


# POLÍTICA GENERAL DE DATOS LA ARAUCANA

Cód.: PO-GDAT-036


Versión 001

ELABORADO	REVISADO	REVISADO	REVISADO	APROBADO
<p>César Caceres Analista Senior Gobierno de Datos</p>	<p>Rodrigo Silva Subgerente de Ciberseguridad</p> <p>Gloria Millán Jefe de División Sistemas</p>	<p>Lorena Ramírez Jefa de Cumplimiento y Normativa</p> <p>Julio Villalobos Abogado</p> <p>Gabriela Covarrubias Fiscal</p>	<p>Alejandro Espinosa Gerente de Planificación Estratégica y Control de Gestión</p> <p>Cecilia Del Valle Gerente de Ecosistemas Digitales</p> <p>Cristian Ibaceta Gerente Contralor</p> <p>Francisco Sepúlveda Gerente General</p>	<p>Cristian Abbott Presidente Comité de Transformación y Tecnología</p> <p>Josefina Montenegro Presidenta del Directorio</p>
Fecha: 01-09-2023	Fecha: 07-09-2023	Fecha: 06-10-2023	Fecha: 25-10-2023	Fecha: 30-01-2024

<b>NOMBRE DOCUMENTO</b>	<b>POLÍTICA GENERAL DE DATOS LA ARAUCANA</b>			
<b>CÓDIGO</b>	<b>FECHA DE REALIZACIÓN</b>	<b>ELABORADO</b>	<b>REVISADO</b>	<b>APROBADO</b>
<b>PO-GDAT-036</b>	<b>Agosto – 2023</b>	<b>Gobierno de Datos</b>	<b>Subgca. Ciberseg. / Jefe de Div. Sist. / Fiscalía / Gcia. Planif. Estrat. y Control de Gestión / Gcia. de Ec. Digitales / Gcia. Contralor / Gcia. General</b>	<b>Comité de Transformación y Tecnología / Directorio</b>
<b>VERSION</b>	<b>FECHA APROBACIÓN</b>			
<b>001</b>	<b>30-01-2024</b>			

## Contenido

I. Objetivo .....	3
II. Alcance .....	3
III. Conceptos Esenciales .....	4
IV. Marco de Referencia .....	7
V. Gobierno de Datos Corporativo .....	7
5.1 Roles y Responsabilidades .....	7
5.2 Principios generales .....	8
5.3 Lineamientos Generales de Gobierno de Datos .....	9
5.3.1 Requerimiento de Negocio .....	9
5.3.2 Requerimientos Regulatorios .....	9
5.4 Lineamiento General de Protección de datos .....	10
5.4.1 Definir Niveles de Confidencialidad de Datos .....	11
5.4.2 Definir Categorías Regulatorias de Datos .....	11
5.4.3 Definir Roles de Seguridad .....	11
5.4.4 Evaluar riesgos de Seguridad Actual .....	11
5.4.5 Implementar Controles y procedimientos .....	11
5.5 Lineamiento para consentimiento de Datos .....	12
5.6 Derechos ARCO .....	12
5.6.1 Acceso a la información .....	12
5.6.2 Rectificación .....	13
5.6.3 Cancelación o Supresión .....	13
5.6.4 Oposición .....	13
5.6.5 Derechos Complementarios .....	14
VI. Política General de Datos .....	14
6.1 Políticas de tratamiento de activos estratégicos .....	14
6.2 Políticas específica de Seguridad de Información y datos .....	15
6.2.1 Políticas de control de acceso .....	15
6.2.2 Políticas de protección de datos .....	16
6.2.3 Políticas de Cumplimiento .....	16
VII. Aplicación de la Política de Datos .....	16
VIII. Frecuencia de Revisión y Actualización .....	17
IX. Sanciones por incumplimiento de la Política .....	17
X. Tabla de Control de Cambios .....	17

<b>NOMBRE DOCUMENTO</b>	<b>POLÍTICA GENERAL DE DATOS LA ARAUCANA</b>			
<b>CÓDIGO</b>	<b>FECHA DE REALIZACIÓN</b>	<b>ELABORADO</b>	<b>REVISADO</b>	<b>APROBADO</b>
<b>PO-GDAT-036</b>	<b>Agosto – 2023</b>	<b>Gobierno de Datos</b>	<b>Subgca. Ciberseg. / Jefe de Div. Sist. / Fiscalía / Gcia. Planif. Estrat. y Control de Gestión / Gcia. de Ec. Digitales / Gcia. Contralor / Gcia. General</b>	<b>Comité de Transformación y Tecnología / Directorio</b>
<b>VERSION</b>	<b>FECHA APROBACIÓN</b>			
<b>001</b>	<b>30-01-2024</b>			

## I. Objetivo


El objetivo de contar con la Política General de Datos tiene relación con incorporar las regulaciones vigentes en la materia de privacidad, protección, confidencialidad, disponibilidad, integridad y auditoría, las cuales permitirán definir los estándares de la Caja, proteger todos los datos y activos de información físicos y digitales de la Caja en concordancia con los acuerdos contractuales y requerimientos de negocio tales como:

- Partes interesadas:** Reconocer necesidades de seguridad y privacidad de nuestros afiliados, proveedores o socios de negocio.
- Regulaciones gubernamentales:** Dichas regulaciones no solo restringen el acceso a la información, la obtención de datos de terceras partes mediante convenios, tecnologías y otros sino también, como puede ser usada con transparencia y rendición de cuentas.
- Interés del negocio:** Los datos de la Caja entregan información sobre nuestros afiliados, si los datos confidenciales son robados o vulnerados, podemos perder ventaja competitiva y el impacto en la reputación de la Caja.
- Acceso restringido:** Los procesos de negocio de la Caja requieren que los trabajadores con determinados roles puedan acceder, mantener y utilizar los datos.
- Obligaciones contractuales:** Los acuerdos contractuales y de confidencialidad deben ser considerados en los requerimientos de seguridad de datos.
- Deber de protección y exactitud de datos:** Los datos de la Caja deben ser resguardados y protegidos a lo largo de todo el ciclo de vida de los datos, desde su captura, creación, almacenamiento, utilización y eliminación velando siempre por la exactitud y veracidad de estos.
- Derecho del titular de datos:** Los afiliados de la Caja podrá en todo momento ejercer los derechos otorgados por la ley sobre protección de datos vigentes.

## II. Alcance

La Política General de Datos de La Araucana aplica a todas las personas y unidades de negocio de la Caja y su foco comprende lo siguiente:

*“Será el marco de referencia para garantizar que las personas adecuadas puedan capturar, usar y actualizar los datos físicos y/o digitales de manera correcta, resguardar y proteger los datos y que todo acceso y actualización inapropiada esté restringida.*


NOMBRE DOCUMENTO	POLÍTICA GENERAL DE DATOS LA ARAUCANA			
CÓDIGO	FECHA DE REALIZACIÓN	ELABORADO	REVISADO	APROBADO
PO-GDAT-036	Agosto – 2023	Gobierno de Datos	Subgca. Ciberseg. / Jefe de Div. Sist. / Fiscalía / Gcia. Planif. Estrat. y Control de Gestión / Gcia. de Ec. Digitales / Gcia. Contralor / Gcia. General	Comité de Transformación y Tecnología / Directorio
VERSION	FECHA APROBACIÓN			
001	30-01-2024			

*Por otro lado, entregará un lineamiento sobre cómo entender y cumplir con todas las regulaciones y políticas relevantes para que la recopilación, privacidad, protección y confidencialidad sean abordadas al usar los datos “.*


### III. Conceptos Esenciales

Para efectos de la siguiente política se consideran los siguientes conceptos y definiciones:


- **Dato:** Se define como una representación simbólica de un hecho, concepto, entidad o atributo en forma de número, letra, imágenes, sonidos, etc. Los datos son elementos básicos que se utilizan como insumos para obtener información y conocimiento a través de distintos procesos de interpretación y análisis.
- **Datos Personales:** Según la ley 19.628, los datos personales son toda aquella información que puede utilizarse para identificar a una persona o que esté relacionada con una persona ya identificada, con el objetivo de resguardar su privacidad y garantizar que estos datos sean utilizados de manera adecuada y segura por parte de la organización y entidades que los recopilan. Por otro lado, dicha ley otorga a los titulares de los datos personales ciertos derechos como el acceso, rectificación y la cancelación u oposición en determinadas circunstancias.
- **Datos personales sensibles:** Aquellos datos personales que revelen el origen étnico o racial, la afiliación política, sindical o gremial, las convicciones ideológicas o filosóficas, las creencias religiosas, los datos relativos a la salud, al perfil biológico humano, los datos biométricos, y la información relativa a la vida sexual, a la orientación sexual y a la identidad de género de una persona natural.
- **Dato Caduco:** Es el que perdió actualidad por disposición de la ley, por el cumplimiento de la condición o la expiración del plazo señalado para su vigencia o, si no hubiere norma expresa, por el cambio de los hechos o circunstancias que consigna.
- **Metadato:** Consiste en la información de datos que describen otros datos. Proporciona información acerca de la estructura y características de los propios archivos de datos. Se caracterizan por ser datos sumamente estructurados que contienen información acerca del tamaño, contenido, calidad y otros atributos de los archivos.
- **Ciclo de vida del dato:** Consta de una serie de fases en la vida útil del dato, desde la creación de datos, almacenamiento de datos, intercambio y uso de datos, archivo de datos y eliminación de datos. La gestión del ciclo de vida del dato tiene beneficios en la mejora de procesos, control de costos, usabilidad de los datos y Conformidad regulatoria y gestión de datos.

<b>NOMBRE DOCUMENTO</b>	<b>POLÍTICA GENERAL DE DATOS LA ARAUCANA</b>			
<b>CÓDIGO</b>	<b>FECHA DE REALIZACIÓN</b>	<b>ELABORADO</b>	<b>REVISADO</b>	<b>APROBADO</b>
<b>PO-GDAT-036</b>	<b>Agosto – 2023</b>	<b>Gobierno de Datos</b>	<b>Subgca. Ciberseg. / Jefe de Div. Sist. / Fiscalía / Gcia. Planif. Estrat. y Control de Gestión / Gcia. de Ec. Digitales / Gcia. Contralor / Gcia. General</b>	<b>Comité de Transformación y Tecnología / Directorio</b>
<b>VERSION</b>	<b>FECHA APROBACIÓN</b>			
<b>001</b>	<b>30-01-2024</b>			

- **Tratamiento de Datos:** Cualquier operación o conjunto de operaciones o procedimientos técnicos, de carácter automatizado o no, que permitan utilizar de cualquier forma datos personales o conjuntos de datos personales a lo largo del Ciclo de vida del dato.
- **Comunicación de transmisión de datos:** Dar a conocer de cualquier forma los datos de carácter personal a personas distintas al titular, sean determinadas o indeterminadas.
- **Almacenamiento de Datos:** La conservación o custodia de datos en un registro o banco de datos.
- **Atributos Críticos:** Son todos aquellos atributos que, de acuerdo con su definición y características propias, son identificados como importantes para la comprensión del Dominio al que está relacionado además de tener un impacto directo y medible en las necesidades del negocio.
- **Consentimiento:** Toda manifestación de voluntad libre, específica, inequívoca e informada, otorgada a través de una declaración o una clara acción afirmativa, mediante la cual el titular de datos, su representante legal o mandatario, según corresponda, autoriza el tratamiento de los datos personales que le conciernen.
- **Fuente de acceso público:** Son todas aquellas bases de datos personales, públicas o privadas, cuyo acceso o consulta puede ser efectuado en forma lícita por cualquier persona, sin excluir restricciones o impedimentos legales para su acceso o utilización.
- **Información Pública:** La información pública se refiere a los datos, documentos y contenido que están disponibles y accesibles para el público en general sin restricciones significativas. Estos datos son considerados como parte del dominio público y su acceso no está limitado a grupos específicos o individuos. La gestión adecuada de la información pública es esencial para promover la transparencia, la rendición de cuentas y el compromiso ciudadano en el funcionamiento del gobierno.
- **Información Privada:** La Información privada se refiere a los datos que están protegidos por regulaciones y leyes de privacidad y que tienen restricciones en su uso, acceso y divulgación. Estos datos contienen información personal sensible que pertenece a individuos o entidades y que requiere protección especial para prevenir su uso indebido, acceso no autorizado o exposición no deseada.
- **Información Confidencial:** La información confidencial se refiere a los datos y la información que requieren un nivel especial de protección debido a su sensibilidad, valor estratégico o la necesidad de cumplir con regulaciones y políticas de privacidad.
- **Gobierno de Datos:** Es una estructura organizativa que sirve para dar soporte y resguardo a la gestión de los datos y activos de datos de La Caja. Está formado por un conjunto de normas, políticas y procesos que permiten asegurar que los datos de la organización sean correcto, fiables, seguro, útiles y alineados con la estrategia permitiendo generar valor a partir del uso de los datos.

<b>NOMBRE DOCUMENTO</b>	<b>POLÍTICA GENERAL DE DATOS LA ARAUCANA</b>			
<b>CÓDIGO</b>	<b>FECHA DE REALIZACIÓN</b>	<b>ELABORADO</b>	<b>REVISADO</b>	<b>APROBADO</b>
<b>PO-GDAT-036</b>	<b>Agosto – 2023</b>	<b>Gobierno de Datos</b>	<b>Subgca. Ciberseg. / Jefe de Div. Sist. / Fiscalía / Gcia. Planif. Estrat. y Control de Gestión / Gcia. de Ec. Digitales / Gcia. Contralor / Gcia. General</b>	<b>Comité de Transformación y Tecnología / Directorio</b>
<b>VERSION</b>	<b>FECHA APROBACIÓN</b>			
<b>001</b>	<b>30-01-2024</b>			

- **Data & Analytics Driven:** Una organización “Data & Analytics Driven” se refiere a una organización que toma sus decisiones estratégicas y operativas basadas en datos y análisis en lugar de depender principalmente de la intuición o experiencias personales. En una organización Data Driven se prioriza la recopilación, almacenamiento y análisis de datos para generar información y respaldar todas las acciones y decisiones tomadas. El uso de datos para generación de análisis considera la utilización de información personal anonimizada.
- **Política de Seguridad de Datos:** Conjunto de normas y directrices que son usadas para establecer los lineamientos sobre la implementación de sistemas de Gestión de Seguridad de la Información, junto con determinar medidas preventivas que permitan asegurar la confidencialidad, integridad y disponibilidad de la información y que permita mantener la continuidad operativa y fomentar el desarrollo de una cultura de seguridad de la información.
- **Derecho ARCO:** Son un conjunto de derechos que se refieren a la protección de datos personales en el ámbito de la privacidad y la regulación de la información personal de nuestros afiliados y trabajadores. Se utiliza para garantizar que las personas tengan control sobre sus datos personales en relación con el acceso, rectificación, cancelación y oposición sobre sus datos personales.
- **Ley Marco sobre Ciberseguridad e Infraestructura crítica de la información:** tiene por objetivo establecer la institucionalidad indispensable para robustecer la ciberseguridad, ampliar y fortalecer el trabajo preventivo, formar una cultura pública en materia de seguridad digital, enfrentar las contingencias en el sector público y privado y resguardar la seguridad de las personas en el ciberespacio.
- **ANCI:** Agencia Nacional de Ciberseguridad, servicio público funcionalmente descentralizado, dotado de personalidad jurídica y patrimonio propio, de carácter técnico y especializado, cuyo objeto es el de asesorar al presidente en materias propias de ciberseguridad, colaborar en la protección de los intereses nacionales en el ciberespacio, coordinar el actuar de las instituciones con competencia en materia de ciberseguridad, velar por la protección, promoción y respecto del derecho a la seguridad informática; y coordinar y supervisar la acción de los organismos de la administración del Estado en materia de ciberseguridad.
- **CSIRT:** Agencia gubernamental chilena dependiente del Ministerio del Interior y Seguridad Pública encargada de fortalecer y promover buenas prácticas, políticas, leyes, reglamentos, protocolos y estándares de ciberseguridad en los órganos de la administración del Estado, las infraestructuras críticas del país y la República de Chile en su conjunto.
- **Ley de protección de datos personales:** tiene como objetivo principal garantizar el derecho a la privacidad y proteger los datos personales de las personas físicas. La Ley se aplica al tratamiento de datos personales realizado por todos los contribuyentes, particulares, empresas y organizaciones.

<b>NOMBRE DOCUMENTO</b>	<b>POLÍTICA GENERAL DE DATOS LA ARAUCANA</b>			
<b>CÓDIGO</b>	<b>FECHA DE REALIZACIÓN</b>	<b>ELABORADO</b>	<b>REVISADO</b>	<b>APROBADO</b>
<b>PO-GDAT-036</b>	<b>Agosto – 2023</b>	<b>Gobierno de Datos</b>	<b>Subgca. Ciberseg. / Jefe de Div. Sist. / Fiscalía / Gcia. Planif. Estrat. y Control de Gestión / Gcia. de Ec. Digitales / Gcia. Contralor / Gcia. General</b>	<b>Comité de Transformación y Tecnología / Directorio</b>
<b>VERSION</b>	<b>FECHA APROBACIÓN</b>			
<b>001</b>	<b>30-01-2024</b>			

- **Ley de Delitos Económico:** En términos generales, la Ley establece un estatuto diferenciado de determinación de pena para los denominados “delitos de cuello y corbata”, aumentando las sanciones y ampliando el catálogo de delitos imputables a las empresas. En este sentido, cuando el delito tenga una pena teórica de presidio o reclusión (cárcel) es mucho más probable que deba cumplirse efectivamente con privación de libertad, ya que lo que busca esta nueva legislación es evitar que se produzca la sensación de impunidad frente a la comisión de delitos económicos, teniendo en cuenta el impacto social, económico y medioambiental que estos pudiesen tener.

#### IV. Marco de Referencia

Para gobernar el comportamiento relacionado con la seguridad de los datos y la información de la Caja, se requiere de un conjunto de niveles de políticas actuales, tales como:

- PO-SIEN-014 Política General de Seguridad de la información
- Ley N°19.628 – Sobre protección de la Vida privada o protección de datos de carácter personal.
- PR-LACI-190 Procedimiento para el levantamiento de activos de información.
- PR-PEDP-157 Procedimiento de protección y eliminación segura de datos personales.
- PR-ABMU-009 Procedimiento de alta, baja y modificación de usuarios

#### V. Gobierno de Datos Corporativo


##### 5.1 Roles y Responsabilidades

Con el objetivo de guiar a la organización en la creación de una cultura de datos que nos permita lograr nuestro objetivo de ser una organización Data & Analytics Driven, se definen los siguientes Roles y Responsabilidades de los trabajadores que deben contribuir siendo embajadores para la correcta ejecución de la estrategia de datos de la Caja.

**Chief Data Officer (CDO):** Ejecutivo que tiene la autoridad e influencia para definir y dirigir la implementación y mantenimiento de la Estrategia de Datos de la Caja. Es el sponsor que debe ser parte de la mesa de datos para asegurar el correcto lineamiento de la estrategia de datos con la estrategia de la organización.

**Executive Data Steward:** Ejecutivo cuya finalidad es definir la estrategia y garantizar el correcto uso de los datos asociados a su o sus dominios, para lo cual, deberá habilitar roles que serán responsables de definir, autorizar, orientar y aprobar reglas de negocio y de calidad asociadas a los datos.



<b>NOMBRE DOCUMENTO</b>	<b>POLÍTICA GENERAL DE DATOS LA ARAUCANA</b>			
<b>CÓDIGO</b>	<b>FECHA DE REALIZACIÓN</b>	<b>ELABORADO</b>	<b>REVISADO</b>	<b>APROBADO</b>
<b>PO-GDAT-036</b>	<b>Agosto – 2023</b>	<b>Gobierno de Datos</b>	<b>Subgca. Ciberseg. / Jefe de Div. Sist. / Fiscalía / Gcia. Planif. Estrat. y Control de Gestión / Gcia. de Ec. Digitales / Gcia. Contralor / Gcia. General</b>	<b>Comité de Transformación y Tecnología / Directorio</b>
<b>VERSION</b>	<b>FECHA APROBACIÓN</b>			
<b>001</b>	<b>30-01-2024</b>			

**Data Owner / Data Steward:** Definir e identificar nuevas necesidades de sus Dominios de Datos, siendo responsables por la operatividad, entendimiento y validación de los datos asociados a los Dominio que son responsables.

**Data Technical Steward:** Responsables de resolver necesidades o incidencias relacionados con las implementaciones y administración técnica de los datos. Proporcionan información sobre la usabilidad y el consumo desde el punto de vista técnico de los datos.

**Mesa de Gobierno de Datos:** Es una instancia liderada por el CDO y conformada por líderes de distintas áreas tecnológicas, cuya función principal es la de definir y resolver distintos requerimientos y necesidades de datos, las cuales deberán estar alineados con la Estrategia y Políticas de Datos y como consecuencia, con la Estrategia de la organización.

**Equipos de Datos:** Equipo de trabajadores internos o externos cuya finalidad es contribuir desde su expertise con el desarrollo de las distintas iniciativas, siempre desde el punto de vista de los datos. Son responsables de mantener el lineamiento del negocio, calidad, estándares y políticas definidas por el Gobierno de datos y como resultado de ello, garantizar la disponibilidad de los productos de datos que sean requeridos.

Alineados con el objetivo descrito anteriormente, otros roles importantes y que por su puesto están asociados a la seguridad de los datos, son los siguientes:

**Área de Ciberseguridad:** Equipo responsable de definir y poner en práctica los mecanismos necesarios para la protección y resguardo de datos tanto internos como externos y la capacitación continua para generar una cultura de ciberseguridad en la organización.

**Auditoría Interna:** Equipo responsable de evaluar y controlar que los mecanismos de seguridad estén funcionando en forma correcta, identificando posibles brechas de seguridad que permitan tener una actitud proactiva frente a las amenazas.


## 5.2 Principios generales

**Enfoque empresarial:** Las políticas y estándares de seguridad de los datos, deben ser aplicados de manera uniforme en toda la organización.

**Colaboración:** De forma similar a la operación de Gobierno de Datos, la seguridad de datos es un esfuerzo colaborativo entre las distintas áreas y roles involucrados con la finalidad de proteger y cumplir con los requerimientos normativos a los que está sujeta la Caja.

**Comunicación:** Todos los acuerdos y lineamientos que se generen desde el Gobierno de Datos deben ser complementados con un plan comunicacional que permita mantener claramente informados a todas las personas y áreas involucradas de la Caja.



<b>NOMBRE DOCUMENTO</b>	<b>POLÍTICA GENERAL DE DATOS LA ARAUCANA</b>			
<b>CÓDIGO</b>	<b>FECHA DE REALIZACIÓN</b>	<b>ELABORADO</b>	<b>REVISADO</b>	<b>APROBADO</b>
<b>PO-GDAT-036</b>	<b>Agosto – 2023</b>	<b>Gobierno de Datos</b>	<b>Subgca. Ciberseg. / Jefe de Div. Sist. / Fiscalía / Gcia. Planif. Estrat. y Control de Gestión / Gcia. de Ec. Digitales / Gcia. Contralor / Gcia. General</b>	<b>Comité de Transformación y Tecnología / Directorio</b>
<b>VERSION</b>	<b>FECHA APROBACIÓN</b>			
<b>001</b>	<b>30-01-2024</b>			

**Seguridad de Información proactiva:** El éxito de la gestión de la seguridad de los datos depende de que los lineamientos sean proactivos y dinámicos, involucre a todas las partes interesadas, gestione el cambio superando obstáculos culturales e identificando las responsabilidades entre la seguridad, las tecnologías y los administradores de datos.

**Protección y resguardo de datos:** Los datos al se tratados como un activo estratégico de la organización deben ser rigurosamente resguardados a lo largo de todo su ciclo de vida por los trabajadores de la Caja con el objetivo de disminuir o mitigar los riesgos asociados a brechas de seguridad de la información.

**Cumplimiento Normativo:** Debido a que las CCAF como La Araucana están reguladas por otros organismos, es necesario que el Gobierno de Datos indique los lineamientos necesarios para el cumplimiento de las regulaciones asociadas a los datos.

**Calidad de Datos:** Los Roles y Responsabilidades definidas, junto con el área de Gobierno de Datos, serán los responsables de garantizar que los datos son consistentes, precisos y completos.

**Rendición de Cuentas:** Los Roles y Responsabilidades deben ser claramente definidos, incluyendo la “cadena de custodia” de los datos a través de la organización y sus funciones.

### 5.3 Lineamientos Generales del Gobierno de Datos

#### 5.3.1 Requerimiento de Negocio


Las necesidades de negocios de una empresa, su misión, estrategia y tamaño, y la industria a la que pertenece, definen el grado de rigidez requerido para la seguridad de los datos. Es necesario analizar las reglas y procesos de negocio para identificar los puntos críticos de seguridad.

#### 5.3.2 Requerimientos Regulatorios

El entorno dinámico y global actual requiere que las organizaciones deban cumplir con una serie de regulaciones y leyes según su ámbito. Los gobiernos establecen nuevas leyes y estándares para abordar los problemas éticos y legales que afectan a las organizaciones, los cuales imponen estrictos controles de seguridad de la información.

La tabla a continuación contiene un listado de regulaciones que la Caja debe cumplir.

Regulación	Área temática	Enlace de Política de Seguridad	Controles implementados
<b>SUSESO - LIBRO V. ASPECTOS OPERACIONALES Y ADMINISTRATIVOS</b>	Relación de las CCAF con los afiliados	Política de privacidad respecto de datos personales del afiliado	

<b>NOMBRE DOCUMENTO</b>	<b>POLÍTICA GENERAL DE DATOS LA ARAUCANA</b>			
<b>CÓDIGO</b>	<b>FECHA DE REALIZACIÓN</b>	<b>ELABORADO</b>	<b>REVISADO</b>	<b>APROBADO</b>
<b>PO-GDAT-036</b>	<b>Agosto – 2023</b>	<b>Gobierno de Datos</b>	<b>Subgca. Ciberseg. / Jefe de Div. Sist. / Fiscalía / Gcia. Planif. Estrat. y Control de Gestión / Gcia. de Ec. Digitales / Gcia. Contralor / Gcia. General</b>	<b>Comité de Transformación y Tecnología / Directorio</b>
<b>VERSION</b>	<b>FECHA APROBACIÓN</b>			
<b>001</b>	<b>30-01-2024</b>			

<b>SUSESO - LIBRO V. ASPECTOS OPERACIONALES Y ADMINISTRATIVOS</b>	Actividades de Control	Control de Información	Sistemas de
---	------------------------	------------------------	-------------

### 5.3.2.1 Privacidad respecto de datos personales del afiliado

Teniendo presente lo dispuesto en el artículo 19 N°4 de la Constitución Política de la República y en las normas pertinentes de la ley N°19.628, sobre protección de la vida privada y sus modificaciones, las Cajas deben implementar mecanismos que permitan asegurar la confidencialidad y seguridad de la información de los datos personales que puedan haber solicitado a sus afiliados a propósito del otorgamiento de alguna de las prestaciones que administre. Lo anterior, en el marco de la regulación contenida en la ya citada Ley N°19.628 indicada.

### 5.3.2.2 Control de los Sistemas de Información


Los controles a los sistemas de información y los sistemas de seguridad de la información deben estar referidos a los controles de los riesgos identificados en las actividades sistémicas, esto es, controles sobre las operaciones ejecutadas en los sistemas, en los centros de procesamientos de datos, de arquitectura de los sistemas, integridad de los datos, sobre la seguridad física y lógica de los datos, la ejecución y/o contratación y mantenimiento del hardware y software, perfiles de acceso, controles de acceso físico y lógico a instalaciones o sistemas y controles sobre desarrollo, mantenimiento e implementación y aseguramiento de la calidad de los sistemas informáticos y de aplicaciones.

Se encuentran dentro de esta categoría de controles los procesos de respaldo de datos y recuperación de caídas de los sistemas informáticos, contemplados en los respectivos planes de continuidad operativa. Esos controles deben ser aplicados a toda la tecnología crítica incluyendo, al menos, los sistemas principales, servidores, bases de datos, almacenamiento de datos, redes de comunicación, enlaces de datos y voz y computadores personales.

## 5.4 Lineamiento General de Protección de datos

Se requieren diferentes niveles de políticas para gobernar el comportamiento relacionado con la seguridad de datos de la Caja. Es obligación de los trabajadores resguardar y proteger los datos en todo el ciclo de vida de este.

Las políticas de seguridad deben estar en un formato fácilmente accesible para los afiliados, trabajadores y grupos de interés. Deben estar disponibles y mantenerse en la intranet de la Caja o en un portal similar de colaboración.

<b>NOMBRE DOCUMENTO</b>	<b>POLÍTICA GENERAL DE DATOS LA ARAUCANA</b>			
<b>CÓDIGO</b>	<b>FECHA DE REALIZACIÓN</b>	<b>ELABORADO</b>	<b>REVISADO</b>	<b>APROBADO</b>
<b>PO-GDAT-036</b>	<b>Agosto – 2023</b>	<b>Gobierno de Datos</b>	<b>Subgca. Ciberseg. / Jefe de Div. Sist. / Fiscalía / Gcia. Planif. Estrat. y Control de Gestión / Gcia. de Ec. Digitales / Gcia. Contralor / Gcia. General</b>	<b>Comité de Transformación y Tecnología / Directorio</b>
<b>VERSION</b>	<b>FECHA APROBACIÓN</b>			
<b>001</b>	<b>30-01-2024</b>			

Los privilegios de acceso a la información serán revisados anualmente y podrán ser revocados en caso de que ya no sea necesario para un usuario la utilización de la información para el desempeño de sus funciones.

#### **5.4.1 Definir Niveles de Confidencialidad de Datos**

La clasificación de confidencialidad es una característica importante de los Metadatos, que guía como se otorga los privilegios de acceso a los usuarios. Es necesario adoptar una clasificación que cumpla con los requerimientos de negocio. La finalidad es clasificar desde niveles menos confidenciales hasta los más confidenciales.

#### **5.4.2 Definir Categorías Regulatorias de Datos**

Las crecientes violaciones a información confidencial o sensible que se han visto comprometidas han generado que se hayan incorporado leyes específicas por los organismos gubernamentales. Los requerimientos regulatorios son una extensión de la seguridad y protección de datos.

Una forma adecuada de manejar las regulaciones de los datos es analizando y agrupando regulaciones similares en categorías.

#### **5.4.3 Definir Roles de Seguridad**

El control de acceso a los datos se puede organizar por niveles individuales o grupales, según se requiera. En el caso de La Araucana, es recomendable administrar el control de acceso basado en roles, otorgando permisos a cada grupo de roles y, por lo tanto, a cada miembro del grupo.

La seguridad basada en roles depende de roles claramente definidos y constantemente asignados.

#### **5.4.4 Evaluar riesgos de Seguridad Actual**


El primer paso para identificar los riesgos es identificar donde se almacenan los datos sensibles y que protección se requiere para esos datos así como quienes y desde donde acceden a esta información.

Es mandatorio documentar los hallazgos ya que crean una línea base para futuras evaluaciones. Las brechas deben ser corregidas mediante procesos de seguridad compatibles con la tecnología.

#### **5.4.5 Implementar Controles y procedimientos**

La implementación y administración de la política de seguridad de datos es responsabilidad de los administradores de seguridad, en coordinación con los administradores de Datos, los equipos técnicos y de todos los trabajadores que tienen acceso a dicha información.

La Caja debe implementar controles estrictos para cumplir con los requerimientos de la política de seguridad.

<b>NOMBRE DOCUMENTO</b>	<b>POLÍTICA GENERAL DE DATOS LA ARAUCANA</b>			
<b>CÓDIGO</b>	<b>FECHA DE REALIZACIÓN</b>	<b>ELABORADO</b>	<b>REVISADO</b>	<b>APROBADO</b>
<b>PO-GDAT-036</b>	<b>Agosto – 2023</b>	<b>Gobierno de Datos</b>	<b>Subgca. Ciberseg. / Jefe de Div. Sist. / Fiscalía / Gcia. Planif. Estrat. y Control de Gestión / Gcia. de Ec. Digitales / Gcia. Contralor / Gcia. General</b>	<b>Comité de Transformación y Tecnología / Directorio</b>
<b>VERSION</b>	<b>FECHA APROBACIÓN</b>			
<b>001</b>	<b>30-01-2024</b>			

Los controles deben ser monitoreados y reportados de forma periódica en los comités correspondientes de gobiernos de datos, seguridad de información y afines.

### 5.5 Lineamiento para consentimiento de Datos

Según lo dispuesto en el Artículo 12 de la Ley 19.628, se indica lo siguiente:

Es lícito el tratamiento de los datos personales que le conciernen al titular, **cuando otorgue su consentimiento para ello**. El consentimiento del titular debe ser libre, informado y específico en cuanto a su finalidad o finalidades.

El consentimiento debe manifestarse, además, en forma previa y de manera inequívoca, mediante una declaración verbal, escrita o expresada a través de un medio electrónico equivalente, o mediante un acto afirmativo que dé cuenta con claridad de la voluntad del titular. Cuando el consentimiento lo otorgue un mandatario, éste deberá encontrarse expresamente premunido de esta facultad.

El titular puede revocar el consentimiento otorgado en cualquier momento y sin expresión de causa, utilizando medios similares o equivalentes a los empleados para su otorgamiento. La revocación del consentimiento no tendrá efectos retroactivos.

Los medios utilizados para el otorgamiento o la revocación del consentimiento deben ser expeditos, fidedignos, gratuitos y estar permanentemente disponibles para el titular.

Se presume que el consentimiento para tratar datos no ha sido libremente otorgado cuando el responsable lo recaba en el marco de la ejecución de un contrato o la prestación de un servicio en que no es necesario efectuar esa recolección.

Con todo, lo dispuesto en el texto anterior, no se aplicará en los casos cuando quien ofrezca bienes, servicios o beneficios, requiera como única contraprestación el consentimiento para tratar datos. Corresponde a la Caja, probar que contó con el consentimiento del titular y que el tratamiento de datos fue realizado en forma lícita, leal y transparente.


### 5.6 Derechos ARCO

El titular de los datos tiene derecho a solicitar y obtener del responsable (La Caja) lo siguiente:

#### 5.6.1 Acceso a la información

Obtener una confirmación acerca de, si los datos personales que le conciernen están siendo tratados, y en tal caso, acceder a dichos datos y a la siguiente información:

1. Los datos tratados y su origen.
2. La finalidad o finalidades del tratamiento.

<b>NOMBRE DOCUMENTO</b>	POLÍTICA GENERAL DE DATOS LA ARAUCANA			
<b>CÓDIGO</b>	<b>FECHA DE REALIZACIÓN</b>	<b>ELABORADO</b>	<b>REVISADO</b>	<b>APROBADO</b>
PO-GDAT-036	Agosto – 2023	Gobierno de Datos	Subgca. Ciberseg. / Jefe de Div. Sist. / Fiscalía / Gcia. Planif. Estrat. y Control de Gestión / Gcia. de Ec. Digitales / Gcia. Contralor / Gcia. General	Comité de Transformación y Tecnología / Directorio
<b>VERSION</b>	<b>FECHA APROBACIÓN</b>			
001	30-01-2024			

3. Las categorías, clases o tipos de destinatarios, o bien, la identidad de cada destinatario, en caso de solicitarlo así el titular, a los que se les hayan comunicado o cedido los datos o se prevea hacerlo.
4. El período de tiempo durante el cual los datos serán tratados.
5. Los intereses legítimos del responsable, cuando el tratamiento se base en lo dispuesto la Ley 19.628.
6. Información significativa sobre la lógica aplicada en el caso de que el responsable realice tratamiento de datos de conformidad con el Artículo 8 de la Ley 19.628 referido al tratamiento de datos por mandato.

La Caja, siempre estará obligada entregar información y a dar acceso a los datos solicitados excepto cuando una ley disponga expresamente lo contrario.

#### 5.6.2 Rectificación

La rectificación de los datos personales que le conciernen y que están siendo tratados por el responsable, cuando sean inexactos, desactualizados o incompletos.

Los datos rectificadas deberán ser comunicados a las personas, entidades u organismos a los cuales La Caja haya comunicado o cedido los referidos datos.

Efectuada la rectificación, no se podrán volver a tratar los datos sin rectificar.

#### 5.6.3 Cancelación o Supresión


La eliminación de los datos personales que le conciernen, especialmente en los siguientes casos:

1. Cuando los datos no resulten necesarios en relación con los fines del tratamiento para el cual fueron recogidos.
2. Cuando el titular haya revocado su consentimiento para el tratamiento y éste no tenga otro fundamento legal.
3. Cuando los datos hayan sido obtenidos o tratados ilícitamente.
4. Cuando se trate de datos caducos.
5. Cuando los datos deban suprimirse para el cumplimiento de una sentencia judicial, de una resolución de la autoridad de protección de datos o de una obligación legal.
6. Cuando el titular haya ejercido su derecho de oposición.

#### 5.6.4 Oposición

Oponerse a que se realice un tratamiento específico o determinado de los datos personales que le conciernan, en los siguientes casos:

1. Cuando la base de licitud del tratamiento sea la satisfacción de intereses legítimos de la Caja.

<b>NOMBRE DOCUMENTO</b>	<b>POLÍTICA GENERAL DE DATOS LA ARAUCANA</b>			
<b>CÓDIGO</b>	<b>FECHA DE REALIZACIÓN</b>	<b>ELABORADO</b>	<b>REVISADO</b>	<b>APROBADO</b>
<b>PO-GDAT-036</b>	<b>Agosto – 2023</b>	<b>Gobierno de Datos</b>	<b>Subgca. Ciberseg. / Jefe de Div. Sist. / Fiscalía / Gcia. Planif. Estrat. y Control de Gestión / Gcia. de Ec. Digitales / Gcia. Contralor / Gcia. General</b>	<b>Comité de Transformación y Tecnología / Directorio</b>
<b>VERSION</b>	<b>FECHA APROBACIÓN</b>			
<b>001</b>	<b>30-01-2024</b>			

2. Si el tratamiento se realiza exclusivamente con fines de mercadotecnia o marketing directo de bienes, productos o servicios.
3. Si el tratamiento se realiza respecto de datos obtenidos de una fuente de acceso público y no existe otro fundamento legal para su tratamiento.

No procederá la oposición al tratamiento cuando este se realice con fines de investigación científica o histórica o fines estadísticos, siempre que fueran necesarios para el cumplimiento de una función pública o para el ejercicio de una actividad de interés público.

## **5.6.5 Derechos Complementarios**

### **5.6.5.1 Portabilidad de los datos personales**

El titular de datos tiene derecho a solicitar y recibir una copia de los datos personales que le conciernen, que haya facilitado a la Caja, en un formato electrónico, estructurado, genérico y de uso común, que permita ser operado por distintos sistemas y, a comunicarlos o transferirlos a otro responsable de datos, cuando concurren las siguientes circunstancias:

- El tratamiento se realice en forma automatizada, y
- El tratamiento esté basado en el consentimiento del titular.

La Caja debe utilizar los medios más expeditos, menos onerosos y sin poner trabas u obstáculos para el ejercicio de este derecho.

La Caja también debe comunicar al titular de manera clara y precisa las medidas necesarias para obtener sus datos personales y especificar las características técnicas para llevar a cabo estas operaciones.

Con todo, el ejercicio del derecho de portabilidad no supondrá la supresión de los datos ante el responsable cedente, a menos que el titular de estos así lo pida conjuntamente en la solicitud.


## **VI. Política General de Datos**

### **6.1 Políticas de tratamiento de activos estratégicos**

La estrategia 2030 de la Caja considera la transformación desde la **“Innovación permanente y experiencia superior para el Afiliado”**. Esto releva la necesidad de definir los procedimientos para el tratamiento de los activos de datos y que éstos respondan a la estrategia de arquitectura, metadata, seguridad, ciberseguridad y cumplimiento que habilitan la transformación.

Para efectos del presente documento, el procedimiento de dicho tratamiento estará dado por:

- Identificación de activos de datos estratégicos: Cód.:PR-LACI-190 Procedimiento para el levantamiento de activos de información

<b>NOMBRE DOCUMENTO</b>	<b>POLÍTICA GENERAL DE DATOS LA ARAUCANA</b>			
<b>CÓDIGO</b>	<b>FECHA DE REALIZACIÓN</b>	<b>ELABORADO</b>	<b>REVISADO</b>	<b>APROBADO</b>
<b>PO-GDAT-036</b>	<b>Agosto – 2023</b>	<b>Gobierno de Datos</b>	<b>Subgca. Ciberseg. / Jefe de Div. Sist. / Fiscalía / Gcia. Planif. Estrat. y Control de Gestión / Gcia. de Ec. Digitales / Gcia. Contralor / Gcia. General</b>	<b>Comité de Transformación y Tecnología / Directorio</b>
<b>VERSION</b>	<b>FECHA APROBACIÓN</b>			
<b>001</b>	<b>30-01-2024</b>			

- Identificación de requisitos de arquitectura:
- Identificación de directrices para identificar, clasificar, determinar la criticidad y analizar riesgos de los activos de información: Cód.:PR-LACI-190 procedimiento para el levantamiento de activos de información.
- Identificación de requisitos de Seguridad y Ciberseguridad: Cód.: PO-SIEN-014 Política general de seguridad de la información.
- Cumplimiento de Protección y Eliminación Segura de Datos Personales: Cód:PR-PEDP-157 procedimiento de protección y eliminación segura de datos personales

**Nota:** *Es necesario considerar que el acceso a los datos unitarios no representa información si no hasta que dichos datos son relacionados con otros, y producto de ello, se logra identificar de forma inequívoca a una persona o sus atributos personales y privados.*

## 6.2 Políticas específica de Seguridad de Información y datos

La Política de Seguridad de la información tiene por objetivo, establecer lineamientos precisos sobre la Administración de la Seguridad de la Información, así como el de determinar el conjunto de medidas preventivas y de control que permitan asegurar estrictos niveles de Confidencialidad, Cumplimiento Normativo, Integridad y Disponibilidad de los datos y la información de La Araucana CCAF. Al mismo tiempo mitigar los riesgos sobre los activos de información, así como impulsar una cultura de seguridad identificando los roles y responsabilidades sobre los datos.

De la Política General de Seguridad de la Información se desprenden las siguientes políticas específicas que complementan e instruyen a todas las áreas, trabajadores internos y externos de la Caja sobre las diferentes responsabilidades y obligaciones que deberán asumir en materias relativas a la seguridad de datos e información.

Las políticas referidas a continuación adoptan las declaraciones y compromisos descritos en el presente documento.


### 6.2.1 Políticas de control de acceso

Con respecto a las Políticas de acceso que rigen a La Caja, estas tienen por objetivo prevenir el acceso no autorizado a los datos que pueda derivar en daños, alteraciones, robo, encriptación o uso no adecuado de los activos de información de la Caja.

Para ello, se hace referencia a lo siguiente:

- Sección **3.1 Política de control de acceso:** Cód: PO-Sein-014 Política General de Seguridad de la Información.



<b>NOMBRE DOCUMENTO</b>	<b>POLÍTICA GENERAL DE DATOS LA ARAUCANA</b>			
<b>CÓDIGO</b>	<b>FECHA DE REALIZACIÓN</b>	<b>ELABORADO</b>	<b>REVISADO</b>	<b>APROBADO</b>
<b>PO-GDAT-036</b>	<b>Agosto – 2023</b>	<b>Gobierno de Datos</b>	<b>Subgca. Ciberseg. / Jefe de Div. Sist. / Fiscalía / Gcia. Planif. Estrat. y Control de Gestión / Gcia. de Ec. Digitales / Gcia. Contralor / Gcia. General</b>	<b>Comité de Transformación y Tecnología / Directorio</b>
<b>VERSION</b>	<b>FECHA APROBACIÓN</b>			
<b>001</b>	<b>30-01-2024</b>			

- Cód: PR-ABMU-009 Procedimiento de Alta, Baja y Modificación de Usuarios.

### 6.2.2 Políticas de protección de datos

En lo relacionado a la protección de datos personales de nuestros afiliados que rigen a La Araucana C.C.A.F., tiene por objetivo establecer los lineamientos orientados a proteger los datos personales y sensibles de nuestros afiliados y trabajadores, estableciendo controles que impidan la filtración o manipulación no autorizada en todo el ciclo de vida de los datos, y para ello se hace referencia a lo siguiente:

- Sección **3.6 Política de protección de datos** del documento: Código: PO-SEIN-014 Política General de Seguridad de la Información.
- Ley 19.628 - Sobre la protección de la vida privada o protección de datos personales y sensibles.
- Código: PR-PEDP-157 Procedimiento de protección y eliminación segura de datos personales.

### 6.2.3 Políticas de Cumplimiento


Existe una serie de compendios de Normas que regulan a las C.C.A.F., las cuales están informadas por la SUSESO y que, entre otros aspectos, hacen referencia a normas de datos que se consideran en la presente política. El objetivo de estas normas es establecer un conjunto de principios, normas internas y un marco de los mejores estándares conforme a los cuales se debe regir el Gobierno Corporativo de las Cajas de Compensación y Asignación Familiar, para que, en su rol de entidades de previsión social, contribuyan al bienestar social de sus afiliados y garantizar el correcto uso de los datos durante el desarrollo de sus actividades.

Para lo anterior, se hace referencia al punto **5.3.2 Requerimiento Regulatorio**, que entrega un lineamiento entregado por la SUSESO con relación a, datos e información de nuestros afiliados.

## VII. Aplicación de la Política de Datos

El presente documento será aplicable una vez que haya sido validado por las distintas áreas participantes en su confección, aprobado por el Directorio y comunicado a la organización por canales formales en La Araucana, junto con disponibilizar el presente documento en distintas plataformas colaborativas como por ejemplo Confluence, Sharepoint y Conectados.

Con respecto al monitoreo continuo, actualización y adecuado cumplimiento, esto deberá estar apoyado por el modelo de responsabilidad expuesto en el punto **5.1 Roles y Responsabilidades** de la presente política, junto con el área de Gobierno de Datos, quienes deberán impulsar no solo las Políticas, sino también de apalancar la Cultura de Datos de la Caja que nos conduzca a convertirnos en una organización Data & Analytics Driven.

<b>NOMBRE DOCUMENTO</b>	<b>POLÍTICA GENERAL DE DATOS LA ARAUCANA</b>			
<b>CÓDIGO</b>	<b>FECHA DE REALIZACIÓN</b>	<b>ELABORADO</b>	<b>REVISADO</b>	<b>APROBADO</b>
<b>PO-GDAT-036</b>	<b>Agosto – 2023</b>	<b>Gobierno de Datos</b>	<b>Subgca. Ciberseg. / Jefe de Div. Sist. / Fiscalía / Gcia. Planif. Estrat. y Control de Gestión / Gcia. de Ec. Digitales / Gcia. Contralor / Gcia. General</b>	<b>Comité de Transformación y Tecnología / Directorio</b>
<b>VERSION</b>	<b>FECHA APROBACIÓN</b>			
<b>001</b>	<b>30-01-2024</b>			

### VIII. Frecuencia de Revisión y Actualización

La presente política será revisado y actualizado al menos una vez al año o cuando sea necesario.

### IX. Sanciones por incumplimiento de la Política

El incumplimiento de las obligaciones establecidas en este procedimiento será sancionado de acuerdo a las disposiciones establecidas en el Título correspondiente del Reglamento Interno de Orden, Higiene y Seguridad de La Araucana C.C.A.F., en concordancia a lo señalado en el numeral 10 del artículo 154 del Código del Trabajo.

Asimismo, las infracciones por incumplimiento de la política podrán constituir una violación a los lineamientos éticos, valores y principios que deben orientar el desempeño de los trabajadores de La Araucana C.C.A.F. consagrados en su Código de Buenas Prácticas y de Conducta, siendo de su responsabilidad aplicarlos en cada una de las actuaciones que el ejercicio de sus funciones demande.

### X. Tabla de Control de Cambios

<b>VERSIÓN</b>	<b>FECHA MODIFICACIÓN</b>	<b>ASPECTOS MODIFICADOS</b>
001	30-01-2024	- Versión inicial del documento. - Sesión de Directorio N° 659.