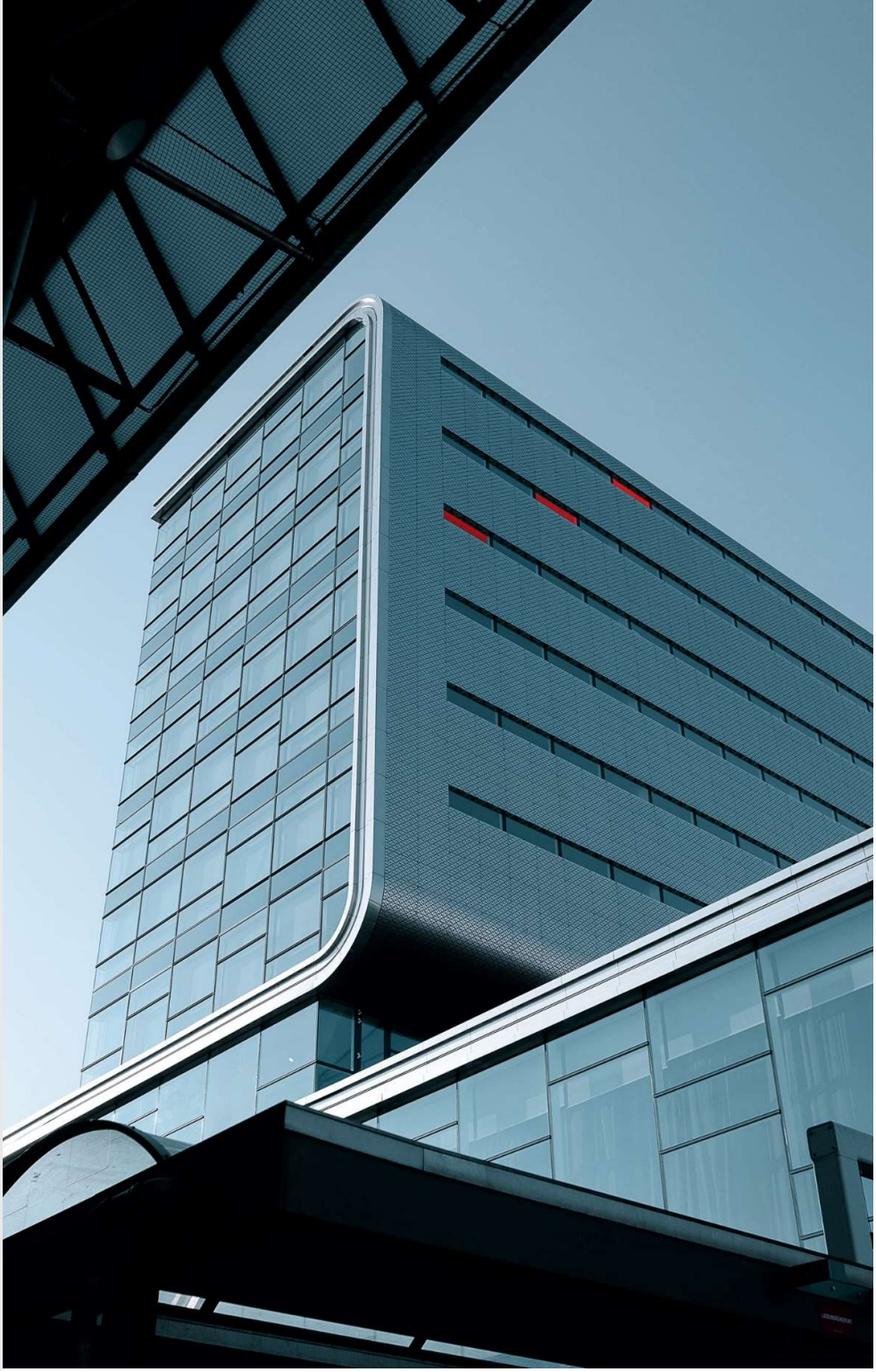
Política de protección de datos

Junio 2023



Santander Alternative Investments, SGIIC, S.A.U.
Sociedad Gestora de
Instituciones de Inversión Colectiva

SAI Risk & Compliance

Contenido

1. INTRODUCCIÓN

La política de protección de datos tiene como objetivo definir los criterios en materia de protección de datos, desarrollando a este respecto el Marco Corporativo de Cumplimiento y Conducta en relación con el control de la información y confidencialidad, y cumpliendo con las exigencias legales en materia de protección de datos.

De esta manera, enlaza con sus valores éticos y ratifica su firme compromiso de mantener una conducta respetuosa, tanto con las normas como con los estándares, que los empleados del Santander Alternative Investments, SGIIC, S.A.U. (en adelante SAI) deben tener en cuenta en su operativa diaria.

El tratamiento de datos personales tiene una incidencia directa en la operativa diaria de SAI dado que, en su actividad diaria, estos se procesan de manera recurrente.

Esta política se enmarca en la regulación siguiente:

- Reglamento General de Protección de Datos (en adelante, RGPD) es el reglamento europeo relativo a la protección de las personas físicas en lo que respecta al tratamiento de sus datos personales y a la libre circulación de estos datos.
- Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales.
- Ley 34/2002 de Servicios de la Sociedad de la Información (LSSI).

2. DEFINICIONES Y ALCANCE

La presente política aplica a los datos de carácter personal y su tratamiento.

Para una mejora comprensión de este documento, se definen los siguientes términos/conceptos:

- Dato de carácter personal: cualquier información numérica, alfabética, gráfica, fotográfica, acústica o de cualquier otro tipo (por ejemplo, datos biométricos), concerniente a personas físicas identificadas o identificables.

    - Información de identificación directa: datos que incluyen información que permita identificar o distinguir a una persona física directamente y por sí mismos sin necesidad de combinarlos con otros datos, como por ejemplo: nombre, dirección, número de teléfono, número de fax, dirección de correo electrónico, perfiles identificadores únicos, como el número de la seguridad social, el número del pasaporte, etc.

        - Datos de carácter identificativo: Documentos identificativos (DNI, número de

identificación oficial o fiscal, o pasaporte), dirección, imagen, voz, número de seguridad social, teléfono, marcas físicas, nombre y apellidos, número de empleado, firma, huella y firma electrónica.

- Datos biométricos: datos personales obtenidos a partir de un tratamiento técnico específico, relativos a las características físicas, fisiológicas o conductuales de una persona física que permitan o confirmen la identificación única de dicha persona, como imágenes faciales o datos dactiloscópicos;

- Información de identificación indirecta: datos personales que incluyen información que, aunque por sí misma no pueda identificar ni distinguir directamente a la persona, SAI o un tercero puedan asociarla o vincularla con una persona física teniendo en cuenta todos los medios que probable y razonablemente se puedan usar. Se trata por tanto de datos que por sí solos no permiten la identificación de las personas pero que combinados junto con otros factores pueden permitir la identificación.

- Dato pseudoanónimos: aquellos que no pueden atribuirse a un interesado específico sin usar información adicional, siempre que dicha información adicional se guarde por separado y esté sujeta a medidas técnicas y organizativas que garanticen que no se atribuye a una persona física identificada o identificable. Estos datos seguirán considerándose datos de carácter personal en tanto en cuanto se pueda llegar a identificar a la persona física a la que corresponden. En cualquier caso, el proceso de pseudonimización de los datos será una de las medidas a aplicar para minimizar riesgos en materia de protección de datos

- Datos anónimos: datos que no permiten identificar a una persona ni la hacen de forma alguna identificable y por tanto los excluyen del ámbito de aplicación de la normativa en materia de protección de datos. Los datos anonimizados nunca serán considerados datos de carácter personal.

- Interesado: persona física titular de los datos sometidos a tratamiento, esto es la persona física a los que los datos identifican o hacen identificable.

- Responsable de Tratamiento: persona física o jurídica, que determina los fines y medios del tratamiento. Aplicará medidas técnicas y organizativas apropiadas con el fin de garantizar y poder demostrar que sus tratamientos son conformes con la normativa de protección de datos en vigor.

- Encargado de Tratamiento: persona física o jurídica que trata datos personales por cuenta del Responsable del Tratamiento. Deberá cumplir con las instrucciones del

Responsable del Tratamiento y con las exigencias de la normativa de protección de datos en vigor.

Pondrá a disposición del Responsable de Tratamiento toda la información necesaria para demostrar el cumplimiento de sus obligaciones y ofrecerán garantías suficientes, de manera que el tratamiento sea conforme con los requisitos de la normativa y garantice la protección de los derechos de los interesados.

- Autoridad de Control: Autoridad pública independiente encargada de supervisar la aplicación de la normativa en materia de protección de datos, con el fin de proteger los derechos y las libertades fundamentales de los interesados.
- Incidente de seguridad: Evento que afecta a datos de carácter personal:
    - Brecha de confidencialidad: Acceso, comunicación y/o uso no autorizado a los datos personales de una o varias personas físicas.
    - Brecha de integridad: Modificación, destrucción, pérdida o alteración accidental o ilícita de los datos personales trasmitidos, almacenados o tratados de una o varias personas físicas sin su autorización.
    - Brecha de disponibilidad: Imposibilidad de acceso a los datos personales.
- Transferencia internacional de datos: flujo de datos personales entre países con diferentes regímenes jurídicos en materia de protección de datos.
- Cookies y tecnologías similares de seguimiento (local shared objects, web beacons, web bugs, pixeles de tracking, etc.): ficheros que se descargan y almacenan en el equipo (ordenador/Smartphone/Tablet) del usuario que navega a través de Internet al acceder a determinadas páginas web y aplicaciones y que se utilizan para almacenar y recuperar información sobre la navegación que se realiza desde ese equipo.
- Responsable de Protección de Datos: Figura encargada de velar y asesorar sobre el cumplimiento de la normativa de protección de datos en la entidad; además es el punto de contacto con la Autoridad de Control y con los interesados.
- Función Corporativa de Protección de Datos: Encargada de supervisar el cumplimiento en las distintas entidades del Grupo Santander afectadas por la normativa de protección de datos. Así mismo, es la encargada del control directo en los negocios y funciones corporativas ubicadas en la Corporación.

La gestora deberá velar por la confidencialidad, seguridad e integridad de la información de carácter personal de la que es responsable, así como procurar que todos los terceros con acceso a datos de la entidad cumplan con las garantías y obligaciones legales y contractuales respecto al tratamiento de los datos e información a los que acceden.

3. AMBITO DE APLICACIÓN Y TRANSPOSICIÓN EN FILIALES

Esta Política, afecta a SAI y ha sido elaborada tomando como referencia la política recibida de SAM Investment Holdings, S.L. adaptándola localmente para establecer el régimen aplicable en materia de protección de datos.

Dicha adaptación ha sido validada previamente por SAM Investment Holdings, S.L.

4. CRITERIOS

Todos los empleados estarán obligados a respetar la intimidad de todos los interesados a cuyos datos tengan acceso como consecuencia de la propia actividad o el desempeño de sus funciones, ya sean clientes, otros empleados o cualesquiera otras personas físicas.

Como principio general se deberá velar por la confidencialidad, seguridad e integridad de la información de carácter personal, y procurar que todos los proveedores con acceso a datos personales cumplan con las garantías y obligaciones legales y contractuales respecto al tratamiento de los datos personales e información a la que accedan.

Se detallan a continuación los criterios corporativos encaminados a asegurar el correcto cumplimiento de las obligaciones de la normativa aplicable en materia de protección de datos de carácter personal:

4.1 Licitud, proporcionalidad y transparencia.

Los datos de carácter personal se tratarán de manera:

- Lícita: Se obtendrán los datos siguiendo los requerimientos que establezca la normativa aplicable.

  El tratamiento de los datos personales se realizará siempre utilizando alguna de las siguientes bases legitimadoras:

  - Se dispone del consentimiento por parte del interesado para el tratamiento de sus datos.
  - El tratamiento es necesario para la ejecución de un contrato en el que el interesado es parte o para la aplicación a petición de éste de medidas precontractuales.
  - El tratamiento es necesario para el cumplimiento de una obligación legal aplicable al Responsable y Encargado del Tratamiento.

- El tratamiento es necesario para proteger intereses vitales de los interesados o de otras personas físicas.

- El tratamiento es necesario para el cumplimiento de una misión realizada en interés público o en el ejercicio de poderes públicos conferidos al Responsable del Tratamiento.

- El tratamiento sea necesario para la satisfacción de intereses legítimos perseguidos por el Responsable del Tratamiento o por un tercero, siempre que sobre dichos intereses no prevalezcan los intereses o los derechos y libertades fundamentales del interesado que requieran la protección de datos personales, en particular, cuando el interesado sea un menor.

En el ámbito de la utilización de cookies u otros dispositivos de seguimiento, deberán ser analizadas y adaptadas, obteniendo el consentimiento en caso necesario.

- Proporcional: Se tratarán los datos únicamente acordes con las finalidades que sean necesarias, adecuadas y pertinentes.
- Transparente: La información a proporcionar en materia de protección de datos debe ser clara, concisa, transparente, inteligible y de fácil acceso, con un lenguaje claro y sencillo sin ambigüedades, es decir, fácil de entender por el interesado.

4.2 Finalidades compatibles con el origen de la recogida.

Deberá asegurarse que el tratamiento de los datos personales se circunscribe a los fines determinados, explícitos y legítimos para los que fueron recogidos los datos en origen y que no serán tratados ulteriormente de manera incompatible con dichos fines.

En este sentido, cabe aclarar que aquellas actividades de tratamiento ulterior con fines de archivo en interés público, fines de investigación científica e histórica o fines estadísticos deben considerarse actividades de tratamiento lícitas compatibles

Como regla general, será necesario que se solicite el consentimiento expreso de los interesados cuando el tratamiento de los datos vaya más allá de los fines para los que se recogieron inicialmente y no sean compatibles con los mismos. Con objeto de determinar la compatibilidad de los fines de tratamiento, se deberá tener en cuenta:

- Cualquier relación entre los fines para los cuales se hayan recogido los datos personales y los fines del tratamiento ulterior previsto;
- El contexto en que se hayan recogido los datos personales.
- La naturaleza de los datos personales, en concreto cuando se traten de datos especialmente protegidos.
- Las posibles consecuencias para los interesados del tratamiento ulterior previsto;

- La existencia de garantías adecuadas, como podrán ser el cifrado o la seudonimización.

Así pues, siempre y cuando el tratamiento de datos no esté basado en el consentimiento, el tratamiento de datos personales con fines distintos de aquellos para los que hayan sido recogidos inicialmente sólo debe permitirse cuando sea compatible con los fines de su recogida inicial. En todo caso habrá que cumplir con los requisitos de transparencia que imponga la normativa local aplicable.

4.3 Minimización y exactitud de los datos personales.

Los datos personales serán adecuados, pertinentes y limitados a lo necesario en relación con los fines específicos para los que son tratados. Se deberá analizar en cada caso (en el alta del tratamiento o cuando se produzca una modificación sustancial del mismo) los tipos de datos que se recogen y los procesos asociados al tratamiento con un criterio de minimización, de manera que se acceda al menor número de datos personales necesarios para su ejecución.

Asimismo, se deberán adoptar todas las medidas razonables para suprimir o rectificar todos aquellos datos que puedan resultar innecesarios, inexactos o incompletos, con respecto a las finalidades para los que se lleva a cabo el tratamiento. Se deberán establecer procesos periódicos de revisión sobre la necesidad, exactitud y completitud de los datos.

4.4 Integridad, confidencialidad, disponibilidad y resiliencia.

Se deberá asegurar que los datos sean tratados con el debido nivel de seguridad, incluida la protección contra el tratamiento no autorizado o ilícito y contra su pérdida, destrucción, indisponibilidad o daño accidental, mediante la aplicación de medidas técnicas u organizativas apropiadas, como por ejemplo la pseudonimización o el cifrado de datos personales. De acuerdo con la Política Corporativa de Gestión y Gobierno del Dato, todos los datos involucrados en un evento de datos (incluidos los datos personales) deberán estar categorizados de acuerdo con la semántica del Grupo.

Adicionalmente, se procurará que los empleados, los terceros que presten servicios, las empresas subcontratadas por los terceros y los empleados de éstas, que en el desempeño de sus funciones tengan acceso a datos personales, se comprometan a guardar secreto y a no comunicar, en ningún caso, a terceras personas dicha información personal, salvo autorización expresa u obligación legal. En este sentido todas las personas con acceso a datos de carácter personal deberán firmar un acuerdo de secreto y confidencialidad o estar sujetas a una obligación de confidencialidad de naturaleza estatutaria.

4.5 Conservación de los datos personales

Se deberá mantener los datos personales que sean objeto de tratamiento de forma que únicamente se permita la identificación de los interesados para los fines legítimos del

tratamiento y durante el tiempo estrictamente necesario. Una vez transcurrido este plazo, el dato deberá ser suprimido (lo que podría suponer en algunos casos el bloqueo o la anonimización cuando no sea posible la supresión. Cualquier retención de los datos deberá ser objetivamente justificable y fundamentada. Para la determinación de los plazos de conservación, se tendrá en cuenta la normativa local y, en particular, los plazos previstos en materia de prevención de blanqueo de capitales y financiación del terrorismo y de prescripción de las acciones penales, mercantiles, civiles y laborales aplicables.

No obstante, y dado que la normativa local aplicable lo permite, los datos personales podrán conservarse durante un período más allá del necesario siempre que se traten exclusivamente con fines de archivo en interés público, fines de investigación científica o histórica o fines estadísticos, sin perjuicio de la aplicación de las medidas técnicas y organizativas apropiadas para proteger los derechos y libertades de los interesados.

4.6 Deber de información

Antes de recabar cualquier tipo de dato personal, se deberá comunicar a los interesados de manera sencilla y clara, de modo que sea fácil de entender, la siguiente información:

- Los datos de contacto de la entidad jurídica Responsable del Tratamiento de los datos.
- Los datos de contacto del Responsable de Protección de datos.
- Los fines del tratamiento a que se destinan los datos personales.
- La base jurídica legitimadora del tratamiento de los datos.
- Los destinatarios o las categorías de destinatarios de los datos personales.
- Las categorías y tipología de datos personales tratadas.
- El plazo durante el cual se conservarán los datos personales o, cuando no sea posible, los criterios utilizados para determinar este plazo.
- La posibilidad para los interesados de ejercitar sus derechos sobre sus datos personales.
- El derecho a presentar una reclamación ante la Autoridad de Control o Autoridad Competente, en su caso.
- Si la recogida de datos personales es un requisito legal, contractual o precontractual.
- Cuando los datos personales se obtengan a través de terceros, la fuente de la que proceden los datos personales y, en su caso, si proceden de fuentes de acceso público.

4.7 Derechos de los interesados

Se deberá informar a todos los interesados o terceros que les faciliten los datos de los interesados sobre la normativa aplicable, los riesgos concurrentes, las salvaguardias y los

derechos relativos al tratamiento de sus datos de carácter personal, mediante las pertinentes cláusulas o avisos de privacidad.

En este sentido, se facilitarán al interesado los medios para el ejercicio de sus derechos de forma sencilla y gratuita y se realizará la gestión oportuna y necesaria de los derechos ejercidos por los interesados.

A modo enunciativo, los derechos de los interesados recogidos por la normativa europea de protección de datos son los siguientes:

- Derecho de acceso: derecho a obtener del Responsable del Tratamiento confirmación sobre el tratamiento de los datos personales y acceso a los mismos.
- Derecho de rectificación: derecho a obtener por parte del Responsable del Tratamiento, sin dilación indebida, la rectificación de los datos personales inexactos de los que es titular.
- Derecho de cancelación o supresión (derecho al olvido): derecho a obtener por parte del Responsable del Tratamiento, sin dilación indebida, la supresión de los datos personales de los que es titular.
- Derecho a la limitación del tratamiento: derecho a solicitar la limitación del tratamiento de los datos personales de los que sea titular en caso de inexactitud, ilicitud, de que ya no sean necesarios para el Responsable del Tratamiento y/o de forma temporal mientras se verifica la solicitud del derecho de oposición por parte del Responsable del Tratamiento.
- Derecho a la portabilidad de los datos: derecho a recibir en un formato estructurado de uso común y lectura mecánica los datos personales de los que es titular y que sean objecto de un tratamiento basado en el consentimiento y se efectúe por medios automatizados.
- Derecho de oposición: derecho a que el Responsable del Tratamiento deje de tratar los datos personales de los que el interesado sea titular salvo que acredite motivos legítimos imperiosos.
- Derecho a no ser objeto de una decisión basada únicamente en un tratamiento automatizado: únicamente en tratamientos automatizados y que produzca efectos jurídicos en el interesado o le afecte significativamente.

4.8 Privacidad desde el diseño y por defecto

La privacidad desde el diseño tiene como objetivo que la protección de los datos de carácter personal se encuentre presente desde las primeras fases de concepción de un producto o servicio, mientras que la privacidad por defecto persigue que sólo sean objeto de tratamiento los datos personales que sean estrictamente necesarios para cada una de las finalidades legitimadas.

Para cumplir con lo anterior, se adoptarán medidas técnicas y organizativas que incorporen en todo momento garantías necesarias, como por ejemplo la pseudonimización, la limitación del

acceso a los datos, el período de conservación de los datos, la homologación de proveedores con acceso a datos personales, las garantías adecuadas en el caso de transferencias internacionales de datos, el análisis de nuevos productos y servicios, etc.

4.9 Responsabilidad proactiva

En línea con el principio de responsabilidad proactiva, en general se dispondrá de todas las evidencias que acrediten el cumplimiento con los requerimientos en la materia, como por ejemplo un registro de actividades de tratamiento, evaluaciones de impacto sobre la protección de datos que determinen las medidas apropiadas que proporcionen un nivel de seguridad adecuado al riesgo de los distintos tratamientos, un inventario de proveedores homologados en materia de protección de datos, procedimientos de gestión de incidentes de seguridad que afectan a datos personales, etc.

4.10 Incidentes de seguridad de los datos personales

Se deberá disponer de las herramientas y procesos de respuesta necesarios frente a cualquier violación de la seguridad que ocasione la destrucción, pérdida o alteración accidental o ilícita de datos personales transmitidos, conservados, o la comunicación o acceso no autorizados a dichos datos.

Adicionalmente, se deberá contar con los medios necesarios para demostrar que se ha aplicado toda la protección técnica adecuada y se han tomado las medidas organizativas oportunas que permitan determinar, a la mayor brevedad: (i) si se ha producido una violación de la seguridad de los datos personales; (ii) si constituye un riesgo para los derechos y libertades de los interesados (iii) si resulta necesario informar a la Autoridad de Control y al interesado.

Deberán existir procedimientos claros y accesibles para todos los empleados que permitan una diligencia debida de los incidentes de seguridad que afecten a datos de carácter personal y faciliten la rápida coordinación de todas las áreas implicadas.

4.11 Transferencias internacionales de datos

Tal y como se ha definido anteriormente, por transferencia internacional de datos, se entiende un flujo de datos personales entre países con diferentes regímenes jurídicos que otorguen diferentes grados de protección en materia de protección de datos.

Se deberán aplicar las garantías adecuadas tanto en el país de origen como en el país de destino de los datos para mantener dentro de un nivel de seguridad apropiado todas las transferencias internacionales de datos personales que se efectúan, que pueden ser aportadas por cláusulas contractuales tipo, códigos de conducta, mecanismos de certificación o normas corporativas vinculantes.

5. GOBIERNO Y FACULTADES

El gobierno en materia de protección de datos se realizará como se describe a continuación, sin perjuicio del cumplimiento de la normativa corporativa general que sea de aplicación.

La función de Protección de Datos informará periódicamente al comité de riesgos de las cuestiones relevantes en materia de protección de datos dentro de SAI, y al menos anualmente del estado de cumplimiento a la función global de protección de datos del grupo SAM

6. TITULARIDAD, INTERPRETACIÓN, FECHA DE VALIDEZ Y REVISIÓN PERIODICA

La elaboración de esta Política es responsabilidad del área de Riesgos y Cumplimiento.

Corresponde al área de Riesgos y Cumplimiento la interpretación de esta Política.

Esta Política entrará en vigor desde la fecha de su publicación. Su contenido será objeto de revisión periódica, realizándose los cambios o modificaciones que se consideren convenientes.

7. CONTROL DE VERSIONES

Versión	Responsable	Modificada por	Revisada por	Órgano de aprobación	Fecha de aprobación
1	Marian Molleda	Ana Diéguez		Consejo de Administración	20.06.2023

Versión	Descripción de los cambios
1	Política inicial aprobada