidades según normativa de URCDP

	03	Setiembre 2021	Se define los voceros responsables ante denuncias sobre el uso de datos personales. Se actualiza el sistema de respaldo de DVR a sistema de filmación.
	04	Marzo 2022	Se define los principios de previo consentimiento informado, de seguridad, gestión de riesgo y evaluación del impacto
	05	Agosto 2022	Se anexa la garantía sobre los derechos del titular y lo que refiere al poder judicial
	06	Junio 2023	Se anexa los artículos 25 Ley 15322 y 54 Ley 18627 sobre secreto profesional en el Principio de Reserva.
	07	Enero 2024	Principio de reserva: En materia de transferencias internacionales de datos, Uruguay cuenta con una regulación específica dispuesta en el art. 23 de la Ley 18.331 de Protección de Datos Personales.
	08	Julio 2024	Se elimina codificación del documento para las políticas según FP 01 Gestión de la informacion.
	09	Julio 2025	Actualización del título del documento pasando a un proceso con codigo adjudicado a RRHH.
	10	Octubre 2025	Ingreso de nuevos documentos relacionados, y nuevo punto relacionado con los datos biométrico como dato especialmente sensible.

Fecha	**Elaborado por**	**Revisado por**	**Aprobado por**
Mayo 2019	**RRHH**	Responsable SGI	Gerencia General