

Política de Privacidad y Protección de datos del Grupo Cooperativo Cajamar

Índice

Control de versiones	3
Objeto	4
Ámbito de aplicación	5
Marco normativo y criterios de referencia	5
Principios aplicables al tratamiento de datos personales	5
Marco de gobierno	6
Bases legitimadoras del tratamiento	7
Categorías de datos, actividades de tratamiento y registro	7
Información a las personas interesadas y ejercicio de derechos	8
Conservación y supresión de los datos	8
Seguridad de la información y confidencialidad	9
Encargados del tratamiento, terceros y transferencias internacionales	9
Privacidad desde el diseño, evaluación de riesgos y evaluaciones de impacto	9
Gestión de incidentes y brechas de seguridad	10
Formación, concienciación y deber de confidencialidad	10
Supervisión, control y mejora continua	11
Aprobación, entrada en vigor y revisión	11

Control de versiones

Versión	Fecha	Descripción
1	30.06.2026	Publicación de la primera versión resumida de la Política de Privacidad y Protección de Datos del Grupo Cooperativo Cajamar

Objeto

La presente Política de Privacidad y Protección de Datos (en adelante, la Política) establece los principios, criterios, responsabilidades y medidas generales que rigen el tratamiento de datos personales en cada una de las entidades que integran el Grupo Cooperativo Cajamar (en adelante, todas ellas incluidas, el Grupo o GCC, indistintamente), con el fin de garantizar una gestión lícita, leal, transparente y segura de la información, así como el respeto efectivo de los derechos de las personas físicas.

El objeto de esta Política es definir el marco corporativo de cumplimiento en materia de privacidad y protección de datos personales, asegurando que los tratamientos de datos realizados por las entidades del GCC se desarrollen conforme a la normativa aplicable, a los principios de responsabilidad proactiva y a las mejores prácticas de gobierno del dato.

A tal efecto, el Grupo se compromete a:

- Cumplir con la legislación vigente, incluyendo el Reglamento (UE) 2016/679, General de Protección de Datos (RGPD), Ley Orgánica 3/2018, de Protección de Datos Personales y garantía de los derechos digitales (LOPDGDD), y demás normativas aplicables.
- Garantizar la confidencialidad, integridad y disponibilidad de los datos personales tratados.
- Promover la transparencia en el uso de los datos, informando adecuadamente a los titulares sobre su tratamiento.
- Fomentar la formación continua en privacidad y protección de datos entre sus empleados.
- Implementar medidas de seguridad avanzadas, incluyendo ciber resiliencia, simulaciones de ataques y supervisión continua.
- Facilitar el ejercicio de derechos de los titulares de datos: acceso, rectificación, supresión, oposición, portabilidad y limitación del tratamiento.

La protección de los datos personales constituye una manifestación del compromiso del Grupo Cooperativo Cajamar con el respeto de los derechos fundamentales, la privacidad y la protección de la información de las personas. En este sentido, el Grupo integra la protección de datos dentro de su marco de actuación responsable, promoviendo una gestión ética, transparente y segura de la información.

Ámbito de aplicación

Esta Política aplica a todas las entidades que conforman el GCC, incluyendo Banco de Crédito Social Cooperativo, S.A. (BCC) como entidad cabecera, y a todos los empleados, socios, clientes, proveedores y terceros que interactúan con el Grupo.

Su aplicación abarca el tratamiento de datos personales en cualquier formato (físico o digital) y en todos los procesos operativos, comerciales, tecnológicos y de gestión.

Asimismo, los requisitos de privacidad y seguridad se extienden a proveedores y terceros mediante obligaciones contractuales y controles de cumplimiento.

Marco normativo y criterios de referencia

Esta Política se interpreta y aplica de conformidad con el RGPD, la LOPDGDD, la normativa sectorial que resulte aplicable, así como los criterios y directrices emitidos por las autoridades de control competentes.

En particular, la Política incorpora los principios de transparencia, responsabilidad proactiva, privacidad desde el diseño y por defecto, gestión del riesgo, seguridad y trazabilidad documental exigidos por la normativa vigente.

Principios aplicables al tratamiento de datos personales

Los principios que rigen la privacidad y la protección de los datos en el GCC son los siguientes:

- Licitud, lealtad y transparencia en todos los tratamientos de datos personales.
- Limitación de la finalidad, de modo que los datos se recojan con fines determinados, explícitos y legítimos y no sean tratados ulteriormente de manera incompatible con dichos fines.
- Minimización de datos, asegurando que los datos tratados sean adecuados, pertinentes y limitados a lo necesario.
- Exactitud y actualización de la información tratada.
- Limitación del plazo de conservación, manteniendo los datos únicamente durante el tiempo necesario para cumplir la finalidad del tratamiento y las obligaciones legales asociadas.

- Integridad, confidencialidad y disponibilidad de la información mediante medidas técnicas y organizativas adecuadas.
- Responsabilidad proactiva, de forma que el Grupo pueda demostrar el cumplimiento de la normativa y la eficacia de los controles implantados.

Marco de gobierno

La gobernanza de la privacidad de datos se articula a través de una estructura formalizada, integrada en el modelo global de gobierno corporativo del Grupo, que define responsabilidades claras, estructuras de supervisión y mecanismos de gestión del cumplimiento.

En este marco, el Grupo identifica al responsable del tratamiento y dispone de un Delegado de Protección de Datos (DPD), adscrito a la función de Cumplimiento Normativo, como punto de contacto especializado en materia de protección de datos.

El DPD asume funciones de supervisión, asesoramiento y control del cumplimiento de la normativa de protección de datos personales, con independencia, autonomía y ausencia de conflicto de interés, en coordinación con las áreas técnicas y, en su caso, con terceros implicados en el tratamiento de datos, disponiendo de acceso a la información y a los recursos necesarios para el adecuado desempeño de sus responsabilidades, de conformidad con la normativa aplicable.

La supervisión del cumplimiento de la Política se articula a través de la Dirección General de Cumplimiento Normativo (en adelante, DGCN), responsable de su implementación, seguimiento y de la gestión de los derechos de los interesados, garantizando una adecuada integración de la protección de datos en los procesos operativos.

El sistema se completa con mecanismos de control y sensibilización, entre los que destacan un canal de denuncias confidencial y seguro para la comunicación de posibles incumplimientos o incidencias, así como un Plan Anual de Formación que incluye contenidos específicos en materia de protección de datos, ciberseguridad, prevención de riesgos y buenas prácticas en el uso de la información.

En su conjunto, este modelo de gobernanza permite asegurar una gestión estructurada y eficaz de la privacidad, reforzar el cumplimiento normativo y garantizar la integración de la protección de datos en la operativa y en la gestión de riesgos del Grupo.

Asimismo, el Consejo de Administración recibe información periódica sobre protección de datos en el marco del sistema de gobernanza corporativa, a través de reportes elaborados desde la DGCN, con la participación del DPD.

Bases legitimadoras del tratamiento

En el Grupo, todo tratamiento de datos personales se apoya en una base jurídica válida y previamente identificada. Entre otras, pueden ser aplicables la ejecución de una relación contractual o precontractual, el cumplimiento de obligaciones legales, la satisfacción de intereses legítimos prevalentes debidamente ponderados, la protección de intereses vitales, el cumplimiento de una misión realizada en interés público o el consentimiento de la persona interesada cuando resulte exigible.

Cuando el tratamiento de datos se basa en el consentimiento expreso, el Grupo adopta las medidas necesarias para que este sea libre, específico, informado e inequívoco, y su obtención, gestión y eventual retirada pueda acreditarse adecuadamente.

En este sentido, para el tratamiento de datos con fines comerciales basado en el consentimiento del interesado, que puede ser otorgado o retirado en cualquier momento, el Grupo proporciona mecanismos para:

- Aceptar o rechazar comunicaciones comerciales (opt-in / opt-out)
- Oponerse al tratamiento
- Modificar las preferencias en cualquier momento

Categorías de datos, actividades de tratamiento y registro

Las entidades del Grupo mantienen identificado el inventario o Registro de Actividades de Tratamiento (RAT) bajo su responsabilidad, con el contenido mínimo exigido por la normativa aplicable.

Dicho registro recoge la identificación del responsable, las finalidades del tratamiento, las categorías de interesados y datos, los destinatarios, en su caso las transferencias internacionales, los plazos de conservación y una descripción general de las medidas técnicas y organizativas de seguridad.

Las categorías de datos tratadas deberán ser proporcionales a la finalidad perseguida. El tratamiento de categorías especiales de datos, de datos relativos a infracciones o de cualquier otra información sometida a especial protección solo podrá llevarse a cabo cuando exista habilitación jurídica suficiente y se apliquen garantías reforzadas.

Información a las personas interesadas y ejercicio de derechos

El Grupo garantiza que las personas interesadas reciban, de forma concisa, transparente, inteligible y fácilmente accesible, la información exigida por la normativa sobre protección de datos, incluyendo la identidad del responsable, las finalidades del tratamiento, la base jurídica, los destinatarios o categorías de destinatarios, los plazos de conservación, la existencia de transferencias internacionales cuando proceda y la forma de ejercer sus derechos.

El Grupo promoverá una comunicación transparente, clara y accesible sobre sus prácticas de privacidad y protección de datos hacia clientes, empleados, proveedores y demás grupos de interés, fomentando la confianza y la adecuada comprensión de los tratamientos realizados.

Asimismo, tiene establecidos procedimientos internos para atender, dentro de plazo y con las debidas garantías, las solicitudes de ejercicio de los derechos de acceso, rectificación, supresión, oposición, limitación del tratamiento y portabilidad, así como cualquier otro derecho reconocido por la normativa aplicable.

Toda la información que se ofrece a los interesados para cumplir con el deber de información que contempla la normativa de protección de datos es pública y consultable en la página web de cada una de las entidades de crédito del Grupo (por ejemplo, en el caso de Cajamar Caja Rural, encontramos la información a través de

[Inicio>Tablón de anuncios y tarifas>Otra información de interés para los clientes>Información sobre protección de datos personales](#)

Del mismo modo, cada una de las páginas web de las entidades del Grupo ofrece a sus usuarios una política de protección de datos (por ejemplo, en el caso de Cajamar Caja Rural, encontramos la información a través de

[Inicio>Política de Protección de Datos](#)

Conservación y supresión de los datos

Los datos personales se conservarán durante el tiempo necesario para cumplir la finalidad para la que fueron recabados y, posteriormente, durante los plazos exigidos por la normativa aplicable o necesarios para la formulación, ejercicio o defensa de reclamaciones. Transcurridos dichos plazos, los datos deberán ser suprimidos, anonimizados o bloqueados, según proceda, mediante procedimientos seguros y trazables.

Seguridad de la información y confidencialidad

El Grupo adopta y mantiene medidas técnicas y organizativas apropiadas para garantizar un nivel de seguridad adecuado al riesgo, teniendo en cuenta el estado de la técnica, los costes de aplicación, la naturaleza, el alcance, el contexto y los fines del tratamiento, así como los riesgos de diversa probabilidad y gravedad para los derechos y libertades de las personas físicas.

Estas medidas incluyen, entre otras, controles de acceso y uso restringido de la información, segregación de funciones, gestión de identidades y privilegios, cifrado o seudonimización cuando proceda, copias de seguridad, registro y monitorización de eventos, gestión segura del ciclo de vida de los activos, medidas de continuidad, deberes de confidencialidad y procedimientos de revisión periódica de la eficacia de los controles.

Encargados del tratamiento, terceros y transferencias internacionales

Cuando el Grupo recurre a terceros que traten datos personales por su cuenta, selecciona únicamente proveedores que ofrecen garantías suficientes para aplicar medidas técnicas y organizativas apropiadas, formalizando los correspondientes contratos o actos jurídicos con el contenido exigido por la normativa.

Asimismo, establece mecanismos de supervisión, seguimiento y reevaluación del nivel de cumplimiento de dichos terceros.

En su caso, las transferencias internacionales de datos personales únicamente se realizan cuando existe una base jurídica válida y se cumplen las garantías, salvaguardas o excepciones previstas en la normativa aplicable.

Privacidad desde el diseño, evaluación de riesgos y evaluaciones de impacto

En el Grupo la protección de datos está integrada desde las fases iniciales de diseño de productos, servicios, procesos, canales, aplicaciones y sistemas de información, aplicando el principio de privacidad desde el diseño y por defecto.

Con carácter previo a la puesta en marcha o modificación relevante de tratamientos,

se evalúan los riesgos para los derechos y libertades de las personas afectadas y, cuando procede, se realizan evaluaciones de impacto relativas a la protección de datos, incorporando las medidas de mitigación necesarias y, en su caso, el proceso de consulta previa a la autoridad competente.

El Grupo integra la gestión de los riesgos de privacidad dentro de su marco general de control interno, llevando a cabo análisis y evaluaciones en materia de privacidad de forma periódica, con el objetivo de identificar, evaluar y mitigar los riesgos asociados al tratamiento de datos personales.

En este contexto, la Entidad contempla la realización de evaluaciones de impacto en protección de datos (PIA/DPIA) cuando los tratamientos puedan implicar un riesgo elevado para los derechos y libertades de las personas, de conformidad con la normativa aplicable.

El marco de seguridad se complementa con la realización de revisiones, evaluaciones y auditorías internas, así como con revisiones operativas dirigidas a verificar la adecuación y eficacia de los controles implantados y del modelo de protección de datos, promoviendo su mejora continua.

Asimismo, estas actuaciones incluyen, cuando resulta aplicable, la actualización de los Registros de Actividades de Tratamiento (RAT) y la evaluación continua de los tratamientos existentes.

Gestión de incidentes y brechas de seguridad

El Grupo dispone de mecanismos de detección, comunicación y gestión de incidentes relacionados con la seguridad de la información, incluyendo la obligación del personal de comunicar cualquier incidencia.

Asimismo, cuenta con un procedimiento específico para la gestión y notificación de brechas de datos personales, que define los procesos de identificación, análisis, gestión y, en su caso, notificación a la autoridad de control y a los interesados, de conformidad con la normativa aplicable.

Formación, concienciación y deber de confidencialidad

El Grupo promueve la formación continua en materia de protección de datos y seguridad de la información, incluyendo la impartición de formación obligatoria en

privacidad para sus empleados, integrada dentro de los programas corporativos.

Esta formación se complementa con materiales de apoyo, como contenidos divulgativos e infografías, con el objetivo de reforzar el conocimiento y la correcta aplicación de los principios de protección de datos en el desempeño de las funciones profesionales.

Asimismo, la entidad realiza comunicaciones periódicas en materia de protección de datos dirigidas a los empleados, con el objetivo de reforzar la cultura de privacidad y recordar las obligaciones derivadas del cumplimiento normativo.

El personal, por su parte, está sujeto a obligaciones de confidencialidad, uso adecuado de la información y cumplimiento de las políticas internas, existiendo medidas disciplinarias en caso de incumplimiento.

Supervisión, control y mejora continua

El cumplimiento de esta Política está sujeto a mecanismos de supervisión, seguimiento y revisión periódica, con el fin de verificar su eficacia, detectar oportunidades de mejora y adaptarla a cambios normativos, organizativos, tecnológicos o de riesgo.

Las incidencias, desviaciones o incumplimientos relevantes se escalarán conforme a los procedimientos internos establecidos.

Aprobación, entrada en vigor y revisión

La presente Política ha sido aprobada por el Delegado de Protección de Datos y es objeto de revisión periódica, al menos cuando se produzcan cambios normativos relevantes, modificaciones significativas en las actividades de tratamiento o variaciones sustanciales en el perfil de riesgo en materia de privacidad y protección de datos.