Política de privacidad y protección de datos de UNION DE CREDITO PARA LA FINANCIACION MOBILIARIA E INMOBILIARIA CREDIFIMO E.F.C., S.A.U.

[17 de junio de 2025]

Control de versiones

Versión	Fecha	Control
1	24/05/2018	Versión inicial aprobada por el Consejo de Administración
2	20/05/2022	Revisión y actualización bienal de la Política Adaptación al modelo de Política Corporativa.
3	30/05/2025	Revisión y actualización de la Política, de acuerdo a la actualización de la Política Corporativa de CaixaBank de Diciembre de 2024: • Adaptación de la Política al modelo corporativo 2024: modificaciones menores en la estructura del documento y en la redacción sin suponer modificaciones de fondo. Corrección de errores tipográficos menores. • En el **apartado 3 Marco normativo**, actualización normativa aplicable. • En el **apartado 7 Marco de control** incorporación de la Dirección de Medios y la Dirección de Riesgos No Financieros en la primera y segunda línea de defensa respectivamente para el control de los riesgos tecnológicos asociados al riesgo de protección de datos. • En el **apartado 9 Actualización de la Política**, ajuste de la periodicidad de las revisiones de la Política.

Contenido

1. Introducción 5
1.1 Antecedentes 5
1.2 Riesgo de protección de datos y confidencialidad de la información. 6
1.3 Objetivo 7
2. Ámbito de aplicación 9
3. Marco normativo. Normativa y estándares de aplicación 10
4. Principios generales de la gestión de la privacidad 11
5. Marco de gobierno 12
5.1 Órganos de Gobierno de CaixaBank 12
5.1.1 Consejo de Administración de CaixaBank 12
5.1.2 Comisión de Riesgos 13
5.1.3 Comisión de Auditoría y Control 13
5.2 Órganos colegiados de CaixaBank en el ámbito de riesgo de privacidad y protección de datos 14
5.2.1 Comité de Dirección 14
5.2.2 Comité Global del Riesgo 14
5.2.3 El Comité de Privacidad de CaixaBank 14
5.2.4 Comité de Gestión de Riesgo y Evaluación de impacto 16
5.2.5 Grupo de Seguimiento de protección de datos de Empresas del Grupo 16
5.3 .Órganos de Gobierno de Credifimo 16
5.3.1 Consejo de Administración 17
6. Marco de gestión para la privacidad y la protección de datos 17
6.1. Delegado de Protección de Datos (DPO) 17
6.1.1 Nombramiento 17
6.1.2 Encaje organizativo y funciones 17
6.1.3 Facultades 18
6.1.4 Independencia 19
6.1.5 Disponibilidad y participación efectiva 19
6.1.6 Dotación de medios 19
6.1.7 Prevención de conflictos de interés 19
6.1.8 Reporte a los órganos de administración y dirección 20
6.1.9 Comunicación interna y externa en materia de privacidad 20
6.1.10 Relaciones con las funciones de control 21
6.1.11 El Delegado de Protección de Datos Corporativo 21
6.2 Otras figuras responsables 22
6.2.1 Responsable de Privacidad 22
6.3 Tratamientos y Legitimación 22
6.4 Derechos de los interesados 22
6.5 Evaluaciones de impacto 23
6.6 Medidas técnicas 23
6.7 Proveedores 24
6.8 Comunicación y formación 24
7. Marco de control 24

8. Marco de información **27**

9. Actualización de la Política **28**

10. Glosario **29**

11. Anexos **31**

ANEXO 1 - DERECHOS DE LOS INTERESADOS **31**

1. Introducción

1.1 Antecedentes

Unión de Crédito para la financiación mobiliaria e inmobiliaria S.A.E.F.C, (en adelante "Credifimo" o "la Entidad") es una entidad de crédito que gestiona los créditos que dispone en cartera y que no concede nuevos préstamos , que a su vez, se integra dentro del Grupo CaixaBank, encabezado por la entidad de crédito CaixaBank, S.A. (en adelante, "CaixaBank"). Como tal, se ha venido rigiendo por los más altos estándares de respeto al derecho fundamental de protección de datos de carácter personal, así como a la preservación de la confidencialidad de la información que trata. Estos constituyen pilares fundamentales sobre los que se asienta la confianza, valor esencial de su actividad.

En este contexto, el Consejo de Administración de CaixaBank, coincidiendo con el inicio de la aplicación el 25 de mayo de 2018 del Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos (en adelante, el **"Reglamento General de Protección de Datos"** o el "**RGPD**"), dio un paso más en su compromiso con la confidencialidad y con la protección de los datos personales estableciendo mediante esta política (en adelante, la "**Política**") un marco general de gestión de la privacidad y la protección de datos en el grupo CaixaBank, adaptada a las nuevas disposiciones normativas y que formalizó la adopción y seguimiento de los principios que la mencionada norma incorpora como son, la privacidad por defecto y por diseño, el enfoque de riesgos y la responsabilidad pro activa. Credifimo incorporó la Política a su normativa interna mediante adhesión a la misma y a sus sucesivas actualizaciones, aceptando ahora su compromiso con el cumplimiento en esta materia mediante adaptación de la Política.

Asimismo, en abril de 2019 la Comisión Europea publicó las Directrices Éticas para una Inteligencia Artificial fiable, que constituye el primer marco europea para lograr el uso en la Unión de una inteligencia artificial licita, ética y robusta. A estas directrices las siguió la publicación en febrero de 2020 del Libro Blanco sobre Inteligencia Artificial: "Un enfoque europeo orientado a la excelencia y la confianza" que plantea la necesidad de establecer un marco regulador europea de la Ética en el uso de los datos y los sistemas de inteligencia artificial.

Fruto de todo ello, la Comisión Europea, en abril de 2021, publico su primera propuesta de texto para lo que será el futuro Reglamento Europeo mediante el que se pretenden establecer normas armonizadas en materia de inteligencia artificial (ley de inteligencia artificial).

A esta propuesta le siguió la posición adoptada por el Consejo de la Unión Europea, en diciembre de 2022, sobre el Reglamento de Inteligencia Artificial, encaminado a garantizar que los sistemas de inteligencia artificial (IA) introducidos en el mercado de la UE y utilizados en la Unión sean seguros y respeten la legislación vigente en materia de derechos fundamentales, así como los valores de la Unión.

El 9 de diciembre de 2023 el Consejo de la Unión Europea, liderado por la presidencia española, y el Parlamento Europeo llegaron a un acuerdo provisional para la aprobación definitiva del futuro Reglamento por el que se establecen normas armonizadas en materia de inteligencia artificial (Reglamento de Inteligencia Artificial o AI Act).

Fruto de todo ello, el 21 de mayo de 2024, el Consejo de la Unión Europea dio su aprobación final al Reglamento por el que se establecen normas armonizadas en materia de inteligencia artificial (Reglamento de IA), y finalmente, el día 12 de julio de 2024 se publicó en el Diario Oficial de la Unión Europea (DOUE). A partir de esta publicación, el Reglamento entró en vigor el día 2 de agosto de 2024, siendo directamente aplicable en todos los Estados

miembros, sin necesidad de transposición a leyes nacionales. La regla general es que será aplicable a los 24 meses desde la entrada en vigor (a partir del 2 de agosto de 2026) con excepciones para ciertas disposiciones específicas: i) las prohibiciones de sistemas de IA que planteen riesgos inaceptables -prácticas de IA prohibidas—surtirán efecto al cabo de 6 meses (2 de febrero de 2025); ii) las normas de gobernanza y las obligaciones para los modelos de IA de uso general que deban cumplir requisitos de transparencia serán aplicables al cabo de 12 meses (2 de agosto de 2025); iii) a los 24 meses se aplicarán el resto de disposiciones (sistema de gestión de riesgos, de calidad, etc.,), y iv) a los 36 meses se aplicarán las reglas de clasificación de los sistemas de IA de alto riesgo –componentes de seguridad de un producto- (2 de agosto de 2027).

Asimismo, el día 5 de septiembre de 2024, la Comisión firmó, en nombre de la Unión Europea, el Convenio Marco del Consejo de Europa sobre Inteligencia Artificial y Derechos Humanos, Democracia y Estado de Derecho. Es el primer tratado internacional legalmente vinculante destinado a garantizar que el uso de los sistemas de inteligencia artificial es totalmente coherente con los derechos humanos, la democracia y el Estado de derecho. En este sentido, proporciona un marco legal que abarca el ciclo de vida completo de los sistemas de IA, promueve el progreso y la innovación en IA, a la vez que gestiona los riesgos que puede plantear para los derechos humanos, la democracia y el Estado de derecho.

Por su parte, la Agencia Española de Protección de datos publicó dos guías sobre inteligencia Artificial, la Guía sobre Adecuación al RGPD de tratamientos que incorporan Inteligencia Artificial. Una introducción, en febrero de 2020 y de Requisitos para Auditorias de tratamientos que incluyan IA, en enero de 2021.

El Consejo de Administración de Credifimo, mediante la presente Política, desea establecer los principios que la Entidad aplica en el tratamiento de la información personal, los derechos que reconoce a los Interesados y el marco de gobierno interno del que, en materia de privacidad, quieren dotarse. En la Política se regula también la figura del Delegado de Protección de Datos.

Finalmente, el Consejo de Administración de Credifimo con la presente Política pretende garantizar el establecimiento de los procedimientos y medidas necesarias para asegurar una gestión del riesgo de la privacidad acorde con el apetito al riesgo de la Entidad.

El Consejo de Administración tiene la facultad indelegable para la determinación de las políticas y estrategias de la Entidad de acuerdo con el artículo 249 bis del Texto Refundido de la Ley de Sociedades de Capital.

1.2 Riesgo de protección de datos y confidencialidad de la información.

El artículo 8 de la Carta de los Derechos Fundamentales de la Unión Europea establece el derecho de toda persona a la protección de los datos de carácter personal que le conciernan, concretando que los datos deberán ser tratado de modo leal y para fines concretos. En este sentido, el RGPD, es el marco del que se ha dotado la Unión Europa para garantizar este derecho fundamental y su no afectación estableciendo las reglas que deben regir los tratamientos de datos. Esta Política cubre el riesgo de Credifimo de afectar a este derecho fundamental cuando en sus procesos tratan datos personales.

Asimismo, esta Política cubre el riesgo de secreto bancario establecido en el art. 83 de la Ley 10/2014, de 26 de junio, de ordenación, supervisión y solvencia de entidades de crédito consistente en el deber de reserva de la información al que están obligadas las entidades de crédito en relación con las informaciones relativas a los saldos, posiciones, transacciones y demás operaciones de sus clientes.

Finalmente, y derivado de los anteriores, el riesgo objeto de gestión y control por la presente Política es el riesgo de protección de datos y privacidad, contemplado en el segundo nivel dentro del Catálogo Corporativo de Riesgos, como componente del riesgo legal y regulatorio, y definido como el riesgo relacionado con el incumplimiento de la normativa relacionada con la protección de datos de carácter personal y la privacidad de las personas,

Derivada de esta configuración, el riesgo de protección de datos y privacidad está estrechamente relacionado con otros riesgos corporativos como el riesgo tecnológico, y más concretamente con el riesgo de seguridad de la información.

1.3 Objetivo

La presente Política tiene como objetivos:

- Transmitir a todos los/las empleados, directivos y miembros del órgano de administración de la Entidad, el mensaje de que Credifimo vela porque su actividad esté basada en el respeto a las leyes y a las normas vigentes en cada momento, así como en la promoción y defensa de sus valores corporativos y principios de actuación establecidos en su Código Ético y, por consiguiente, enlaza con sus valores éticos, ratificando la firme voluntad por mantener una conducta de estricto cumplimiento en materia de privacidad y uso ético de los datos y los componentes de inteligencia artificial.
-
- Establecer un marco general para la gestión de la privacidad y la protección de datos de carácter personal y uso ético de los datos y los componentes de inteligencia artificial, adaptándolo a las nuevas disposiciones normativas. El marco comprenderá el conjunto de medidas dirigidas a la prevención, detección y reacción e identificará los riesgos de privacidad y controles asociados a los mismos que se establezcan.

- Asegurar ante los clientes, proveedores, organismos supervisores y la sociedad en general, que la Entidad cumple con los deberes de supervisión y control de su actividad en relación con la privacidad y uso ético de los datos y los componentes de inteligencia artificial, estableciendo medidas adecuadas para prevenir o reducir el riesgo de actuaciones no respetuosas con la normativa vigente y que, por tanto, se ejerce el debido control legalmente procedente sobre administradores, directivos, empleados y demás personas asociadas.

El contenido de esta Política incluye:

- Estrategia o principios generales que rigen la gestión de la privacidad y la protección de datos
- Marco de gobierno
- Marco de gestión en materia de privacidad, la y protección de datos y uso ético de los datos y los componentes de inteligencia artificial:
    - Delegado de protección de datos (en adelante, DPO) y otras figuras responsables
    - Tratamientos y legitimación
    - Derechos de los interesados

    - Evaluaciones de impacto
    - Medidas técnicas
    - Proveedores
    - Comunicación y formación
- Marco de control
- Marco de información

2. Ámbito de aplicación

La presente Política tiene la consideración de política individual de Credifimo. Los principios de actuación definidos son aplicables a Credifimo con exposición al riesgo de protección de datos y al uso ético de los datos y los componentes de inteligencia artificial. El Consejo de Administración de Credifimo adoptará las decisiones oportunas con el objeto de integrar las disposiciones de esta Política adaptando, siguiendo el principio de proporcionalidad, el marco de gobierno a la idiosincrasia de su estructura de órganos de gobierno, comités y departamentos, y sus principios de actuación, metodologías y procesos a lo descrito en este documento.

La Dirección de Compliance de CaixaBank, dado su carácter corporativo, velará por que la integración de esta Política en Credifimo sea proporcionada, y esté alineada con la política corporativa, y por la consistencia en todo el Grupo CaixaBank.

La presente Política es de aplicación directa a los empleados, directivos y miembros del órgano de administración de la Entidad en relación con el marco de gobierno de los tratamientos de datos que se realizan con personas físicas (potenciales clientes, accionistas, empleados, representantes y apoderados de personas jurídicas tales como proveedores o *partners).*

3. Marco normativo. Normativa y estándares de aplicación

La presente Política se regirá por lo previsto en la normativa aplicable vigente, así como por aquella que la modifique o sustituya en el futuro. En concreto, a fecha de su elaboración, la normativa vigente aplicable a la Entidad es la siguiente:

- Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento General de Protección de Datos).
- Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales
- Ley 11/2022, de 28 de junio, General de Telecomunicaciones.
- Ley 34/2002, de 11 de julio, de servicios de la sociedad de la información y de comercio electrónico.
- Reglamento (UE) 2023/2854, Ley de datos
- Reglamento (UE) 2022/868, Ley de gobernanza de datos
- Reglamento (EU) 2022/2065, Ley de servicios digitales
- Ley 10/2014, de 26 de junio, de ordenación, supervisión y solvencia de entidades de crédito, en relación con lo previsto en su artículo 83, Obligación de secreto.
- Reglamento (UE) 2024/1689 del Parlamento Europeo y del Consejo, de 27 de abril de 2016 de 13 de junio de 2024 por el que se establecen normas armonizadas en materia de inteligencia artificial de acuerdo con lo establecido en el considerando 9 y 10 de este, así como en su art. 27. Guías de los supervisores nacionales y europeos (AEPD y EDPB).

En el caso de Credifimo las políticas y procedimientos que la Entidad desarrolle, tendrán en cuenta, además de su normativa propia, las obligaciones contenidas en la normativa antes referenciada en tanto no sean contradictorias con los requisitos específicos de la jurisdicción o normativa sectorial correspondiente.

Finalmente se desarrollarán los marcos, normas, guías o procedimientos que sean necesarios para la correcta implementación, ejecución y cumplimiento de esta Política.

4. Principios generales de la gestión de la privacidad

Los principios que orientarán la toma de decisiones de la Entidad en materia de privacidad y protección de datos son los que siguen:

- **Tratamiento de los datos de manera lícita, leal y transparente**. Se respetará el ordenamiento jurídico de aplicación, el tratamiento de los datos personales se realizará siempre al amparo de alguna de las condiciones legales que lo permiten y se informará al Interesado al respecto incluyendo, en su caso, información sobre la elaboración de perfiles y sus consecuencias.
- **Tratamiento de los datos para fines determinados, explícitos y legítimos.** No se tratará la información para fines incompatibles con aquellos de los que se hayan informado al Interesado.
- **Tratamiento únicamente los datos adecuados, pertinentes y limitados** a cada finalidad del tratamiento.
- **Tratamiento de datos exactos y actualizados**. Se adoptarán las medidas que permiten suprimir o modificar la información, de forma que se mantenga exacta y al día.
- **Conservación de los datos únicamente durante el tiempo necesario**. En la mayoría de casos, los datos dejan de ser necesarios cuando finaliza la relación contractual o de negocio (o cuando se retira el consentimiento para su uso). A partir de ese momento, se procederá a la adaptación y modificación de los tratamientos de datos correspondientes adecuándolos, en su caso, al nuevo título habilitante (tales como el cumplimiento de obligaciones legales o para la formulación, el ejercicio o la defensa de sus derechos e intereses) y finalmente, se suprimirán.
- **Tratamiento de datos con medidas de seguridad de la información.** Credifimo asegura la adecuada protección de los datos personales y de la información, desplegando medidas de seguridad para protegerse adecuadamente contra amenazas y riesgos que pudieran impactar sobre la confidencialidad, integridad y disponibilidad de sus sistemas, activos de información o recursos.
- **Actuación con responsabilidad proactiva**. Credifimo se dotará de los procedimientos y herramientas necesarios para documentar y conservar todas las acciones que lleven a cabo, de conformidad con la Política y la normativa de protección de datos, en relación con los tratamientos que realizan, a los efectos no sólo de cumplir proactivamente con la normativa vigente, sino también para estar, en todo momento, en disposición de acreditar su cumplimiento.
- **Privacidad desde el diseño y por defecto**. Credifimo dispone de medidas técnicas y organizativas a lo largo de todo el ciclo de vida del tratamiento teniendo en cuenta los riesgos para los derechos y libertades de este y atendiendo a la naturaleza, el ámbito, el contexto y los fines del tratamiento.

5. Marco de gobierno

Los pilares sobre los que se asienta el marco de gobierno del riesgo de protección de datos y privacidad en Credifimo son:

- Cumplimiento de los principios recogidos en la presente Política por parte de Credifimo dentro de su ámbito de aplicación.
- Supervisión corporativa de la entidad matriz.
- Alineación de estrategias entre las sociedades del Grupo, y a su vez alineación con las mejores prácticas, con las expectativas supervisoras y con la regulación vigente.
- Implicación máxima de los órganos de gobierno y dirección de Credifimo.
- Marco de control interno basado en el modelo de Tres Líneas de Defensa que garantiza la estricta segregación de funciones y la existencia de varias capas de control independiente.

5.1 Órganos de Gobierno de CaixaBank

Los Órganos de Gobierno de CaixaBank, en tanto que matriz del Grupo CaixaBank, realizan determinadas funciones asociadas a su responsabilidad de aprobación y supervisión de las directrices estratégicas y de gestión establecidas en interés de todas las sociedades del Grupo, así como de supervisión, seguimiento y control integrado de los riesgos del Grupo en su conjunto.

5.1.1 Consejo de Administración de CaixaBank

El Consejo de Administración de CaixaBank es responsable de implantar un marco de gobierno del riesgo acorde con el nivel de propensión al riesgo del Grupo. Incluye la difusión de una cultura del riesgo sólida y diligente, la fijación del apetito por el riesgo articulado en un Marco de Apetito al Riesgo (RAF) y responsabilidades definidas para las funciones de toma, gestión y control de riesgos.

En relación con la gestión del riesgo de privacidad y protección de datos destacan las siguientes responsabilidades:

- Establece la estrategia y los principios fundamentales de gestión del riesgo de privacidad y protección de datos en el Grupo, vigilando su aplicación y controlando y evaluando periódicamente su eficacia, adoptando en su caso las medidas adecuadas para solventar sus posibles deficiencias.
- Aprueba la Política corporativa de privacidad y protección de datos de CaixaBank y vela por su cumplimiento.
- Establece el marco de seguimiento de la situación y evolución del riesgo de privacidad y protección de datos (naturaleza, tipo de información y frecuencia) y del comportamiento de las respectivas métricas en comparación con los límites establecidos en cuanto al perfil de riesgo definido y bajo diferentes escenarios de estrés.
- Supervisa el cumplimiento del respeto en CaixaBank al derecho fundamental a la protección de datos personales, directamente o a través de los órganos que se prevén en la Política corporativa de privacidad y protección de datos de CaixaBank.

Adicionalmente, y ya en el ámbito de actuación propio de CaixaBank, el Consejo de Administración de CaixaBank:

- Establece y supervisa la implantación de una cultura de riesgos en CaixaBank que promueva conductas acordes con la identificación y mitigación del riesgo de privacidad y protección de datos.

- Establece y mantiene una estructura organizativa en CaixaBank adecuada para la gestión del riesgo de privacidad y protección de datos que es proporcionada a la naturaleza, escala y complejidad de las actividades que desarrolla.
- Vela por que el personal involucrado en la gestión del riesgo de privacidad y protección de datos cuente con la competencia y experiencia adecuadas.
- Establece los mecanismos de seguimiento y escalado en caso de traspasar alguno de los umbrales que se definan.
- Vela por que existan suficientes controles internos sobre privacidad y protección de datos.

5.1.2 Comisión de Riesgos

La Comisión de Riesgos asesora al Consejo de Administración de CaixaBank sobre la propensión global al riesgo del Grupo y su estrategia en este ámbito. En el marco de la gestión del riesgo de privacidad y protección de datos, esta Comisión:

- Propone al Consejo la aprobación de la Política corporativa de privacidad y protección de datos de CaixaBank.
- Realiza el seguimiento del grado de adecuación del riesgo asumido al perfil previamente decidido y vela por que las actuaciones del Grupo sean consistentes con los niveles de tolerancia establecidos.
- Determina, junto con el Consejo de Administración la información que debe recibir el Consejo de Administración y establece la que la Comisión tiene que recibir, de forma que sea suficiente el conocimiento de la exposición a este riesgo en la toma de decisiones.
- Valora el riesgo de cumplimiento normativo en este ámbito de actuación y decisión, detectando cualquier riesgo de incumplimiento y, llevando a cabo su seguimiento y el examen de posibles deficiencias con los principios de deontología.
- Comprueba que el Grupo se dota de los medios, sistemas, estructuras y recursos acordes con las mejores prácticas que permitan implantar su estrategia en la gestión del riesgo de privacidad y protección de datos.

5.1.3 Comisión de Auditoría y Control

La Comisión de Auditoría y Control de CaixaBank supervisa la eficacia de los sistemas de control interno velando por que las políticas y sistemas establecidos en esta materia se apliquen de modo efectivo, y también supervisa y evalúa la eficacia de los sistemas de gestión de los riesgos financieros y no financieros.

Adicionalmente, y ya en el ámbito de actuación propio de CaixaBank, la Comisión de Auditoría y Control de CaixaBank:

- Informa, con carácter previo, al Consejo de Administración sobre la información financiera, y no financiera relacionada, que CaixaBank deba hacer pública periódicamente a los mercados y a sus órganos de supervisión.
- Supervisa la eficacia de los sistemas de control interno de la información financiera (SCIIF) y no financiera (SCIINF), concluyendo sobre el nivel de confianza y fiabilidad de estos sistemas.
- Supervisa que la unidad de auditoría interna vele por el buen funcionamiento de los sistemas de información y control interno, comprobando la adecuación e integridad de estos.

5.2 Órganos colegiados de CaixaBank en el ámbito de riesgo de privacidad y protección de datos

5.2.1 Comité de Dirección

El Comité de Dirección tiene atribuidas todas las facultades relacionadas con la implementación de la estrategia de CaixaBank, el desarrollo y gestión ordinaria de los negocios, las derivadas de la planificación y la actividad financiera, las líneas de gastos, las de organización y recursos humanos, tecnología y operaciones, así como las que puedan encomendarle el Consejo de Administración, y cualesquiera otras funciones que se le atribuyan por una política aprobada por los órganos de gobierno. En este desarrollo adopta acuerdos, directamente o a través de sus comités delegados, relativos a privacidad y protección de datos.

En concreto, y ya en el ámbito de actuación propio de CaixaBank, el Comité de Dirección es el encargado de:

- Impulsar la comunicación y el conocimiento de la Política corporativa de privacidad y protección de datos de CaixaBank entre las personas sujetas a la misma.
- Nombrar al Delegado de Protección de Datos
- Supervisar el cumplimiento de la normativa de protección de datos, así como de lo establecido en la Política corporativa de privacidad y protección de datos de CaixaBank.

Por otra parte, el Comité de Dirección adopta acuerdos que afectan a la vida organizativa de CaixaBankl. Además, aprueba, entre otros, los cambios estructurales, los nombramientos, las líneas de gasto y también las estrategias de negocio.

5.2.2 Comité Global del Riesgo

El Comité Global del Riesgo de CaixaBank es el órgano dependiente de la Comisión de Riesgos responsable de proponer los marcos de control interno y de gestión del riesgo, gestionar, controlar y monitorizar de forma global, entre otros, el riesgo de privacidad y protección de datos, así como las implicaciones en la gestión de la liquidez, la solvencia y el consumo de capital regulatorio y económico.

Para ello, analiza el posicionamiento global en relación con este riesgo y establece, directamente o a través de sus Comités delegados, las políticas o procedimientos que optimicen su gestión, seguimiento y control en el marco de los objetivos estratégicos para el Grupo.

Es objetivo específico de este Comité adecuar la estrategia en esta materia a lo establecido por el Consejo de Administración en el marco de apetito al riesgo, coordinar las medidas de mitigación de los incumplimientos y la reacción a las primeras alertas, y mantener informado al Consejo de CaixaBank a través de su Comisión de Riesgos de las principales líneas de actuación y de su situación en el Grupo.

5.2.3 El Comité de Privacidad de CaixaBank

El Comité de Privacidad es el órgano dependiente directamente del Comité de Dirección, que es quien nombra a sus miembros, que actúa como órgano superior y decisorio para todos los aspectos relacionados con la privacidad y protección de datos de carácter personal. Este comité ostenta la condición de Comité Corporativo de Privacidad.

En el caso de Credifimo, al no tener Comité de Privacidad propio, las funciones se realizan desde el órgano de gobierno de la matriz, por delegación de funciones.

Su finalidad es garantizar el respeto al derecho fundamental a la protección de datos (consignado en la Carta de los Derechos Fundamentales de la Unión Europea) en todas las actividades que se lleven a cabo mediante el seguimiento de la aplicación de la legislación aplicable en cada momento, la resolución de las incidencias que se detecten y, en su caso, el liderazgo en la implementación de la normativa y en el establecimiento de criterios interpretativos de la materia.

En este sentido, el Comité de Privacidad es el encargado de:

- Mantener un programa de gestión de la privacidad y la ética en el uso de los datos que permita conservar un inventario de todas las actividades de tratamiento y los componentes de inteligencia artificial;
- Dotarse de las políticas, normas y manuales, así como cualesquiera otros documentos necesarios para incluir la privacidad y la ética por defecto y desde el diseño en todas las actividades y procedimientos de CaixaBank, así como realizar una gestión de la privacidad y la ética en el uso de los datos y los componentes de inteligencia artificial basada en un enfoque de riesgos;
- Adoptar y mantener procedimientos para que la realización de cualquier tratamiento de datos deba superar una evaluación de impacto en materia de protección de datos que incluya el análisis de la ética en el uso de los datos y los componentes de inteligencia artificial;
- Tener en cuenta y coordinar en su seno los programas de gobernanza del dato y de gestión del riesgo de seguridad de la información cuya gobernanza y competencia se gestionan en los respectivos comités de Seguridad de la Información y de Gobierno de la Información y calidad del dato, en la medida que afectan a la confidencialidad de la información y la protección de datos personales. A estos efectos formaran parte del comité de privacidad el CISO y el CDO.
- Disponer de un protocolo de gestión de brechas de datos personales;
- Diseñar y promover cuantos programas de formación y concienciación sean necesarios para reforzar la cultura de la privacidad, la confidencialidad de la información, la protección de los datos personales y el uso ético de los datos y los componentes de inteligencia artificial, así como cumplimiento de las políticas y normas de privacidad y protección de datos y ética de las que se haya dotado CaixaBank; en esta tarea, el comité de privacidad se coordinará con el resto de acciones formativas que se realicen en CaixaBank en la medida en que dichas formaciones y programas de concienciación se dirijan a garantizar la protección de la información y de los datos personales
- Acreditar una selección responsable de proveedores con acceso a datos de carácter personal;
- Monitorizar los criterios externos en materia de protección de datos y ética en el uso de los datos y los componentes de inteligencia artificial de manera que estén identificados, en todo momento los requerimientos legales vigentes, los criterios de las autoridades de control, así como de las “mejores prácticas” del sector;
- Proponer al Comité de Dirección el nombramiento de un Delegado de Protección de Datos de acuerdo con los criterios establecidos en la presente Política y en el RGPD.

5.2.4 Comité de Gestión de Riesgo y Evaluación de impacto

El Comité de Gestión de Riesgo y Evaluación de impacto es el órgano (en adelante Comité PIA) dependiente del Comité de Privacidad de CaixaBank,en el que Credifimo delega sus funciones de análisis y sanción de nuevos tratamientos de datos personales y del uso ético de los datos y los componentes de inteligencia artificial.

Sus decisiones deben ser ratificadas en el Comité Corporativo de Privacidad, y en el caso de Credifimo, en el Consejo de Administración.

5.2.5 Grupo de Seguimiento de protección de datos de Empresas del Grupo

El Grupo de seguimiento de protección de datos de Empresas del Grupo es el órgano dependiente del Comité de Privacidad, mediante el cual, el Delegado Corporativo de Protección de Datos desempeñará, respecto de las sociedades del Perímetro, entre las que se encuentra Credifimo, las funciones previstas en la normativa, así como en sus respectivas Políticas de Privacidad.

En este comité el DPO trasladará a Credifimo los criterios adoptados por el Comité de Privacidad en relación con la privacidad. Al mismo, asisten además de los responsables de privacidad de las sociedades del Perímetro los DPOs nacionales que, en su caso, se hayan nombrado.

5.3 .Órganos de Gobierno de Credifimo

Los órganos de gobierno de Credifimo:

- Adoptarán las decisiones oportunas a efectos de integrar las disposiciones de la presente Política y aplicar las directrices en ellas establecidas, atendiendo a las particularidades propias de cada sociedad y a la normativa legal o regulatoria que les resulte aplicable.
- Establecerán y supervisarán la implantación de una cultura de riesgos en la organización que promueva conductas acordes con la identificación y mitigación del riesgo de privacidad y protección de datos.
- Establecerán y mantendrán una estructura organizativa adecuada para la gestión del riesgo de privacidad y protección de datos que sea proporcionada a la naturaleza, escala y complejidad de las actividades que desarrollan.
- Velarán por que el personal involucrado en la gestión del riesgo de privacidad y protección de datos cuente con la competencia y experiencia adecuadas.
- Establecerán los mecanismos de seguimiento y escalado en caso de traspasar alguno de los umbrales que se definan.
- Velarán por que existan suficientes controles internos sobre la privacidad y la protección de datos.
- Adoptaran como propia, con las especialidades que se consideren necesarias, la metodología de Evaluaciones de Impacto (PIA) de CaixaBank, en los casos en los que se tenga la obligación de realizar las mencionadas Evaluaciones de Impacto.
- Adoptaran como propia, con las especialidades que se consideren necesarias, la metodología de atención de ejercicio de derechos de CaixaBank.
- Adoptaran como propia, con las especialidades que se consideren necesarias, la metodología de comunicaciones de violaciones de seguridad de CaixaBank

5.3.1 Consejo de Administración

Como máximo responsable del establecimiento de estrategias y políticas generales de la Entidad es el encargado de:

- Aprobar la Política de Privacidad de Credifino.
- Aprobar las normas, estatutos o reglamentos internos necesarias para cumplir con la normativa de protección de datos.
- Supervisar el cumplimiento del respeto en la Entidad al derecho fundamental a la protección de datos personales, directamente o a través de los órganos que se prevén en la mencionada Política.

6. Marco de gestión para la privacidad y la protección de datos

6.1. Delegado de Protección de Datos (DPO)

Es el asesor y supervisor del cumplimiento de la normativa sobre privacidad. El Delgado de Protección de Datos de CaixaBank es corporativo, y Credifimo, por acuerdo correspondiente de su Consejo de Administración, designó como Delegado de Protección de Datos al Delegado de Protección de Datos de CaixaBank.. Sus responsabilidades, obligaciones, y pautas de funcionamiento se detallan a continuación.

6.1.1 Nombramiento

Es responsabilidad del Consejo de administración de Credifimo el nombramiento del Delegado de Protección de Datos, así como el seguimiento de su desempeño. Se nombrará al Delegado de Protección de Datos:

- Atendiendo a sus cualidades profesionales y, en particular, a sus conocimientos especializados en derecho, la práctica en materia de protección de datos y a su capacidad para desempeñar las funciones que se le asignan.
- Con carácter corporativo, ya que el Delegado de Protección de Datos de CaixaBank será el Delegado Corporativo de Protección de datos, del que dependerán funcionalmente los Delegados de Datos de las Empresas del Perímetro y los que pudieran nombrarse en otras jurisdicciones distintas a la española.

El nombramiento del Delegado de Protección de Datos se publicará y se comunicará a la autoridad de control.

6.1.2 Encaje organizativo y funciones

La Entidad garantizará, en todo momento, que el Delegado de Protección de Datos:

- Participa de forma adecuada y en tiempo oportuno en todas las cuestiones de protección de datos.
- Dispone de los recursos necesarios para el desempeño de sus funciones y el mantenimiento de sus conocimientos especializados y recibe formación adecuada.
- Tiene el acceso a los datos personales y operaciones objeto de tratamiento.
- Rinde cuentas directamente al más alto nivel jerárquico.
- Goza de independencia en el ejercicio de sus funciones.

El Delegado de Protección de datos, desempeñará, como mínimo, las siguientes funciones:

- Asesorar, informar y supervisar acerca del cumplimiento en las siguientes áreas/materias:
    - Aplicación de los principios relativos al tratamiento de los datos personales.
    - Identificación y aplicación de las bases jurídicas del tratamiento.
    - Compatibilidad de finalidades distintas de las que originaron la recogida.
    - Normativa sectorial que pueda afectar al tratamiento de los datos personales.
    - Información a los afectados.
    - Ejercicio de derechos de los Interesados.
    - Contratación de encargados.
    - Transferencias internacionales de datos.
    - Política de protección de datos.
    - Concienciación a los empleados y la organización.
    - Formación a los empleados.
    - Auditoría de protección de datos.
    - Registros de actividades de tratamiento.
    - Protección de datos desde el diseño.
    - Análisis de riesgo de los tratamientos.
    - Medidas de seguridad adecuadas.
    - Violaciones de seguridad.
    - En su caso, garantías para el responsable.
- Actuar como mediador entre los clientes y La Entidad en las reclamaciones sobre protección de datos.
- Cooperar y actuar como punto de contacto entre La Entidad y la AEPD u otra autoridad de control, para cuestiones relativas al tratamiento y realizar consultas sobre cualquier otro asunto.
- Actuar como punto de contacto para los Interesados y el ejercicio de derechos por su parte.

El Delegado de Protección desarrollará sus funciones prestando la debida atención a los riesgos asociados a las operaciones de tratamiento y teniendo en cuenta la naturaleza, el alcance, el contexto y fines del tratamiento.

Las funciones anteriores que, según lo establecido en la Política de Control Interno, estén atribuidas a las áreas de Cumplimiento y Auditoría Interna de CaixaBank, serán desempeñadas directa y autónomamente por estas unidades, con la coordinación establecida en el apartado 6.1.10.

6.1.3 Facultades

En el desarrollo de sus funciones el Delegado de Protección de Datos tiene atribuidas las siguientes facultades:

- Acceder a la información y a los datos personales de los Interesados.
- Acceder a las operaciones del tratamiento automatizadas y no automatizadas.
- Consultar documentación, sistemas, programas, bases de datos, y en general cualquier soporte relativo a los datos personales o a su tratamiento.
- Participar en reuniones en las que se aborden cuestiones relativas a los tratamientos de datos personales.
- Mantener la interlocución con la AEPD y con otras autoridades de control.

- Tener acceso directo y reportar periódicamente a la alta dirección, a través del Comité de Privacidad y de manera directa.
- Organizar internamente sus recursos.

6.1.4 Independencia

La Entidad no impartirá instrucciones, sancionará o destituirá al DPO por el desempeño de sus funciones. Lo anterior se entiende sin perjuicio de la facultad organizativa que le asiste.

El Delegado de Protección de Datos tiene acceso y rinde cuentas al más alto nivel jerárquico, siendo el Consejero Delegado, el Comité de Dirección y el Comité de Privacidad y los órganos de gobierno de Credifimo _en concreto, el Consejo de Administración, los órganos a los que el Delegado de Protección de Datos debe reportar periódicamente. Este reporte se concreta en el apartado 6.1.8 de esta política.

6.1.5 Disponibilidad y participación efectiva

La Entidad se asegurará de que el DPO está disponible para sus funciones internas y externas y participa efectivamente en los análisis y valoraciones acerca de tratamientos de datos personales.

6.1.6 Dotación de medios

El Delegado de Protección de Datos en el desarrollo de sus funciones contará con los medios organizativos necesarios para desarrollar su actividad y, contará con el soporte interno legal y regulatorio de La Entidad para ello. También podrá recurrir a la contratación de asesores externos para aquellos temas que, a su juicio, resulten necesarios.

Para el desarrollo correcto de sus atribuciones, el DPO deberá contar con medios adecuados para, al menos, desarrollar las siguientes funciones básicas:

- Asesorar y dar soporte a la Entidad mediante la actualización de la normativa de aplicación en protección de datos y en la detección de posibles situaciones de riesgo de cumplimiento.
- Asesorar y dar asistencia a la Entidad mediante la interpretación de normas y aportando conocimiento y análisis de la normativa vigente y de los proyectos normativos en curso con el fin de prever su impacto en La Entidad.
- Asesorar en la supervisión y en particular en el diseño de controles de primer nivel.
- Asesorar y dar soporte en la formación de los empleados en materia de protección de datos.
- Asesorar y dar soporte a la tercera línea de defensa en la realización de controles periódicos en materia de protección de datos.
- Coordinar, asesorar y dar soporte en la realización de PIAs.

6.1.7 Prevención de conflictos de interés

La Entidad aplicará al DPO y a sus colaboradores las siguientes normas para promover la independencia en el ejercicio de sus funciones:

- No podrán participar en la prestación de las actividades y servicios que controlen. Sólo podrán desarrollar responsabilidades distintas a las que le son propias cuando ello no genere potenciales conflictos de interés, lo que será garantizado por el órgano de dirección de La Entidad. La Entidad no atribuirá a una misma persona la función de DPO y las relativas a un puesto de responsabilidad en Negocio, Marketing, Recursos Humanos o Compras.
- La remuneración del DPO no podrá comprometer, ni real ni potencialmente, su objetividad y, por tanto, no podrá estar ligada al beneficio de las áreas o actividades sobre las que ejerce sus funciones como DPO.
- La remuneración variable, cuando exista, estará vinculada al nivel de gestión y desempeño y será aprobada de acuerdo con los criterios establecidos por los órganos de administración y dirección de La Entidad.

6.1.8 Reporte a los órganos de administración y dirección

El Delegado de Protección de Datos recopilará y reportará, con la periodicidad con la que se reúna el Comité de Privacidad y, como mínimo, semestralmente, la siguiente información al Comité de Privacidad y al Consejero Delegado de la Entidad:

- Estado de situación o conclusiones de los proyectos específicos que deban ser conocidos por el Comité de Privacidad en atención al riesgo inherente para los derechos de los Interesados en materia de protección de datos.
- Infracciones de la normativa de protección de datos que se hayan detectado, riesgos derivados de las mismas y medidas planteadas para su mitigación.
- Inicio y estado de situación de procedimientos inspectores y sancionadores por la AEPD u otra autoridad de control.
- Requerimientos de recursos adicionales necesarios para cumplir adecuadamente con sus funciones.
- KPIs (cuadro de mando con estadísticas) sobre ejercicios de derechos y brechas de seguridad.

Adicionalmente, el DPO reportará semestralmente esta información al Comité de Dirección y con carácter anual a los órganos de gobierno de la Entidad.

Asimismo, el DPO podrá, con carácter excepcional, elevar cualquier asunto que por su sensibilidad considere no puede esperar al *reporting* ordinario al Comité de Dirección y a los Órganos de Gobierno de CaixaBank.

La mencionada información incorporará la información correspondiente de las sociedades del Grupo. En el caso de Credifimo, el DPO reporta anualmente ante el Consejo de Administración la Memoria Anual de Privacidad.

6.1.9 Comunicación interna y externa en materia de privacidad

El DPO tendrá acceso a los instrumentos de comunicación existentes en la Entidad al objeto de fomentar la cultura de cumplimiento. En esta tarea contará asimismo con la colaboración de aquellas áreas que tengan responsabilidades en el ámbito de la comunicación interna. A tal efecto:

- Las páginas web de la Entidad contendrán una referencia al Delegado de Protección de Datos.
- El Delegado de Protección de Datos dispondrá de una sección dentro de la intranet de la Entidad en la que aparecerá la Política de Privacidad así como cualquier otra información que el DPO considere necesaria para el adecuado desarrollo de sus funciones.

6.1.10 Relaciones con las funciones de control

A los efectos de que el Delegado de Protección de Datos pueda cumplir con las funciones establecidas en la normativa, así como en la presente Política, sus relaciones con otras funciones de control (Cumplimiento Normativo, Auditoría Interna, Gestión de Riesgos) se guiarán por los principios de cooperación e información recíproca.

Las áreas de control actuarán independientemente y bajo sus propios criterios, según se establezca en cada momento en la Política de Control Interno de CaixaBank y mantendrán coordinación con el Delegado de Protección de Datos, facilitándose mutuamente la información necesaria para la adecuada supervisión y control del cumplimiento del derecho de protección de datos.

Sin perjuicio de lo anterior y en relación con las facultades de supervisión del cumplimiento de la normativa de protección de datos:

- El DPO asesorará a la primera línea de defensa en relación con los controles a implementar en sus respectivas áreas en relación con el cumplimiento de la normativa de protección de datos, siendo las correspondientes áreas o departamentos los encargados de su establecimiento y seguimiento.
- La supervisión del DPO del cumplimiento de la normativa de protección de datos se concretará en la definición e implementación de controles aleatorios y en función del riesgo de los tratamientos y contemplará tanto la supervisión de los aspectos jurídicos como de los aspectos técnicos y de Seguridad de la Información.
- El DPO se coordinará con la segunda línea de defensa mediante i) su participación en las evaluaciones de impacto y en el Comité de Gestión de Riesgo y Evaluación de impacto y, ii) su participación en el comité Corporativo de Privacidad a efectos de supervisar el cumplimiento de la normativa de protección de datos.
- La tercera línea de defensa realiza su cometido de manera independiente y se coordina con el DPO a través del Comité de Privacidad al que asistirán como área invitada y en el que informan de las actividades que lleven a cabo en relación con la normativa de protección de datos y su cumplimiento.

En este sentido, el Comité de Privacidad será informado periódicamente de las medidas de control en materia de privacidad que, en línea con el modelo de tres líneas de defensa de la Entidad, las áreas responsables establezcan en materia de gestión del riesgo de privacidad y protección de datos.

6.1.11 El Delegado de Protección de Datos Corporativo

Ostentará la condición de Delegado de Protección de Datos Corporativo el Delegado de Protección de Datos de CaixaBank, y tendrá como responsabilidades, adicionales a las propias en su condición de DPO de CaixaBank y de las Empresas del Perímetro que le nombren:

- Establecer las directrices generales para garantizar la adecuada gestión del riesgo de cumplimiento de la normativa de protección de datos y la implantación de la cultura de cumplimiento en relación con esta en el Grupo. Asimismo, le corresponde establecer las directrices generales a los efectos de garantizar una interpretación homogénea de la norma en el Grupo
- Proponer la creación de órganos colegiados con alcance de grupo
- Promover el desarrollo de un marco de relaciones con los equipos de las Sociedades del grupo

- Comunicar todos aquellos aspectos que sean de interés (lecciones aprendidas, mejores prácticas, etc…) en las empresas del grupo
- Participar en el nombramiento y, en su caso, en el cese de los DPO nacionales de manera que propuesto el o los candidatos o el cese y sus motivos, el DPO Corporativo procederá a remitir su informe
- Participar, en lo que se refiere a la fijación de retos, evaluación del desempeño y determinación de la remuneración fija y variable de los DPO nacionales, para lo que la sociedad con presencia en el extranjero informará al DPO Corporativo con carácter previo a la adopción de las correspondientes decisiones debiendo este último remitir su informe a la filial
- Participar y conocer toda comunicación regular con los supervisores locales por parte de las sociedades del grupo
- Participar y conocer en todo momento el estado de la gestión de la privacidad en las sociedades del grupo

6.2 Otras figuras responsables

6.2.1 Responsable de Privacidad

Figura responsable del control y cumplimiento de la normativa de privacidad en Credifimo nombrado por los órganos de gobierno. El Responsable de Privacidad será el máximo responsable de la gestión de la privacidad en su organización. A estos efectos, se coordinará con el Delegado de Protección de Datos.

Ostentará la condición de Responsable de Privacidad quien así haya sido nombrado por el Consejo de Administración de la Entidad.

6.3 Tratamientos y Legitimación

La Entidad tratará los datos personales de los Interesados para las siguientes finalidades:

- “Precontractuales” o “contractuales”: para atender solicitudes en relación con sus servicios y prestarlos con arreglo a la calidad que se espera. La actividad de Credifimo, como entidad de crédito, requiere que se obtenga determinada información, se analice, conserve, actualice, y acceda a ella, en respuesta a quienes se interesan o piden los servicios a la Entidad. También se necesita tratar la información de los candidatos y empleados para, en su caso, entablar una relación laboral o gestionarla. Lo mismo sucede en el caso de la relación mercantil que mantiene con sus proveedores.
- “Regulatorias o normativas”: para cumplir las obligaciones exigidas por las diferentes normativas, políticas y códigos, como, por ejemplo: la adopción de medidas de diligencia debida en la prevención del blanqueo de capitales y de la financiación del terrorismo, fiscal, de prevención del fraude, sanciones internacionales o aquellas obligaciones de reporte requeridas por las autoridades reguladoras del sector financiero.
- “Organizativos y de prevención del fraude”: La Entidad puede tratar los datos con dicha finalidad según la necesidad para la ejecución de las relaciones contractuales, la obligación legal o el interés legítimo.

6.4 Derechos de los interesados

La Entidad facilita a los Interesados el ejercicio de sus derechos según se definen en el **Anexo 1**:

- Derecho de acceso.

- Derecho de rectificación.
- Derecho de supresión.
- Derecho a la limitación del tratamiento.
- Derecho de portabilidad.
- Derecho de oposición.
- Derecho a la retirada del consentimiento.
- Derecho a no ser objeto de una decisión automatizada

Para ello, La Entidad se ha dotado de los procedimientos, así como de las herramientas y recursos necesarios para realizar una gestión centralizada de los derechos que le permita facilitar a los interesados el ejercicio de éstos mediante canales físicos como digitales. El detalle de estos procedimientos se reflejará actualizado en la Norma de Privacidad de La Entidad.

6.5 Evaluaciones de impacto

Entre los requerimientos y obligaciones que establece el RGPD destaca la necesidad de evaluar el impacto de las actividades de tratamiento en la protección de los datos personales siempre y cuando sea probable que el tratamiento suponga un riesgo significativo para los derechos y libertades de las personas (PIA).

En este sentido, La Entidad se ha dotado de un procedimiento, así como de una metodología para la realización de las mencionadas evaluaciones de impacto.

Este procedimiento se basa en el principio de que todos los tratamientos que se realicen deben ser detallados por su promotor, debe hacerse una evaluación de sus riesgos, y las medidas necesarias para mitigarlos y la decisión sobre la viabilidad del tratamiento propuesto debe ser sancionada por el Comité de Gestión del Riesgo y Evaluación de impacto.

El detalle de estos procedimientos se reflejará actualizado en la norma de privacidad de La Entidad.

6.6 Medidas técnicas

La Entidad aplica las medidas técnicas y organizativas necesarias para mitigar los riesgos asociados con la protección de la información personal y de los derechos y libertades de los Interesados.

Las medidas generales destinadas a evitar los riesgos sobre la alteración, pérdida, indisponibilidad y tratamiento o acceso no autorizado a la información se describen en la Política de Seguridad de la Información del Grupo CaixaBank, la cual resulta de aplicación a la Entidad. Desde un enfoque preventivo y proactivo se definen las medidas a aplicar en los sistemas de información para proteger la información en todo su ciclo de vida. En cualquier caso, la aplicación de las medidas concretas será consecuencia del análisis y evaluación del riesgo específico para cada tratamiento, siguiendo la metodología prevista para las Evaluaciones de Impacto (PIAs).

Además, la Entidad, aplica un procedimiento común para la gestión de las brechas o violaciones de seguridad de los datos personales de acuerdo a la Política de Seguridad de la Información del Grupo CaixaBank. Dicho procedimiento incluye el registro, gestión y notificación de las violaciones de seguridad de los datos personales a la AEPD y, cuando un entrañe un alto riesgo para los derechos y libertades, también al Interesado.

Adicionalmente, Credifimo cuenta con un procedimiento interno en virtud del cual se analizan y gestionan las presuntas vulneraciones de confidencialidad que terceros denuncian. En este procedimiento de gestión, interviene la función de auditoría interna, así como el Delegado de Protección de Datos. Finalmente, es el Comité

de Incidencias quien, por delegación del Comité de Dirección, ostenta la potestad disciplinaria y, en consecuencia, a la luz de las conclusiones obtenidas de la investigación del caso concreto, aplicará el régimen disciplinario correspondiente a los y las profesionales de la Entidad.

6.7 Proveedores

La Entidad se ha dotado de los procedimientos, así como de las normas internas necesarias para realizar una selección responsable de sus proveedores de acuerdo con lo que establece la normativa de protección de datos de carácter personal.

Los procedimientos de contratación de Proveedores y los contratos de prestación de servicios de La Entidad incorporan requerimientos específicos en el caso de que la prestación de servicios correspondiente implique el tratamiento de datos personales, así como medios de seguimiento y control de los proveedores.

6.8 Comunicación y formación

Para la Entidad es fundamental que sus empleados y clientes conozcan el derecho a la protección de datos y sean conscientes de la importancia que para la Entidad tiene la confidencialidad y el respeto al derecho fundamental de la protección de datos de carácter personal de los titulares de los datos.

Por ello la Entidad cuenta con un programa de formación interno y externo en virtud del cual se forma tanto a los especialistas que asesoran y supervisan en esta materia, liderado por el Delegado de Protección de Datos. Asimismo, el Delegado de protección de Datos lidera el programa formativo al resto de los empleados de las Entidades del grupo con carácter general.

Adicionalmente, la Entidad lleva a cabo campañas de concienciación periódicas a los efectos de reforzar el mensaje acerca de la importancia de cumplir con la normativa y las obligaciones derivadas de ésta y de la presente Política. En este sentido, las campañas se definen en función de los colectivos a los que se quiere concienciar tales como clientes o empleados y dentro de esta última categoría también se adapta al puesto de trabajo. Así los programas de concienciación abarcan tanto a los empleados como a los miembros de los distintos comités y a los miembros de los órganos de gobierno.

En relación con los proveedores y su personal a los que la Entidad puede recurrir para la prestación de servicios, Credifimo incorpora en sus relaciones contractuales con los mismos, la necesidad de formación en materia de protección de datos, así como disponen de un programa de formación directa a sus agentes y ETTs en materia de protección de datos

7. Marco de control

CaixaBank promueve una cultura de riesgos en el Grupo que fomente el control del riesgo y el cumplimiento, así como el establecimiento de un marco de control interno robusto que alcance a toda la organización y que permita tomar decisiones plenamente informadas sobre los riesgos asumidos.

El marco de control interno del Grupo CaixaBank se vertebra según el modelo de Tres Líneas de Defensa, que garantiza la estricta segregación de funciones y la existencia de varias capas de control independiente:

- La **primera línea de defensa** estará integrada en los procedimientos y procesos de las unidades operativas que gestionen efectivamente el riesgo de privacidad y protección de datos. Estas unidades serán responsables de la aplicación de las políticas y procedimientos internos en materia de privacidad y protección de datos; implantarán proactivamente medidas de identificación, gestión y mitigación del riesgo de privacidad y protección de datos; establecerán e implantarán controles adecuados, y será la responsable de conocer y aplicar las obligaciones derivadas de la presente Política.

  En concreto, y ya en el ámbito de actuación propio de la Entidad, actúa como primera línea de defensa en la gestión del riesgo de privacidad y protección de datos la Dirección de Asesoría Jurídica de CaixaBank junto con la Dirección de Medios de CaixaBank, que proporcionará los criterios y métodos generales para la identificación, evaluación, tratamiento y comunicación de los riesgos tecnológicos asociados al riesgo de protección de datos y privacidad a través de la figura del CISO de CaixaBank (*Chief Information Security Officer*), responsable de la Dirección de *Information Security*, que pertenece a la Dirección de CTO (*Chief Technology Officer*). Asimismo, la Dirección de Medios tiene la competencia del análisis, diagnóstico y adopción de las medidas de contención y protección necesarias a nivel técnico y operativo:

  - Identificar y evaluar los riesgos asociados a sus procesos. Identificar posibles riesgos emergentes.
  - Identificar, definir, implantar y actualizar los controles de dichos riesgos y controlar, en primera instancia, su aplicación.
  - Elaborar e implantar las normas y procedimientos que desarrollen las políticas de asunción y gestión de riesgos establecidas por las segundas líneas de defensa, y establecer controles, en primera instancia, para su aplicación.
  - Identificar, implantar y revisar indicadores de medición de riesgos y controles.
  - Monitorizar y evaluar periódicamente la efectividad de los indicadores y controles.
  - Identificar, de manera proactiva, las posibles debilidades de control.
  - Establecer, ejecutar y realizar el seguimiento de los planes de acción para la remediación de las debilidades de control identificadas.
  - Informar a la Dirección en los ámbitos de negocio y soporte, así como a las segundas y tercera líneas de defensa sobre la situación de los riesgos y controles, entre otros aspectos, sobre debilidades de control, planes de acción, riesgos emergentes, impacto de nueva normativa, resultados y evaluación de los riesgos y efectividad de los controles.

  Estas funciones podrán estar integradas en las propias unidades de negocio y soporte al negocio. No obstante, cuando el nivel de complejidad o intensidad así lo requieran, se establecerán unidades de control específicas, dotadas de mayor especialización, para asegurar un nivel adecuado de control de los riesgos sobre dichas actividades.

- La función de Compliance, como función de control interno que constituye la **segunda línea de defensa** del riesgo de privacidad y protección de datos**,** asegurará la calidad de todo el proceso de gestión de la privacidad y la protección de datos; revisará la coherencia con la política interna y las directrices públicas con los procesos internos relacionados con privacidad y protección de datos; validará el entorno de control específico sobre ámbitos de privacidad y protección de datos; proporcionará orientaciones sobre el diseño y revisión de los procesos relativos a privacidad y protección de datos y sobre los controles que se establezcan en las unidades de gestión de estos riesgos, y realizará un seguimiento periódico de las debilidades identificadas y de la implantación de los planes de acción asociados

En concreto, y ya en el ámbito de actuación propio de la Entidad, actúan como segunda línea de defensa en la gestión del riesgo de privacidad y protección de datos la Dirección de Compliance de CaixaBank. la Dirección de Riesgos No Financieros de CaixaBank, por el riesgo tecnológico asociado al riesgo de privacidad. Sin perjuicio de lo anterior, la Dirección de *Corporate Risk Management Function & Planning* ejercerá las funciones transversales de segunda línea de defensa que le correspondan según lo establecido en la Política corporativa de control interno.

- La función de auditoría interna, como **tercera línea de defensa**, es una función independiente y objetiva de aseguramiento y consulta, concebida para agregar valor y mejorar las operaciones del Grupo. Contribuye a la consecución de los objetivos estratégicos del Grupo CaixaBank aportando un enfoque sistemático y disciplinado en la evaluación y mejora de los procesos de gestión de riesgos y controles, y de gobierno corporativo. En particular, Auditoría Interna supervisará las actuaciones de la primera y segunda líneas con el objetivo de proporcionar una seguridad razonable a la Alta Dirección y a los Órganos de Gobierno.

El modelo de Tres Líneas de Defensa se articula en el Grupo de forma que las funciones de control interno de la entidad matriz desempeñan su misión con una visión consolidada de las sociedades del Grupo. Así, la Dirección de Compliance y la Dirección de Auditoría Interna, como áreas responsables, respectivamente, de las funciones de cumplimiento y auditoría interna en la entidad matriz, asumen la orientación estratégica, la supervisión y la coordinación con respecto a las respectivas funciones de control interno de las filiales, salvaguardando al mismo tiempo el ámbito propio de estas.

Cada una de las sociedades del Grupo CaixaBank deberá garantizar la existencia de controles sobre la adecuada aplicación de los principios generales establecidos en esta Política, así como su desarrollo en marcos y procedimientos internos de privacidad y protección de datos.

De manera adicional a lo anterior, en el marco de gobierno que establece la presente Política, y manteniendo en todo caso la independencia que la segunda y tercera líneas de defensa deben mantener, se tendrán en cuenta las funciones de supervisión que el RGPD atribuye al Delegado de Protección de Datos en relación con el cumplimiento de lo dispuesto en la normativa de protección de datos y que se concreta en la presente Política.

8. Marco de información

El establecimiento de un marco de información adecuado es fundamental para la gestión del riesgo de privacidad y protección de datos.

Los principales objetivos del marco de información son:

- Proporcionar a los Órganos de Gobierno y a la Alta Dirección, con el tiempo suficiente, información exacta, clara y suficiente que facilite la toma de decisiones y permita verificar que se está operando dentro de la tolerancia al riesgo marcada.
- Satisfacer los requerimientos de información de los organismos supervisores.
- Mantener informados a los accionistas, así como a los grupos de interés del Grupo CaixaBank en el ámbito de privacidad y protección de datos.
- Suministrar a los responsables de las distintas áreas, en especial a las áreas gestoras y a las áreas de control, los datos necesarios para poder realizar el control del cumplimiento de la estrategia definida para el Grupo en relación con la privacidad y la protección de datos.

En el ámbito del riesgo de privacidad y protección de datos, el DPO informará en los términos expuestos en el apartado 6.1.8 de esta Política.:

Asimismo, la función de gestión de riesgos y la función de cumplimiento facilitarán de forma periódica información relevante sobre el riesgo de privacidad a los Órganos de Gobierno. También se facilitará a los Órganos de Gobierno cualquier información que sobre el riesgo de privacidad se solicite.

Los informes de riesgo que se elaboren cumplirán con los principios para una eficaz agregación de datos sobre riesgos y presentación de informes de riesgos establecidos por el Comité de Supervisión Bancaria de Basilea (BCBS 239).

9. Actualización de la Política

Esta Política se someterá a revisión del Consejo de Administración con una periodicidad trienal. No obstante, la Dirección de Compliance de CaixaBank, como responsable de la Política, y el DPO, revisarán su contenido anualmente y, en caso de que lo estime pertinente, propondrá modificaciones que elevará para su aprobación por el Consejo de Administración.

Adicionalmente, la actualización de la Política se podrá iniciar, en cualquier momento, a petición de cualquiera de los implicados en la gestión del riesgo de privacidad y protección de datos que haya identificado la necesidad de su modificación; motivada, entre otras causas, por:

- Cambios en el marco normativo.
- Cambios en los objetivos y estrategia de negocio.
- Cambios en el enfoque o procesos de gestión.
- Cambios derivados de los resultados obtenidos en las actividades de seguimiento y control
- Nuevas políticas o modificaciones sobre las existentes que afecten al contenido de esta Política.
- Modificación de la estructura organizativa que implique un cambio de funciones en la gestión del riesgo de privacidad y protección de datos.

Como procedimiento de revisión, el responsable de la Política:

- Compartirá el resultado del análisis realizado con el resto de implicados en la gestión del riesgo de privacidad y protección de datos y realizará las modificaciones de la Política que sean necesarias.
- Incluirá un resumen de la revisión efectuada en el apartado “Control de versiones” de la Política.
- Propondrá al Comité Global del Riesgo presentar la revisión a la Comisión de Riesgos, donde se recabará su conformidad como paso previo a elevarla al Consejo de Administración para su aprobación.

No obstante, cuando se realicen modificaciones fuera del periodo establecido por defecto (trienal), si estas son de carácter menor, se habilita la aprobación por el Comité Global del Riesgo. A estos efectos se entiende por modificaciones menores las derivadas de cambios organizativos sin implicaciones en las funciones de gestión del riesgo de privacidad y protección de datos, correcciones meramente tipográficas o resultado de la actualización de documentos referenciados en la Política[1]. Se informará siempre a la Comisión de Riesgos de las modificaciones aprobadas por el Comité Global del Riesgo. Si la Comisión de Riesgos lo considerase oportuno, elevaría las modificaciones al Consejo de Administración.

La Dirección de Compliance, será el responsable del almacenamiento y accesibilidad de esta Política y se encargará de asegurar el correcto funcionamiento de los procesos de archivo, distribución y, en su caso, publicación. Sin prejuicio de su eventual publicación interna o externa, el acceso a la política estará limitado a aquellas personas que en su momento determine la Dirección de *Compliance*.

[1] *La “actualización de documentos referenciados en la Política” incluiría únicamente la transcripción de fragmentos de documentos aprobados por los órganos competentes (Consejo de Administración, Comité Global del Riesgo, etc.) o de preceptos normativos, siempre que el contenido modificado no sea objeto de regulación por la propia Política.*

10. Glosario

A los efectos de la presente Política se tendrán en cuenta los siguientes términos:

Término	Definición
Datos Personales	Toda información sobre una persona física identificada o identificable (el **"Interesado"**).
Interesado	Persona física identificada o identificable titular de los datos personales.
Tratamiento	Cualquier operación o conjunto de operaciones realizadas sobre datos personales o conjunto de datos personales. Comprende el tratamiento automatizado y el no automatizado. Incluye la obtención de la información, el análisis, la utilización, la modificación, la extracción o la comunicación por transmisión. También es el acceso a la información, su consulta, conservación, organización, estructuración, comunicación por difusión o por cualquier forma de habilitación de acceso, el cotejo o interconexión, la limitación y la supresión o destrucción.
Nuevo Tratamiento	Tratamiento no existente previamente en el inventario de tratamientos de la Entidad o bien tratamiento existente que presenta alguna modificación significativa, entendiendo como tal una modificación en la finalidad del tratamiento, categoría de Interesados, tipología de datos, base legitimadora del tratamiento, volumen de datos utilizados, destinatarios del tratamiento, existencia de transferencias internacionales de datos, o recursos técnicos utilizados.
Responsable	Persona física o jurídica que, solo o junto con otro, determina los fines y medios del tratamiento de datos.
Encargado	Persona física o jurídica, autoridad pública, servicio u otro organismo que trata datos personales por cuenta del responsable de un tratamiento. A efectos de esta Política, aquellos proveedores que, en el marco de la prestación de servicios correspondiente, tratan datos personales.
Delegado de Protección de Datos (DPO)	Figura responsable del asesoramiento y supervisión del cumplimento de lo dispuesto en la normativa de protección de datos.
PIA	Evaluación de impacto relativa a la protección de datos. Debe incluir, como mínimo, una descripción de las operaciones de tratamiento y de los fines; una evaluación de la necesidad y proporcionalidad de estas operaciones respecto a su finalidad; una evaluación de los riesgos para los Interesados; y las medidas de seguridad para afrontar dichos riesgos.
Comité de Gestión del Riesgo y Evaluación de impacto	Comité delegado del Comité de Privacidad responsable de evaluar las PIAs, aprobarlas, rechazarlas, o elevarlas al Comité de Privacidad.
Dossier PIA	Documento que engloba el Cuestionario PIA y el Análisis de Riesgo
Brechas o violaciones de seguridad	Violación de seguridad que ocasione la destrucción, pérdida o alteración accidental o ilícita de datos personales transmitidos, conservados o tratados de otra forma, o la comunicación o acceso no autorizados a dichos datos.
Perímetro o Grupo CaixaBank	Hace referencia a CaixaBank, S.A. y al conjunto de sociedades participadas por CaixaBank en las que ésta ejerce control conforme al art. 42 del Código de Comercio.

RGPD Reglamento General de Protección de Datos	Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos
CISO	Chief Information Security Officer
CDO	Chief Data Officer

11. Anexos

ANEXO 1 - DERECHOS DE LOS INTERESADOS

La Entidad facilita a los Interesados el ejercicio de sus derechos respecto de sus datos personales. En concreto, cuando el Interesado solicita:

- **Derecho de acceso:** La Entidad confirma al Interesado si está tratando sus datos personales y le facilita copia en formato electrónico si ha presentado su solicitud por estos medios, en su caso.
- **Derecho de rectificación:** La Entidad rectifica o completa los datos personales del Interesado, si estos son inexactos.
- **Derecho de supresión:** La Entidad suprime los datos personales del Interesado si se dan determinadas circunstancias (cuando estos ya no sean necesarios para los fines para los que fueron recogidos; el Interesado ha retirado su consentimiento, etc.). No obstante, la Entidad mantendrá los datos bloqueados, es decir, con acceso limitado, en caso de que sean necesarios para el cumplimiento de una obligación legal y solo para estos fines o cuando el tratamiento siga siendo necesario conforme al RGPD.
- **Derecho a la limitación del tratamiento:** La Entidad restringe el tratamiento de los datos si se cumple alguna de las condiciones previstas en el RGPD, esto es, cuando se ejerza un derecho de rectificación, o de oposición, o lo solicite el Interesado. No obstante, la Entidad podrá tratar los datos para conservarlos y para la formulación, el ejercicio o la defensa de sus derechos, o para proteger los derechos de otra persona física o jurídica o por razones de interés público importante de la Unión o de un Estado miembro
- **Derecho de portabilidad:** La Entidad facilita al Interesado los datos que este haya proporcionado, en un formato estructurado, de uso común y lectura mecánica, siempre y cuando el tratamiento esté basado en el consentimiento del Interesado o en un contrato y se efectúe por medios automatizados.
- **Derecho de oposición:** La Entidad se abstiene de un tratamiento de datos personales si el Interesado se opone por motivos relacionados con su situación particular o si el tratamiento se basa en el interés legítimo de la Entidad salvo que esta tenga motivos legítimos imperiosos prevalentes.
- **Derecho a la retirada del consentimiento**: La Entidad no realizará tratamientos basados en el consentimiento cuando el titular del dato haya manifestado su voluntad de revocarlo
- **Derecho a no ser objeto de una decisión automatizada:** ante decisiones automatizadas la Entidad facilitará a los titulares de los datos objeto de ésta su derecho a expresar su punto de vista y a impugnar la decisión, así como obtener intervención humana.