

## 1. OBJETIVO

Dar a conocer las exigencias de la Ley de Protección de Datos Personales (Ley N° 29733) y su Reglamento a todos los colaboradores de CONTUGAS S.A.C, en adelante CONTUGAS, así como garantizar su cumplimiento.

## 2. ALCANCE

Todos aquellos procesos de CONTUGAS que involucren información de datos personales de los Bancos de Datos de colaboradores, clientes, proveedores, postulantes y terceros.

## 3. DEFINICIONES

- 3.1. **Autorización:** Consentimiento previo e informado del titular para llevar a cabo el tratamiento de datos personales.
- 3.2. **Aviso de Privacidad:** Comunicación verbal o escrita generada por el responsable, dirigida al titular para el tratamiento de sus datos personales.
- 3.3. **Banco de datos personales:** Conjunto organizado de datos personales, automatizado o no, y con una determinada finalidad, cualquiera que sea la forma de su creación, formación, almacenamiento, organización y acceso; pudiendo inclusive pertenecer los mismos datos personales a más de un banco de datos personales.
- 3.4. **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.
- 3.5. **Bloqueo:** Es la medida por la que el encargado del banco 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.
- 3.6. **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.
- 3.7. **Datos personales:** Toda aquella información numérica, alfabética, gráfica, fotográfica, acústica o de cualquier otro tipo concerniente a las personas naturales que las identifica o las hace identificables.
- 3.8. **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.
- 3.9. **Dato público:** Es el dato que no sea semiprivado, privado o sensible, se encuentra usualmente en registros públicos.
- 3.10. **Datos indispensables:** Son aquellos datos personales de los titulares que son indispensables para llevar a cabo la afiliación a un seguro de vida, estos deben ser proporcionados por el titular.
- 3.11. **Datos opcionales:** Son aquellos datos que CONTUGAS requiere para ofrecer servicios adicionales.
- 3.12. **Datos sensibles:** Datos personales referidos al origen racial o étnico de una persona, ingresos económicos, datos relacionados a la salud, opiniones o convicciones políticas, religiosas, filosóficas o morales, afiliación sindical, e información relacionada a la salud o a la vida sexual.
- 3.13. **Derechos ARCO: Derechos con los que cuentan los titulares del Dato.**
  - Acceso: Toda persona tiene derecho a obtener la información que sobre sí mismo sea objeto de tratamiento en banco de datos de administración pública o privada.
  - Rectificación: Es el derecho del titular de datos personales que se modifiquen los datos que resulten ser parcial o totalmente inexactos, incompletos, erróneos o falsos.
  - Cancelación: El titular de los datos personales podrá solicitar la supresión o cancelación de sus datos personales de un banco de datos personales cuando estos hayan dejado de ser necesarios o pertinentes para la finalidad para la cual hayan sido recopilados.
  - Oposición: Toda persona tiene la posibilidad de oponerse, por un motivo legítimo y fundado, referido a una situación personal concreta, a figurar en un banco de datos o al tratamiento de sus datos personales.

- 3.14. Encargado del tratamiento:** Persona Natural o Jurídica, pública o privada que por sí misma o en asociación con otros, realice el Tratamiento de datos personales en nombre del Responsable del Tratamiento.
- 3.15. 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.
- 3.16. Principios Rectores:** Principios que deben regir el uso de los datos personales:
- **Consentimiento:** El tratamiento de los datos personales es lícito cuando el titular del dato personal hubiere prestado su consentimiento libre, previo, expreso, informado e inequívoco.
  - **Finalidad:** Una finalidad está determinada cuando haya sido expresada con claridad, sin lugar a confusión y cuando de manera objetiva se especifica el objeto que tendrá el tratamiento de los datos personales.
  - **Calidad:** Los datos contenidos en un banco de datos personales, deben ajustarse con precisión a la realidad. Se presume que los datos directamente facilitados por el titular de los mismos son exactos.
  - **Seguridad:** El tratamiento de los datos personales deben adoptarse las medidas de seguridad que resulten necesarias a fin de evitar cualquier tratamiento contrario a la Ley o al presente reglamento.
  - **Legalidad:** Todo tratamiento de datos personales debe ser apropiado a la finalidad para la que estos hubiesen sido recopilados, usando la información que sea imprescindible y suficiente, sin excesos.
  - **Proporcionalidad:** El tratamiento de los datos personales se hace conforme a lo establecido en la Ley de Protección de Datos Personales. Se prohíbe la recopilación de los datos personales o por medios ilícitos.
- 3.17. Procedimiento de anonimización:** Tratamiento de datos personales que impide la identificación o que no hace identificable al titular de estos. El procedimiento es irreversible.
- 3.18. Procedimiento de disociación:** Tratamiento de datos personales que impide la identificación o que no hace identificable al titular de estos. El procedimiento es reversible.
- 3.19. Rectificación:** Es aquella acción genérica destinada a afectar o modificar un banco de datos personales ya sea para actualizarlo incluir información en él o específicamente rectificar su contenido con datos exactos.
- 3.20. Responsable del Banco de datos personales:** Persona encargada de cada banco de datos personales, y del cumplimiento de las exigencias de la ley sobre el mismo.
- 3.21. Responsable del Tratamiento:** Es aquél que decide sobre el tratamiento de datos personales, aun cuando no se encuentren en un banco de datos personales.
- 3.22. Titular de datos personales:** Persona natural a quien corresponde los datos personales.
- 3.23. Titular del banco de datos personales:** Determina la finalidad y contenido de los bancos de datos personales, el tratamiento de estos y las medidas de seguridad.
- 3.24. 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.
- 3.25. Transferencia de datos personales:** Toda transmisión, suministro o manifestación de datos personales, de carácter nacional o internacional, a una persona jurídica de derecho privado, a una entidad pública o a una persona natural distinta del titular de datos personales.

#### 4. RESPONSABILIDADES

##### 4.1. Titular del Banco de Datos

- Responsable de coordinar con la Autoridad Nacional de Protección de Datos Personales en términos del registro, modificación o cancelación de Bancos de Datos Personales.

- Responsable de coordinar con el Encargado de los Bancos de Datos Personales en caso de modificaciones, cancelación o registro de un nuevo Banco de Datos Personales.
- Responsable de mantener un registro de las modificaciones generadas en los Bancos de Datos Personales.
- Responsable de responder a los Titulares de Datos Personales según la resolución de sus solicitudes siguiendo los lineamientos de los procedimientos de Atención a las Solicitudes ARCO.
- Responsable de alertar ante la falta de respuesta del Encargado del Banco de Datos Personales, considerando los tiempos de respuesta establecidos en el procedimiento de Atención a las Solicitudes ARCO.

#### **4.2. Encargado del Banco de Datos**

- Responsable de identificar y reportar nuevos repositorios, datos y medios por los cuales se registra información personal.
- Responsable del tratamiento y resguardo de la información contenida en el Banco de Datos Personales bajo su responsabilidad.
- Responsable de responder antes las auditorías anuales en relación a los controles de seguridad del Banco de Datos Personales bajo su responsabilidad.
- Responsable de coordinar la comunicación con el Titular del Dato Personal en caso se considere necesario por un incidente de seguridad al Banco de Datos Personales bajo su responsabilidad.
- Coordinar con el Titular de los Bancos de Datos Personales para la respuesta en caso de modificación, cancelación o registro de un nuevo Banco de Datos Personales.
- Autorizar transferencias de información cuando se solicite información del banco del cual es responsable.

#### **4.3. Seguridad de la Información**

- Cumple el rol de Representante de seguridad de los bancos de datos personales, por lo cual será responsable de coordinar la aplicación de la Directiva de Seguridad de la Información de la Ley de Protección de Datos Personales en CONTUGAS.
- Definir los controles de seguridad necesarios destinados a evitar el acceso no autorizado, pérdida o corrupción durante el tránsito hacia su destino, teniendo en cuenta los mecanismos mínimos de seguridad que la Ley de Protección de Datos Personales y su reglamento exigen.
- Revisar periódicamente la efectividad de los controles de seguridad adoptados para la protección de los bancos de datos personales y generar acciones de mejora.
- Implementar controles relacionados a la Seguridad de Información como parte del plan de adecuación a las exigencias de la Ley de Protección de Datos Personales y su reglamento.

#### **4.4. Usuario**

- Realizar un adecuado tratamiento, según lo definido en la presente política, a la información de datos personales, e inclusive datos sensibles de los clientes, proveedores, colaboradores, postulantes, prospectos y terceros de CONTUGAS.
- Proteger los activos de información que contienen datos personales de alteraciones, destrucción o transferencia no autorizada.
- Adecuarse a los procedimientos que defina CONTUGAS según las exigencias de la Ley de Protección de Datos Personales y su Reglamento.
- Notificar cualquier incidente que incumpla con la presente política de Seguridad de la Información.
- Solicitar autorización al Encargado del Banco respectivo para realizar transferencias de información.

#### **4.5. Asesor Legal**

- Brindar asesoría legal a las distintas áreas de CONTUGAS en cuanto a la absolución de consultas sobre las especificaciones exigidas por la Ley de Protección de Datos Personales y su Reglamento.

## 5. DESARROLLO DE LA POLÍTICA

### 5.1. Consideraciones generales

- 5.1.1. CONTUGAS debe definir a los responsables de cada banco de datos personales, los cuales tendrán responsabilidad directa y velarán por el cumplimiento de la presente política.
- 5.1.2. Es de aplicabilidad a CONTUGAS toda aquella exigencia definida por la Ley de Protección de Datos Personales, salvo que esta difiera o contradiga alguna otra ley específica aplicable, para lo cual regirá esta última.
- 5.1.3. Es responsabilidad de CONTUGAS proporcionar la información relativa al tratamiento de datos personales a la Autoridad Nacional de Protección de Datos Personales cuando esta lo requiera, así mismo permitirle el acceso a los bancos de datos personales que CONTUGAS administra.
- 5.1.4. Toda persona que labore en CONTUGAS deberá suscribir un acuerdo de confidencialidad, a través del cual se brinda protección a la información perteneciente a los Bancos de datos personales.

### 5.2. Obtención de datos personales y consentimiento del titular de datos personales

- 5.2.1. CONTUGAS prohíbe la recopilación de los datos personales por medios fraudulentos, desleales o ilícitos. Dicha recopilación de datos personales debe ser actualizada, necesaria, pertinente y adecuada, con relación a las finalidades determinadas, explícitas y lícitas para las que se hayan obtenido. Así mismo, se debe garantizar la calidad de los datos contenidos en el banco de datos personales, y aplicar las medidas de seguridad necesarias que ayuden a prevenir la adulteración, pérdida y desviación de datos personales.
- 5.2.2. Previo a cualquier tratamiento de datos personales, el responsable de cada banco de datos encargado de la captura de los mismos, tiene la responsabilidad de garantizar que se cuente con el consentimiento del titular de datos personales, el cual debe ser previo, informado, expreso e inequívoco, así mismo deben ser recopilados y utilizados para una finalidad determinada, explícita y lícita, por lo que no debe extenderse a otra que no haya sido establecida en el momento de su recopilación.
- 5.2.3. Dicho consentimiento debe ser obtenido por escrito tanto para datos personales como para datos sensibles. Así mismo, es considerado un consentimiento por escrito el ejecutar un clic por la web.
- 5.2.4. En caso de necesitar efectuar el tratamiento de datos personales de un menor de edad, se requerirá del consentimiento de los titulares o tutores de los mismos.

### 5.3. Tratamiento de Datos Personales

- 5.3.1. El área de TI deberá definir los controles mínimos de seguridad necesarios con el fin de cumplir las exigencias de la Ley de Protección de Datos Personales, así mismo deberá asesorar y darle seguimiento a las áreas correspondiente para que se lleve a cabo la implementación de dichos controles.
- 5.3.2. El área de TI es responsable de la protección de activos de información que incluyen datos personales, con el fin de asegurar la confidencialidad, disponibilidad e integridad de los mismos. Como tal, se encargan de suprimir los datos personales cuando estos hayan dejado de ser necesarios o hubiese vencido el plazo para su tratamiento, salvo que medie procedimiento de anonimización o disociación.

### 5.4. Transferencia de Datos Personales

- 5.4.1. Los responsables de cada banco de datos deberán asegurarse de que toda transferencia de datos personales cuente con el consentimiento de su titular de datos, salvo excepciones previstas en la Ley y su Reglamento.

**5.4.2.** Toda transferencia de datos personales, tanto a nivel nacional como internacional, procederá con autorización de cada responsable del banco de datos personales, y el medio por el cual se llevará a cabo dicha transferencia de datos deberá cumplir con la política de seguridad de la información vigente. En caso sea necesario efectuar un flujo transfronterizo de datos personales, los responsables de cada banco de datos deben garantizar que el país destinatario mantenga los niveles de protección adecuados conforme a la ley vigente.

## **5.5. Alteración no autorizada del Banco de Datos Personales**

**5.5.1.** Toda traslado o uso de los Bancos de Datos Automatizados o cualquier información asociada a estos hacia fuera de los ambientes de CONTUGAS, deberá contar con la autorización por escrito del Encargado del Banco de Datos Personales. Los Sistemas de Información que se encuentran dentro del ámbito de la presente Política son: SAS, OPEN, GIS, Tarjetas de Proximidad, Sistema de Huella Dactilar y Videovigilancia.

**5.5.2.** Toda información personal almacenada en un medio informático removible debe ser borrada totalmente y/o evaluar la destrucción del medio de traslado luego de su uso; de forma tal que, no permita la recuperación de datos.

**5.5.3.** CONTUGAS, por intermedio del Titular del Banco de Datos Personales, debe designar a las personas encargadas de eliminar la información de datos personales contenidas en los medios informáticos removibles.

**5.5.4.** Para mantener la seguridad en las copias o reproducciones de documentos, se debe de cumplir con las siguientes medidas:

- a) Solo se deben utilizar los equipos de reproducción (impresoras, fotocopiadoras, scanners) autorizados.
- b) El Proceso de copia o reproducción de documentos debe ser supervisado constantemente, evitando desatender el equipo.
- c) Los documentos copiados o reproducidos no pueden ser dejados en los equipos; deben ser retirados inmediatamente después de finalizada la copia o reproducción.
- d) Se deben registrar las reproducciones o copias de los documentos con datos personales y/o sensibles. La información que se debe registrar es:
  - Nombre de la persona que solicita la copia.
  - Nombre de la persona autorizada a realizar copias.
  - Descripción de los datos personales copiados.
  - Número de copias.
  - Motivo de copia.
  - Nombre de la persona que recibe la copia.
  - Lugar de destino.
  - Periodo de validez de la copia.

## **5.6. Contratación de terceros que efectúan un tratamiento de datos personales**

**5.6.1.** Todo tercero con quien CONTUGAS comparta información de datos personales deberá considerar y cumplir, como parte del servicio vigente, con las exigencias de la Ley de Protección de datos personales y su reglamento, lo cual deberá ser formalizado mediante un contrato firmado por ambas partes.

**5.6.2.** Será de responsabilidad de cada área la regularización de los contratos vigentes con terceros mediante la inclusión de las adendas necesarias que contemplen los términos de la ley. De ser el caso, el área legal de CONTUGAS, brindará el asesoramiento a los responsables de las áreas correspondientes en cuanto a los términos tratados y definidos en el contrato.

## **5.7. Ejercicio de Derechos del Titular de Datos Personales**

**5.7.1.** Se deben almacenar los datos personales de manera que se posibilite el ejercicio de los derechos de su titular.

**5.7.2.**CONTUGAS debe posibilitar el ejercicio de los derechos del titular de los datos personales:

**5.7.3.**Derecho de Información:

- a) Finalidad para la que sus datos serán tratados.
- b) Quiénes son o pueden ser sus destinatarios.
- c) Identidad y domicilio del titular del banco de datos personales.
- d) La transferencia de los datos personales.
- e) Las consecuencias de proporcionar sus datos personales y de su negativa a hacerlo.
- f) Tiempo de conservación de los datos.

**5.7.4.**Derecho de Acceso:

- a) Obtener la información, de manera gratuita, que sobre sí mismo sea objeto de tratamiento en bancos de datos.
- b) La forma en que sus datos fueron recopilados.
- c) Razones que motivaron su recopilación.
- d) A solicitud de quién se realizó la recopilación.
- e) Transferencias realizadas o que se prevén hacer.

**5.7.5.**Derecho de rectificación, cancelación y oposición:

- a) Cuando se hubiere advertido omisión, error o falsedad.
- b) Cuando hayan dejado de ser necesarios o pertinentes a la finalidad para la cual hayan sido recopilados.
- c) Cuando hubiera vencido el plazo establecido para su tratamiento.

## **5.8. EXCEPCIONES**

**5.8.1.**Toda información perteneciente a las solicitudes de información que apliquen a alguna de estas excepciones podrá ser enviada sin requerir la autorización del encargado del banco de datos; sin embargo, debe llevarse un registro del envío de esta información:

- a) Cuando son necesarios para la ejecución de una relación contractual y que son utilizados exclusivamente para dicha finalidad.
- b) Cuando son relativos a la salud y son utilizados para un diagnóstico o tratamiento médico.
- c) Cuando se otorgan en el marco de un procedimiento administrativo o judicial.
- d) Cuando se trate de datos personales contenidos o destinados a ser contenidos en fuentes accesibles para el público.
- e) Cuando los datos personales sean utilizados con fines de actividades de valor histórico, estadístico o científico cuando se utilice un procedimiento de disociación o anonimización.