

POLÍTICA CORPORATIVA DE PROTECCIÓN DE DATOS PERSONALES

A. DISPOSICIONES GENERALES

1. DECLARACIÓN DE LA POLÍTICA

Esta Política expresa formalmente la dirección e intención que CCA otorga respecto al cumplimiento de la normativa que regula el tratamiento de datos personales, tanto para aquellos tratamientos de datos personales de clientes, proveedores, directores, colaboradores o cualquier operación de tratamiento de datos en que esta clase de información intervenga.

2. OBJETIVO

El propósito de este documento es declarar formalmente la posición de CCA, respecto a los principios generales que deben regir el tratamiento de los datos personales en la empresa, asociado a aquellos tratamientos de datos personales de clientes, proveedores, directores y colaboradores o cualquier operación de tratamiento de datos en que esta clase de información intervenga.

Esta Política es una guía de alto nivel, cuyo propósito es orientar las actividades, normas, procedimientos y estándares que rigen a la compañía, con el objetivo de potenciar el sistema financiero chileno a través del procesamiento electrónico de transacciones, pero siempre en un entorno de protección de los derechos de los titulares de datos personales.

Esta Política tiene por objeto garantizar una protección adecuada de los datos personales y la prestación continuada de los servicios, de modo tal que CCA esté preparada para prevenir, detectar, reaccionar y recuperarse de incidentes que afecten el tratamiento de datos personales, con el objeto principal de proteger los derechos y libertades fundamentales de las personas y, en particular, su derecho a la protección de los datos personales, ratificando su compromiso con los derechos humanos.

El régimen de protección de datos personales que se implementa en CCA a través de esta Política debe ser traspuesto e implementado en los diferentes instrumentos que regulan la relación con sus clientes, proveedores y colaboradores.

3. ALCANCE

Este documento contiene los lineamientos mínimos que debe considerar la compañía para el tratamiento de los datos personales en los términos establecidos en el artículo 19 N° 4 de la Constitución Política de la República, la Ley N°19.496 sobre protección de los derechos de los consumidores, de la Ley N°19.628 sobre protección de la vida privada, vigente hasta el 30 de noviembre de 2026 y la nueva Ley N°21.719 sobre protección de datos personales que comenzará

a regir el 01 de diciembre de 2026, así como también la normativa que desarrolla la Comisión para el Mercado Financiero (**CMF**), el Servicio Nacional del Consumidor (**SERNAC**) y que en el futuro pueda establecer la Agencia de Protección de Datos Personales.

La presente política es de aplicación general, comprende a toda la organización, y considera el involucramiento y compromiso de todos los colaboradores, proveedores, contratistas y asesores externos, independientemente de su rango, función o localización.

4. DEFINICIONES

Datos personales: los relativos a cualquier información concerniente a personas naturales, identificadas o identificables. Se considerará identificable toda persona cuya identidad pueda determinarse, directa o indirectamente, mediante información combinada con otros, en particular mediante un identificador, tales como el número de cédula de identidad, el análisis de elementos propios de la identidad física, fisiológica, genética, psíquica, económica, cultural o social de dicha persona, excluyendo aquellos casos en que el esfuerzo de identificación sea desproporcionado.

Son considerados datos personales: el nombre, RUN, número de pasaporte, fotografía, remuneración, domicilio, número telefónico, estado civil, dirección de correo electrónico institucional nombrado, sexo o género, datos bancarios de personas (números de tarjeta de crédito, número de cuenta bancaria) datos de autenticación (claves de acceso, PIN u otros similares), fallos disciplinarios, entre otros.

Dato personal sensible: aquellos datos personales que se refieren a las características físicas o morales o a hechos o circunstancias de su vida privada o intimidad, tales como: los hábitos personales, el origen racial, las ideologías y opiniones políticas, las creencias o convicciones religiosas, los estados de salud físicos o psíquicos y la vida sexual u orientación sexual, identidad de género, identidad genética y biomédica, datos genéticos y datos biométricos, procesados únicamente para identificar a un ser humano.

5. SUJETOS INTERVINIENTES

Titular: es la persona a quién se refieren los datos y sobre la cual se recopila la información.

Responsable: es quien lleva a cabo el tratamiento de los datos personales y que decide cómo y para qué se tratarán los datos. Para efectos de esta política, el responsable es CCA.

Encargado(a) o Mandatario(a): Es quien trata los datos por cuenta del responsable, según sus instrucciones y respetando el propósito definido.

Delegado(a) de Protección de Datos: Es la persona al interior de la empresa que vela por el cumplimiento de las normas de protección de datos.

6. DE CARÁCTER GENERAL

- a. CCA reconoce el cumplimiento de las normativas que rigen a CCA como parte de sus ejes estratégicos, por lo que vela por su permanente cumplimiento.
- b. El o la Delegado (a) de Protección de Datos debe respaldar que los principios recogidos en esta Política sean considerados:
 - Durante el diseño e implantación de los procedimientos establecidos para CCA.
 - En los servicios ofrecidos por CCA.
 - En todos los contratos y obligaciones que se formalicen o se asuman por CCA.
 - En la implantación de los sistemas y plataformas que permitan el acceso de empleados o terceros a la información y/o los datos personales.
- c. La seguridad ha de ser entendida como un proceso integral que involucra a todos y cada uno de los elementos humanos, técnicos, materiales y organizativos relacionados con la operación de CCA. En consecuencia, habrán de adoptarse las medidas oportunas para que todas las personas que intervienen en los procesos de CCA conozcan esta Política y desarrollen sus funciones de conformidad con la misma.
- d. Los principios del tratamiento de dato son normas, con pretensión de carácter universal, que inspirarán la forma y oportunidad en las que se desarrolla el tratamiento de datos personales por los responsables y mandatarios. De este modo los tratamientos de datos quedan siempre regidos por estas normas.
 - Principio de licitud y lealtad del tratamiento. Los datos personales sólo pueden tratarse de manera lícita y leal.
 - Principio de finalidad. Los datos personales deben ser recolectados con fines específicos, explícitos y lícitos. El tratamiento de los datos personales debe limitarse al cumplimiento de estos fines.

En aplicación de este principio, no se puede tratar los datos personales con fines distintos a los informados al momento de la recolección, salvo que el tratamiento sea fines compatibles con los autorizados originalmente, que exista una relación contractual o precontractual entre el titular y el responsable que justifique el tratamiento de los datos con una finalidad distinta, siempre que se enmarque dentro de los fines del contrato o sea coherente con las tratativas o negociaciones previas a la celebración del mismo, que el titular otorgue nuevamente su consentimiento, y cuando lo disponga la ley.

- Principio de proporcionalidad. Los datos personales que se traten deben limitarse a aquellos que resulten necesarios, adecuados y pertinentes en relación con los fines del tratamiento y deben ser conservados sólo por el período de tiempo que sea necesario para cumplir con los fines del tratamiento, luego de lo cual deben ser suprimidos o anonimizados, sin perjuicio de las excepciones que establezca la ley. Un período de

tiempo mayor requiere autorización legal o consentimiento del titular.

- Principio de calidad. Los datos personales deben ser exactos, completos y actuales, en relación con los fines del tratamiento.
 - Principio de responsabilidad. Quienes realicen tratamiento de los datos personales serán legalmente responsables del cumplimiento de los principios, obligaciones y deberes de conformidad a la ley.
 - Principio de seguridad. En el tratamiento de los datos personales, el responsable debe garantizar estándares adecuados de seguridad, protegiéndolos contra el tratamiento no autorizado o ilícito, y contra su pérdida, filtración, daño accidental o destrucción. Las medidas de seguridad deben ser apropiadas y acordes con el tratamiento que se vaya a efectuar y con la naturaleza de los datos.
 - Principio de transparencia e información. Las políticas y las prácticas sobre el tratamiento de los datos personales deben estar permanentemente accesibles y a disposición de cualquier interesado de manera precisa, clara, inequívoca y gratuita.
 - Principio de confidencialidad. El responsable y quienes tengan acceso a ellos deben guardar secreto o confidencialidad acerca de los mismos. El responsable debe establecer controles y medidas adecuadas para preservar el secreto o confidencialidad. Este deber subsiste, aun después de concluida la relación con el titular.
- e. CCA tratará los datos personales a los que tenga acceso únicamente cuando exista una base de licitud que habilite dicho tratamiento de acuerdo con la normativa vigente en materia de Protección de Datos Personales. Estas bases de licitud podrán ser las siguientes:
- Consentimiento del titular de los datos
 - Ejecución de un contrato o medidas precontractuales
 - Cumplimiento de una obligación legal
 - Interés legítimo de CCA o de un tercero, salvo que prevalezcan los derechos de los titulares.
- f. El análisis y la gestión de riesgos es una parte esencial del proceso de seguridad. Los niveles de riesgo han de mantenerse dentro de niveles adecuados, mediante el despliegue de las medidas de seguridad técnicas y organizativas que permitan que se establezca un equilibrio y proporcionalidad entre la naturaleza de los datos personales tratados y las operaciones de tratamiento que se efectúan, los riesgos a los que estén expuestos y las medidas de seguridad aplicadas.
- g. La recolección de datos personales siempre se debe realizar dando pleno cumplimiento a las consideraciones para el tratamiento de datos personales señaladas precedentemente, debiendo en todo caso siempre velarse porque se informe de modo transparente, expreso, preciso e inequívoco, sobre el uso de sus datos. Como norma general, los datos personales que se tratan se recogerán directamente de los titulares, sea que se haga directamente o

cuando se actúe como responsables del tratamiento o a través de mandantes cuando se actúe como mandatarios del tratamiento.

Siempre que se recojan datos personales el titular debe poder reconocer personalmente los siguientes aspectos, o ser informado sobre los mismos:

- La identidad de la instancia responsable que recoge los datos.
- El fin del tratamiento de los datos.
- Los terceros o categorías de terceros a los que se transfieren en su caso los datos.
- La fuente de licitud del tratamiento.
- El plazo de conservación de los datos.
- Los datos de contacto del o la Delegado (a) de Protección de Datos.

CCA sólo tratará datos personales de conformidad con los requisitos establecidos por la ley.

CCA establece un tiempo de conservación de 10 años para la información que recibe de sus clientes y colaboradores, con la finalidad de satisfacer requerimientos legales, de clientes y/o los propios del giro del negocio, como por ejemplo para un uso estadístico. Para dar cumplimiento a ello, la información de más de 10 años debe ser considerada para su eliminación o protegida a través de mecanismos que permitan garantizar la anonimización en el proceso que para estos efectos defina CCA. Respecto de la información que conserve en medios de respaldos u otros, CCA debe evaluar la implementación de medidas de seguridad necesarias para cumplir con las exigencias de la normativa legal vigente, aspectos regulatorios específicos y acuerdos contractuales.

- CCA diseña, implanta, ejecuta y mantiene todas las medidas de seguridad técnicas y organizativas que sean necesarias para garantizar que el tratamiento y la protección de los datos se realicen cumpliendo los más altos estándares de seguridad y confidencialidad.
- La información y los datos recolectados y tratados por CCA se conservan con la máxima confidencialidad y secreto, no siendo utilizados para otros fines que para los que se recolectaron y sin que puedan ser comunicados o cedidos a terceros fuera de los casos permitidos por la ley y de conformidad con los procedimientos legalmente establecidos. Asimismo, se respetan los plazos de conservación señalados para cada caso en concreto.
- Queda prohibida la adquisición, la recolección o la cesión de información o los datos provenientes de fuentes que no puedan garantizar la legítima procedencia de dichos datos o su protección.
- La contratación de mandatarios que en virtud de la actividad o servicio a prestar pudieran tener acceso a información sensible y/o a datos personales cuyo responsable es CCA, debe encontrarse regulada debidamente por un contrato que considere al menos: el objeto del encargo, la duración de este, la finalidad del tratamiento de los datos personales, el tipo de

datos personales que serán tratados, las categorías de titulares a quienes se refieren los datos personales, los derechos y obligaciones de las partes y la forma en que esta Política le será aplicable. La forma en que el tratamiento de datos sea realizado por el mandatario debe ser verificada durante la vigencia de la relación contractual.

La aptitud del mandatario debe ser confirmada, asegurándose que reúne las cualidades necesarias para evitar que los derechos de los titulares de datos puedan ser afectados por la forma en que este realiza el tratamiento y, en consecuencia, pueda convertirse en una fuente de riesgo para CCA.

7. DE GOBIERNO

El cumplimiento de esta Política considera la siguiente estructura de roles y responsabilidades:

a. Directorio

- i. En conjunto con sus comités de apoyo, tiene la responsabilidad última de propender y generar que la Administración de CCA establezca y mantenga implementado un sistema adecuado, efectivo y eficiente de cumplimiento de la normativa sobre protección de datos personales.
- ii. Tiene la responsabilidad de aprobar esta Política y sus actualizaciones. Además, de ejercer un adecuado seguimiento de las definiciones y del cumplimiento de la Política.
- iii. Le corresponde informarse del proceso de cumplimiento de las normativas sobre protección de datos personales, considerando dentro de sus actividades:
 - Aprobar la elección y designación del o la Delegado(a) de Protección de Datos Personales.
 - Velar porque se den todas las facilidades para permitir que CCA, sus directores, ejecutivos(as), colaboradores, asesores y personal externo cooperen con las autoridades en la investigación que estas realicen para verificar el cumplimiento de la normativa sobre protección de datos personales.

b. Delegado(a) de Protección de Datos.

- i. Velar por que la organización cumpla con la Ley de Protección de Datos Personales vigente y otras regulaciones aplicables.
- ii. Participar en el desarrollo de esta política, en total alineación con la legislación vigente, regulaciones y las buenas prácticas en materia de protección de datos personales.
- iii. Difundir y comunicar la política y/o prácticas de protección de datos personales implementadas al interior de la organización.
- iv. Velar por el cumplimiento de esta política y otras que se desprendan de ella, en todos los

procesos y sistemas de la organización, aplicando un enfoque de monitoreo preventivo y proactivo.

- v. Revisar con el área de Gestión de Personas, los derechos y obligaciones que rigen el tratamiento de datos personales para que sean considerados a nivel contractual con los Colaboradores de CCA.
- vi. Monitorear y evaluar los procesos internos de la organización vinculados con la obtención, uso, explotación, conservación, aprovechamiento, cancelación y transferencia de datos personales, a fin de asegurar que la información sea protegida, tratada conforme a los principios de esta Política.
- vii. Fomentar una cultura de protección de datos personales orientada a elevar el nivel de concienciación del personal y terceros involucrados, como encargados, en el tratamiento de datos personales.
- viii. Apoyar y asesorar a CCA, Directores, ejecutivos(as), colaboradores, personal externo, proveedores, terceros encargados o mandatorios, respecto de las obligaciones y responsabilidades de las disposiciones legales y reglamentarios relativas a la protección de los datos personales y a la regulación de su tratamiento para mantener informado en todo momento.
- ix. Verificar el cumplimiento de las directrices emanadas por el Directorio, los organismos certificadores, contralores y fiscalizadores en materias de protección de datos personales, reportando y alertando de los riesgos a las instancias pertinentes dentro de la organización.
- x. Liderar los procesos de certificación en materia de protección de datos personales al interior de CCA y los procesos de revisión que permitan evidenciar el cumplimiento ante la Agencia de Protección de Datos Personales u otro organismo que establezca la ley o el ente regulador.
- xi. Participar activamente en iniciativas de negocio, señalando los lineamientos y definiciones al interior de la empresa relativas a protección de datos personales, así como también realizar y supervisar las evaluaciones de impacto de protección de datos personales cuando sea necesario, en especial en casos de alto riesgo para la privacidad de datos personales.
- xii. Colaborar y coordinar acciones con otras áreas de la organización como la legal, de tecnologías, sistemas, seguridad de la información, ciberseguridad, negocios e innovación, atención al cliente, personas, entre otras, a efecto de asegurar el debido cumplimiento de esta política y/o prácticas de privacidad en sus procesos internos, formatos, avisos, recursos y gestiones que se lleven a cabo.
- xiii. Asistir a los miembros de la organización en la identificación de los riesgos asociados con la protección y las actividades de tratamiento de datos personales y las medidas a adoptar para velar por el resguardo de los derechos de los titulares de datos personales.
- xiv. Administrar procedimientos para la recepción, tramitación, seguimiento y atención

oportuna de las solicitudes para el ejercicio de los derechos de acceso, rectificación, cancelación y oposición, así como para la atención de quejas o solicitudes presentadas por los titulares relacionados con las políticas y/o prácticas de protección de datos personales desarrolladas por la organización.

- xv. Velar por la implementación de medidas correctivas y preventivas en caso de detectar incumplimientos o riesgos potenciales relativos a la protección de datos personales, así como también, evaluar continuamente los procesos de tratamiento de datos personales para identificar áreas de mejora.
- xvi. Asesorar en las consultas y solicitudes de los titulares de datos para velar por la resolución de las situaciones que se presente.
- xvii. Velar porque las brechas de datos personales sean revisadas en las instancias correspondientes dentro de CCA para su priorización y gestión.
- xviii. Actuar como punto de contacto y de cooperación, con la autoridad de protección de datos personales en cuestiones relacionadas con el tratamiento de datos personales.
- xix. Supervisar la respuesta de la organización ante incidentes de seguridad, incluyendo la notificación a las autoridades de protección de datos personales y a los afectados cuando sea necesario.
- xx. Facilitar auditorías en el ámbito de protección de datos personales.
- xxi. Mantener y actualizar registros detallados de las actividades de tratamiento de datos personales (RAT) de CCA.
- xxii. Desarrollar un plan anual de trabajo en materia de protección de datos personales e informar a la alta administración de su avance.
- xxiii. Coordinar la elaboración de un programa de capacitación de los colaboradores de CCA en materia de protección de datos personales, con la finalidad de concientizar en las responsabilidades de CCA y de cada uno en esta materia, proporcionando claridad en los lineamientos y requisitos que sobre el tema establece la ley, marco regulador y normativo y de esta forma fomentar una cultura de protección de datos personales dentro de CCA.

c. Gerentes de CCA

- i. Dotar de las competencias y recursos suficientes a la organización para un adecuado cumplimiento de las normativas vigentes.
- ii. Coordinar el trabajo de levantamiento, actualización y valorización de los riesgos de la organización en materia de tratamiento de datos personales.
- iii. Apoyar y controlar al personal en las tareas de mitigación y cumplimiento de la normativa vigente.

d. Personal de CCA

- i. Los colaboradores de CCA son los primeros encargados de asegurar la aplicación y seguimiento de las distintas políticas, normas y procedimientos definidos por CCA para el logro de los objetivos de esta Política.
- ii. Deben conocer los riesgos asociados a sus procesos y actividades, definir planes de mitigación y procurar la implementación de estos.

8. CONTEXTO NORMATIVO

- a. Se debe implementar un procedimiento para velar por el cumplimiento riguroso de todos los requerimientos legales y regulatorios que afectan al tratamiento de datos personales por CCA.
- b. Se establece que la revisión de esta Política se debe efectuar, a lo menos, una vez al año, revisión que debe ser aprobada por el Directorio o cada vez que se incorporen de nuevas finalidades del tratamiento de datos personales; haya cambios en las bases de licitud invocadas para el tratamiento, aparezcan nuevas tecnologías que impacten en la forma en que se tratan los datos personales, como por ejemplo tecnologías que permiten tomar decisiones automatizadas o nuevos canales digitales o cambios normativos relevantes o pronunciamientos de la futura Agencia de Protección de Datos Personales.
- c. Son aplicables el artículo 19 N°4 de la Constitución Política de la República, la Ley N°19.628 sobre protección de los datos personales modificada por la Ley N°21.719, la Ley N°19.496 sobre protección de los derechos de los consumidores y las regulaciones que de éstas se desprendan.
- d. En cumplimiento de la normativa sobre protección de datos personales, CCA reconoce y garantiza el ejercicio de los derechos de los titulares de datos personales. Las solicitudes podrán ser presentadas a través de los canales definidos para ello por CCA, dirigidas a la Unidad de Atención de Derechos, la cual gestionará la tramitación correspondiente bajo la supervisión del o la Delegado(a) de Protección de Datos. El procedimiento específico de gestión de derechos deberá ser oportunamente documentado a través de una política o protocolo de CCA.
- e. CCA adoptará las medidas técnicas y organizativas necesarias para detectar, contener, investigar, documentar y notificar incidentes que puedan afectar la seguridad, confidencialidad, integridad o disponibilidad de los datos personales bajo su control. Se entenderá por incidente de seguridad cualquier evento que afecte o pueda afectar datos personales, incluyendo accesos no autorizados, pérdidas, destrucción, alteración o divulgación indebida. Esto será documentado por CCA en una política interna de gestión de incidentes.

9. PUBLICACIÓN Y DISPONIBILIDAD

El Directorio de CCA debe promover y generar los mecanismos para que esta Política y sus modificaciones

sean adecuadas al propósito y a las necesidades de CCA. Además, debe promover que la alta administración vele que esta política sea conocida y esté disponible permanentemente para todos los directores, ejecutivos(as), colaboradores, asesores, personal externo, clientes y proveedores de la compañía.

10. SENSIBILIZACIÓN Y CAPACITACIÓN

- a. CCA reconoce como tareas prioritarias la sensibilización, capacitación y entrenamiento del personal, en materias de protección de datos personales, para lo cual el o la Delegado(a) de Protección de Datos debe definir las materias a ser consideradas por los procesos de inducción y capacitación de la organización.
- b. La Gerencia de Administración, Finanzas y Personas de CCA debe velar por que todos los colaboradores completen una inducción y sea capacitado sobre protección de datos personales, con el objetivo de crear una cultura de protección de datos personales, asegurándose que los directores, ejecutivos(as), colaboradores, personal externo y asesores asumen y comprenden sus responsabilidades.

11. INCUMPLIMIENTO

- a. Ante la ocurrencia de algún incumplimiento relativo a las medidas orientadas a resguardar las indicaciones de esta Política, quien lo detecte debe informar a la brevedad al o la Delegado(a) de Protección de Datos, quien debe analizar la situación informada y comunicar al Comité Interno de Cumplimiento para evaluar el incumplimiento y gestionar las medidas necesarias para minimizar los potenciales daños o impactos al CCA y lograr el cumplimiento integral de esta Política, evitando que se reiteren situaciones similares.
- b. Los directores, ejecutivos(as), colaboradores, personal externo y asesores tienen la obligación de notificar cualquier actividad o situación que afecte o pueda afectar el cumplimiento de esta Política y sus actualizaciones, a través del Canal de Denuncias, disponible en la página web de CCA.
- c. Los incumplimientos graves, deben ser informados al Gerente General y este al Directorio de CCA.

12. SANCIONES

Quienes contravengan lo indicado en esta política y/o los documentos de apoyo de estas, se les aplicará lo establecido en el Registro Reglamento Interno de Orden, Higiene y Seguridad de CCA, Título Sanciones y Multas.