Posición de CACEIS en relación con el Reglamento General de Protección de Datos (UE) 2016/679 (el «RGPD»)

Resumen del tratamiento de datos realizado:	CACEIS Investor Services es un banco de servicios de activos especializado en funciones post-trading relacionadas con la administración y el seguimiento de todas las clases de activos. Con una sólida infraestructura de TI, ofrecemos servicios de ejecución, compensación, custodia, depositaría y valoración de activos en los mercados mundiales que ayudan a clientes institucionales y corporativos a cumplir sus objetivos de desarrollo de negocio. CACEIS Investor Services es una empresa regulada, y como tal, cumple los requisitos legales y normativos nacionales, europeos e internacionales.

Índice

1 Descripción general de los datos procesados por CACEIS (Capítulos 1 y 2 del RGPD)

CACEIS ofrece: (a) una serie de servicios de mercado esenciales para sus clientes institucionales: ejecución, compensación, gestión de operaciones, mantenimiento de posiciones, cambio de divisas, servicios de custodia y efectivo, administración de carteras, servicios de Master Data, etc.; (b) servicios adaptados a las necesidades específicas de gestoras de activos, instituciones, banca corporativa, brokers y fondos de private equity, incluidos servicios fiduciarios, estructuración de fondos, distribución de fondos, juntas de accionistas, depositaría y mantenimiento de posiciones, etc.; (c) servicios digitales para la gestión de sus datos.

En la ejecución y la entrega de estos servicios, CACEIS no solo cumple las normas y directrices técnicas, sino que también garantiza el cumplimiento de la normativa de banca y servicios de inversión nacional e internacional, tanto en la UE como en el resto del mundo.

Para cumplir esos requisitos, recogemos y tratamos información. Se recogen y utilizan Datos Personales con fines legales y reglamentarios que incluyen la ejecución de contratos. Solo recogemos, tratamos y archivamos los datos necesarios para cumplir con los requisitos obligatorios de conservación de datos. Nunca se utilizan los datos para otros fines.

En general, CACEIS se considera «responsable del tratamiento» en los servicios que presta a sus clientes.

Los Datos Personales recogidos, almacenados y utilizados pueden ser:

- Datos de personas físicas que actúan como representantes de clientes de CACEIS y sus inversores
- Datos de personas físicas que actúan como representantes de clientes potenciales de CACEIS
- Datos de terceros que nos confían nuestros clientes

Excepto en operaciones de tratamiento excepcionales, CACEIS no trata ninguna categoría especial de Datos Personales (art. 9) basada en obligaciones normativas.

2 Velar por los derechos individuales del interesado (Capítulo 4 del RGPD)

Los «derechos» individuales del interesado se preservan, protegen y garantizan mediante la implementación de políticas y procedimientos internos de CACEIS que el Delegado de Protección de Datos rige, controla y evalúa.

Los Datos Personales tratados por CACEIS los facilitan los clientes con fines contractuales o de regulación, o los recoge CACEIS directamente por motivos legales o de regulación. Esos Datos Personales obtenidos en una relación «Business to Business» se utilizan únicamente para cumplir los compromisos contractuales acordados y los requisitos reglamentarios y legales nacionales e internacionales sobre productos financieros, mercados y servicios de inversión. Los Datos Personales, por lo tanto, se mantienen y se archivan con esos fines.

CACEIS no lleva a cabo perfilados basados en Datos Personales y, a efectos de información personal en relación con blanqueo de capitales y «conozca a su cliente», puede compartir información con las autoridades cuando si estas la solicitan (por ejemplo, la Autoridad de Supervisión Prudencial (ACPR), el BCE, autoridades de Protección de Datos, entre otros).

Todas las solicitudes recibidas por CACEIS se procesan de acuerdo con la normativa aplicable. Los derechos de las personas cuyos datos se tratan y la forma de ejercitar esos derechos se describen en las notificaciones de CACEIS sobre privacidad de los datos, que también están disponibles en el sitio web de CACEIS: **https://www.caceis.com/who-we-are/compliance/**

Los derechos del interesado incluyen:

- Derecho a información básica
- Derecho de acceso
- Derecho de rectificación
- Derecho de eliminación y “derecho al olvido”
- Derecho a limitar el tratamiento
- Derecho a oponerse al tratamiento

3 Configuración de CACEIS con vistas a la aplicación del Reglamento General de Protección de Datos

3.1 CONFIGURACIÓN LEGAL DE CACEIS

CACEIS ha definido la estrategia del Grupo, una organización interna y procedimientos comunes para implementar el RGPD en lo relativo a cuestiones legales y contractuales con clientes, proveedores, contrapartes, interesados y relaciones intragrupo.

El objetivo es establecer la configuración legal y contractual que aplicarán todas las entidades y sucursales del Grupo CACEIS con terceros (clientes, proveedores y contrapartes), con interesados y entre las entidades y sucursales del propio Grupo en relación con la Protección de Datos Personales a fin de implementar los requisitos del RGPD.

3.2 CLASIFICACIÓN DE LA FUNCIÓN DE CACEIS CONFORME AL RGPD

Las definiciones de «responsable» y «encargado» del tratamiento son las siguientes:

Responsable del tratamiento o responsable:	Según el art. 4 (7) del RGPD, la persona física o jurídica, autoridad pública, servicio u otro organismo que, solo o junto con otros, **determine los fines y medios del tratamiento**; si el Derecho de la Unión o de los Estados Miembros determina los fines y medios del tratamiento, el responsable del tratamiento o los criterios específicos para su nombramiento podrá establecerlos el Derecho de la Unión o de los Estados Miembros.

Encargado del tratamiento o encargado:	Según el art. 4 (8) del RGPD, la persona física o jurídica, autoridad pública, servicio u otro organismo que trate Datos Personales **por cuenta del responsable del tratamiento**.

3.2.1 Clasificación de CACEIS conforme al RGPD en relación con sus clientes

Cuando CACEIS presta servicio a sus clientes, los servicios se proporcionan, en primer lugar, cumpliendo con toda la normativa y las obligaciones impuestas a CACEIS (incluidos los periodos de conservación de los datos); en segundo lugar, al tratarse de servicios industrializados prestados con todas las competencias necesarias, CACEIS debe establecer la finalidad y los medios del tratamiento realizado. Así, CACEIS se considera «responsable del tratamiento» conforme a las Directrices 07/2020 del Comité Europeo de Protección de Datos («CEPD») sobre los conceptos de «responsable del tratamiento» y «encargado del tratamiento» del RGPD.

No obstante, si un cliente identifica un tratamiento específico realizado por CACEIS en calidad de encargado del tratamiento en nombre del cliente según los criterios del CEPD, las instrucciones del cliente en relación con ese tratamiento específico deberán ser transmitidas a CACEIS por escrito mediante un documento vinculante que se acordará con CACEIS y que incluirá todas las características exigidas por el artículo 28.3 del RGPD (objeto, duración, naturaleza y finalidad

del tratamiento, tipo de Datos Personales y categorías de interesados del tratamiento de Datos Personales realizado por CACEIS en nombre del cliente).

En la tabla siguiente se muestran ejemplos de las características del tratamiento llevado a cabo por CACEIS:

Servicios en los que CACEIS puede realizar tratamiento de Datos Personales	Objeto, naturaleza y finalidad del tratamiento	Categorías de interesados	Tipo de Datos Personales	Base legal del tratamiento de Datos Personales	Duración del tratamiento	Clasificación de CACEIS	Comentarios
Banco depositario / fiduciario (función de depositaría, custodia de activos y mantenimiento de posiciones)	• Control de la regularidad de las decisiones de inversión y seguimiento de ratios regulatorios. Custodia de activos de fondos (contabilidad de activos financieros y mantenimiento de posiciones en activos no financieros)	Partícipes	Datos identificativos, estado civil, etc.	Ejecución de contrato	El tratamiento continuará mientras siga vigente el acuerdo de servicio pertinente, y posteriormente, sin que los Datos Personales se conserven más tiempo del necesario según la legislación vigente.	Responsable	
Custodia	• Procesos de liquidación • Tramitación de operaciones corporativas sobre posiciones tomadas en préstamo o posiciones de compra/venta • Información fiscal • Tratamiento de juntas de accionistas	Clientes, inversores	Datos identificativos, información fiscal	Ejecución de contrato	El tratamiento continuará mientras siga vigente el acuerdo de servicio pertinente, y posteriormente, sin que los Datos Personales se conserven más tiempo del necesario según la legislación vigente.	Responsable	

Administración y contabilidad de activos: Comunicación de información regulatoria	Generación de informes regulatorios en nombre de clientes (fondos, sociedades de gestión, gestoras de inversión o compañías de seguros) en función del acuerdo de servicios pertinente	Inversores o partícipes	Según el alcance del servicio, Datos Personales o de negocio (apellido, nombre, dirección de correo electrónico, números de teléfono, datos de cuenta bancaria) necesarios para la ejecución del servicio	Interés legítimo, ejecución de contrato, obligación legal	El tratamiento continuará mientras siga vigente el acuerdo de servicio pertinente, y posteriormente, sin que los Datos Personales se conserven más tiempo del necesario según la legislación vigente.	Responsable	CACEIS actúa para los clientes, pero cumple las obligaciones reglamentarias o legales
Diligencia debida de Prevención de Blanqueo de Capitales / Conozca a su cliente en nombre de clientes, tratamiento de órdenes de inversores y/o gestión de información	Tratamiento de Datos Personales de inversores de los clientes conforme a la normativa de Prevención de Blanqueo de Capitales / Conozca a su cliente y el acuerdo de servicio pertinente	Inversores y sus beneficiarios finales	Nombre, fecha de nacimiento, direcciones postal y de correo electrónico, números de pasaporte, números de teléfono, números de cuentas bancarias e información financiera para verificar el origen de patrimonio y el origen de los fondos	Interés legítimo, ejecución de contrato, obligación legal	El tratamiento continuará mientras siga vigente el acuerdo de servicio pertinente, y posteriormente, sin que los Datos Personales se conserven más tiempo del necesario según la legislación vigente.	Responsable	CACEIS cumple sus propias obligaciones regulatorias; esas obligaciones se comparten con el cliente; ni los clientes ni CACEIS tienen la posibilidad de modificar el tratamiento relativo a Prevención de Blanqueo de Capitales / Conozca a su cliente ni el tipo de Datos Personales que deben recogerse. Los clientes no pueden enviar instrucciones documentadas a CACEIS para la realización de este tratamiento.

Servicios relacionados con Distribución: Transfer Agent, agente de pagos, PTA (Prime Transfer Agent), RNI, transmisión (routing) de órdenes, seguimiento de órdenes de inversores y/o información sobre redes de distribución, en su caso, manteniendo el registro local de accionistas o partícipes.	Tratamiento relacionado con distribución local y/o transfronteriza según el acuerdo de servicios pertinente	Inversores	Datos Personales o de negocio (apellido, nombre, dirección de correo electrónico, números de teléfono, datos de cuenta bancaria) necesarios para la ejecución del servicio y posiblemente para algunas categorías especiales de Datos Personales	Interés legítimo, ejecución de contrato, obligación legal	El tratamiento continuará mientras siga vigente el acuerdo de servicio pertinente, y posteriormente, sin que los Datos Personales se conserven más tiempo del necesario según la legislación vigente.	Responsable	CACEIS actúa de acuerdo con la ley y la normativa; es una operación de tratamiento industrial sin personalización
Domiciliación de fondos y servicios de secretaría a los fondos: Particularmente, se presta asistencia para juntas de accionistas y reuniones del Consejo de Administración.	Registro de Datos Personales de «directores» de fondos en el Registro Mercantil. Prestación de servicios de secretaría en relación con juntas generales y reuniones del Consejo y los servicios de secretaría asociados al acuerdo de servicios pertinente.	Directores de fondos, inversores y, en su caso, beneficiarios finales de gestoras de inversión	Datos Personales o de negocio (apellido, nombre, dirección de correo electrónico, números de teléfono, potencialmente datos de cuenta bancaria) necesarios para la ejecución del servicio y posiblemente para algunas categorías especiales de Datos Personales	Interés legítimo, ejecución de contrato, obligación legal	El tratamiento continuará mientras siga vigente el acuerdo de servicio pertinente, y posteriormente, sin que los Datos Personales se conserven más tiempo del necesario según la legislación vigente.	Responsable	No se reciben instrucciones documentadas del cliente en relación con el tratamiento de Datos Personales o los Datos Personales. El equipo de domiciliación solo procesa los Datos Personales conforme a la normativa local aplicable o por interés legítimo para ejecutar el servicio.

Mantenimiento de red de custodios (parte de los servicios de custodia)	Proporcionar Datos Personales de inversores y beneficiarios finales a los subcustodios cuando lo exigen el mercado local o la legislación aplicable	Inversores y sus beneficiarios finales	Nombre, fecha de nacimiento, direcciones postal y de correo electrónico, números de pasaporte, números de teléfono, números de cuentas bancarias e información financiera para verificación de origen de patrimonio y origen de los fondos y posiblemente algunas categorías especiales de Datos Personales	Interés legítimo para gestionar el servicio, obligación legal según la legislación aplicable.	El tratamiento continuará del modo necesario de acuerdo con la legislación local.	Responsable	
Private Equity, Mercado Inmobiliario y Titulizaciones: Administración de fondos	Instrucciones de efectivo / Mantenimiento del Registro / Crear o actualizar y controlar procedimientos de «Conozca a su cliente» de inversores	Inversores, terceros (inquilinos)	Datos Personales o de negocio (apellido, nombre, dirección de correo electrónico, números de teléfono, datos de cuenta bancaria) necesarios para la ejecución del servicio	Interés legítimo, obligación legal	El tratamiento continuará mientras siga vigente el acuerdo de servicio pertinente, y posteriormente, sin que los Datos Personales se conserven más tiempo del necesario según la legislación vigente.	Responsable	

Comunicación multicanal: OLIS, OLISMOBILE, SWIFT y Otros formatos, TEEPI (Tailored Electronic Exchange Platform for Investors)	Portal de Internet único para todos los servicios de cliente; servicio de movilidad para información esencial para gestores de activos (seguimiento y validación de VL, monitorización de inversores en tiempo real); soluciones de conexión multiservicio mediante mensajería SWIFT; red de intercambio de datos para relaciones entre entidades financieras y sociedades de gestión	Usuarios de inversores En su caso, directores de entidades financieras y sociedades de gestión	Datos Personales o de negocio (apellido, nombre, dirección de correo electrónico, números de teléfono, datos de cuenta bancaria) necesarios para la ejecución del servicio	Interés legítimo, ejecución de contrato para clientes, obligación legal		Responsable	

Cuando se externalizan servicios a proveedores, el proveedor en general se considera encargado del tratamiento de CACEIS para el tratamiento de Datos Personales en el contexto del servicio externalizado y siguiendo instrucciones de CACEIS (ya sea CACEIS el responsable o el encargado de los Datos Personales frente al cliente).

CACEIS utiliza cláusulas estándar en todas las relaciones contractuales con sus proveedores. El propósito de la cláusula estándar es garantizar que el proveedor lleve a cabo cualquier tratamiento de Datos Personales de acuerdo con el RGDP y que existan las instrucciones correspondientes en ese sentido.

Algunas situaciones específicas pueden requerir análisis adicional de la clasificación y un ajuste de la configuración del contrato. Así ocurre en las relaciones con consultores, subcustodios y contrapartes financieras.

En todos y cada uno de los casos, las partes celebrarán un acuerdo contractual para establecer la clasificación, definir las obligaciones respectivas y acordar el flujo de comunicaciones o acciones entre las partes para el cumplimiento del RGPD.

4 Medidas organizativas de seguridad

4.1 Delegado de Protección de Datos (Capítulo 4 del RGPD, Sección 4, Artículos 37, 38, 39)

CACEIS ha designado un Delegado de Protección de datos (DPO) del Grupo. Los datos están disponibles en el sitio web de la empresa y en los sitios web de Intranet. El DPO depende directamente del Director de Cumplimiento de CACEIS, que es miembro del Comité Ejecutivo. El DPO será responsable de las actividades de Protección de Datos del Grupo y de coordinar una red de corresponsales de Protección de Datos del centro y la entidad.

Puede contactarse con el DPO de CACEIS por correo electrónico: caceisdpo@caceis.com

dpocaceissp@caceis.com

4.2 Compromiso de secreto bancario y confidencialidad (Capítulo 4 del RGPD, Sección 2, Artículos 32.1)

Todos los empleados de CACEIS tienen un compromiso de secreto profesional y confidencialidad en relación con los datos, la actividad bancaria y los negocios, que se enmarca en el contexto y los límites de la legislación nacional sobre empleo (contratos, estatutos de la empresa, cartas de compromiso, etc.). Ese compromiso incluye una obligación de confidencialidad que continúa una vez finalizado o modificado el contrato de empleo.

El documento de Seguridad de la Información de CACEIS es una directriz emitida a los empleados en la que se señalan las mejores prácticas utilizadas al desarrollar sus actividades de negocio, y que es totalmente coherente con los procedimientos y mejores prácticas de Crédit Agricole.

4.3 Directivas de empleo, instrucción y sesiones de formación sobre Protección de Datos (Capítulo 4 del RGPD, Sección 2, Artículo 39.1(b))

CACEIS publica y mantiene políticas y directrices de **Privacidad** y **Protección de Datos Personales**. La política de Protección de Datos y Seguridad de la Información del Grupo CACEIS exige a todas las entidades que cumplan los requisitos legales aplicables, tanto nacionales como internacionales. Además, CACEIS ha publicado un Estatuto de RR. HH. específico para proteger la información personalmente identificable de los empleados.

Para garantizar el desarrollo y conocimiento continuo de los empleados utilizamos plataformas de formación estándar del sector para entregar contenido actualizado que permita a la plantilla autogestionar su desarrollo durante su carrera profesional. Los empleados de CACEIS reciben campañas de sensibilización sobre prácticas normativas y sectoriales mediante talleres, sesiones de Preguntas y Respuestas y tecnologías informáticas.

RR. HH. gestiona y sigue el registro de formación y participación en esas sesiones.

4.4 Registros de actividades de tratamiento (Capítulo 4 del RGPD, Sección 1, Artículo 30)

CACEIS mantiene un registro de actividades de tratamiento conforme al artículo 30 del RGPD.

Los procedimientos, procesos y políticas internas (que incluyen gobierno de proyectos, recopilación de acuerdos para el lanzamiento de nuevos productos o la modificación de productos existentes, obligación de llevar a cabo estudios de riesgos en cualquier nuevo tratamiento de datos o modificación sustancial de un tratamiento) y una revisión anual obligatoria del registro de operaciones de tratamiento garantizan el mantenimiento por CACEIS de un registro exhaustivo y actualizado.

Para cada actividad de tratamiento, el registro contiene:

- La entidad y el responsable del tratamiento,
- Posibles proveedores de servicios externos,
- Lista de Datos Personales tratados,
- Identificación de transferencias de Datos Personales fuera de CACEIS (al Grupo Crédit Agricole o fuera del Grupo Crédit Agricole, dentro de la UE),
- En su caso, identificación de transferencias de Datos Personales fuera de la UE y el modo en que se garantiza su seguridad,
- Las principales medidas de Protección de Datos.

El DPO supervisa el Registro de tratamiento y el cumplimiento de la normativa. El responsable y sus representantes se encargan de asegurar que la información del Registro sea correcta y se mantenga actualizada.

4.5 Procedimientos sobre brechas de seguridad de los Datos Personales (Sección 2 del RGPD, Artículos 33 y 34)

CACEIS mantiene una postura firme en relación con cualquier infracción de la seguridad de los Datos Personales, independientemente de su naturaleza. El riesgo de brechas de seguridad de los Datos Personales se revisa y se adoptan medidas adecuadas para mitigarlo. Las infracciones se gestionan mediante políticas y directrices internas asociadas a la gestión de crisis.

Bajo la dirección del DPO de CACEIS, la documentación pertinente (política, directrices) se ha actualizado de forma coordinada con el Grupo Crédit Agricole. Se han emitido e incorporado directrices del Grupo.

Por defecto, después de detectarse un incidente relacionado con Datos Personales, y si la gravedad y el alcance del mismo lo justifican, el DPO de CACEIS, el CISO de CACEIS y el DPO del Grupo Crédit Agricole intervienen para evaluar y coordinar la gestión del incidente y las respuestas adecuadas. En caso necesario, el plan de acción se escalará y notificará a los DPO de todas las partes afectadas conforme a los acuerdos contractuales correspondientes.

En función de la gravedad del impacto sobre los derechos y libertades de las personas físicas, y de acuerdo con el artículo 33 del RGPD, el DPO de CACEIS notificará a la Autoridad de Protección de Datos aplicable al Grupo CACEIS y, si es necesario, informará a las personas afectadas. Todo ello, siempre que el contrato celebrado con sus clientes no especifique que CACEIS actuará como «encargado», en cuyo caso CACEIS no notificará directamente a los interesados, ya que la responsabilidad recaerá sobre el cliente en calidad de «responsable» (artículo 34 del RGPD).

CACEIS espera de los encargados que le notifiquen cualquier violación de la seguridad de los Datos Personales en un plazo predefinido, sin retraso injustificado, y ha tomado medidas para que así sea.

4.6 Directrices de seguridad de la información (Capítulo 2, Artículo 6; Capítulo 4, Sección 2, Artículos 24, 25; y Sección 3, Artículo 35)

La seguridad de la información y TI se rige por la Política de Seguridad de la Información de CACEIS (hay una versión disponible en el sitio de Internet de CACEIS) y se apoya en directrices específicas en la materia y procedimientos operativos estándar (standard operating procedures, SOP). Cubren los temas principales, como clasificación, funciones y responsabilidades, gestión de identidad y control de accesos, seguridad de las infraestructuras, tecnologías de usuario que incluyen sistemas de ordenador y móvil, directrices de desarrollo, copias de seguridad de los datos, etc. Se revisan periódicamente y se actualizan para tener en cuenta tecnologías y riesgos emergentes.

El pasaporte de Seguridad de la Información de CACEIS es una directriz emitida a todos los empleados en la que se señalan las mejores prácticas que deben utilizar al desarrollar sus funciones de negocio. Es totalmente coherente con los procedimientos y mejores prácticas de Crédit Agricole.

Se realizan evaluaciones de riesgos para cada nuevo requisito de tratamiento y cada modificación de un tratamiento existente. TUNES, el método de evaluación de riesgos de CACEIS, es obligatorio en cualquier nuevo tratamiento de Datos Personales para cumplir las obligaciones de «privacidad desde el diseño» y «privacidad por defecto» definidas por el RGPD. Cuando el tipo de actividad de tratamiento presenta riesgos altos para los derechos y libertados de personas físicas, se realiza una evaluación de impacto relativa a la Protección de Datos (Artículo 35 del RGPD). La metodología de esa evaluación es totalmente coherente con la de Crédit Agricole.

Los sistemas de CACEIS contienen medidas de protección desde el diseño y por defecto, algunas de las cuales se han descrito más arriba. Por defecto, no hay acceso. Conforme al artículo 25 del RGPD, algunas de las directrices de seguridad existentes se reforzarán a fin de lograr una reducción adicional de los riesgos para los derechos y libertados de las personas físicas, en particular para categorías de datos especiales.

En cuanto al desarrollo de software y sistemas, existe una política específica que rige la adquisición, el desarrollo y el mantenimiento, y que cubre estos temas:

- integración de la seguridad en los proyectos
- análisis de riesgos y requisitos de seguridad

- diseño e implementación de solución de seguridad
- comprobación, aceptación y encargo
- documentación
- mantenimiento
- integración de la seguridad en el desarrollo

También se aplican distintos procedimientos y normas:

- MESARI para evaluaciones de riesgos.
- SECAPI, un estándar del Grupo CASA que proporciona principios seguros de privacidad desde el diseño.
- SOP (Standard Operating Procedures) en el departamento de TI.

El desarrollo, la implementación y el mantenimiento de software se documentan y garantizan la existencia de procedimientos operacionales. La documentación emplea mejores prácticas y estándares como COBIT e ITIL.

4.7 Almacenamiento / tratamiento de datos fuera de Europa (Capítulo 5 del RGPD, Artículo 44)

Todos los Datos Personales se almacenan y tratan en los centros de datos de CACEIS en Europa. En algunas actividades, principalmente de administración y contabilidad de fondos, un pequeño número de tratamientos en remoto se produce desde oficinas de CACEIS en Hong Kong o en Canadá.

En algunas actividades de tratamiento, como el desarrollo y mantenimiento de software, intervienen terceros. La actividad se realiza en remoto en sistemas de centros de datos europeos y utiliza datos convertidos en anónimos.

5 Medidas técnicas de seguridad para proteger los Datos Personales

5.1 Resumen de la arquitectura técnica

Los servicios de Tecnología de la Información de CACEIS se centran sobre todo en el diseño, la creación y la gestión de sistemas de información de negocio altamente automatizados. Esos sistemas utilizan tecnologías como Mainframe, Microsoft Windows, Linux, bases de datos de Oracle y middleware basado en web.

El alojamiento de la plataforma técnica y la gestión operativa desasistida se externalizan a DXC y están ubicados en Luxemburgo. Los servicios de escritorio los gestiona y presta Crédit Agricole CAGIP y están ubicados en Francia.

5.2 Medidas de conversión de Datos Personales en anónimos y seudonimización (Capítulo 4 del RGPD, Sección 2, Artículo 32.1 (a))

La Política de Seguridad de la Información de CACEIS establece que no habrá disponibilidad de datos de producción en entornos de no producción (desarrollo, pruebas, etc.), a menos que se hayan convertido en datos totalmente anónimos. Esta norma se aplica a los Datos Personales.

5.3 Medidas de cifrado de Datos Personales (Capítulo 4 del RGPD, Sección 2, Artículo 32.1 (a))

Se aplican las medidas siguientes:

1. Los ordenadores portátiles están equipados con tecnologías de cifrado de disco duro
2. Se ha implementado el protocolo de seguridad TLS en el intercambio de mensajes de correo electrónico
3. Se utiliza el protocolo de seguridad HTTPS para asegurar el acceso a aplicaciones en Web
4. Las transferencias de datos con clientes están cifradas
5. Hay una solución disponible para el cifrado de correos electrónicos de contenido sensible

5.4 Medidas para garantizar el mantenimiento continuo de la confidencialidad (Capítulo 4 del RGPD, Sección 2, Artículo 32.1 (b))

Se aplican las medidas siguientes:

1. Los edificios y las zonas exteriores están controladas por personal de Seguridad. Hay alarmas instaladas. Las entradas están protegidas por controles técnicos de acceso (control de entrada y control por vídeo) y medidas organizativas (Recepción).
2. Identificación y revisión adecuadas de usuarios y administradores con acceso a Datos Personales.
3. Política de contraseñas implementada.
4. Bloqueo de pantalla después de un periodo de inactividad.
5. Medidas de seguridad de infraestructura de red.
6. Los USB están bloqueados por defecto.
7. Se impide el acceso a Datos Personales por personas físicas no autorizadas.
8. Medidas de seguridad del transporte físico.
9. Control de eliminación de datos almacenados y texto en ordenadores desechados.
10. Uso de una solución de impresión segura.

5.5 Medidas para garantizar la integridad continua de los datos (Capítulo 4 del RGPD, Sección 2, Artículo 32.1 (b))

Se aplican las medidas siguientes:

1. ID de usuario único.
2. Los derechos de acceso con altos privilegios están separados de la actividad de negocio y pueden vincularse con un usuario identificado.
3. La transmisión física de datos se registra y se confirma.
4. La transmisión electrónica de datos se registra y se controla.
5. Sobre la base de un análisis de riesgos, la introducción de datos en algunas aplicaciones de alto riesgo solo es posible siguiendo el principio de «4 ojos».
6. El acceso a Datos Personales se controla y se registra.
7. Se registran las actividades de administración.

5.6 Medidas para garantizar la disponibilidad continua (Capítulo 4 del RGPD, Sección 2, Artículo 32.1 (b) (c))

Se aplican las medidas siguientes:

1. SLA firmados con proveedores.
2. Instalaciones provistas de seguridad frente a robos, incendios, inundaciones, fallos de calefacción y electricidad.
3. Centros y procedimientos de copia de seguridad para recuperar la disponibilidad puntual de Datos Personales.
4. Comprobaciones de la capacidad de recuperación/restablecimiento.
5. Conceptos de Plan de Continuidad de Negocio diseñados e implementados.
6. Desarrollo de escenarios de alto riesgo específicos para cubrir incidentes tales como los relacionados con la plantilla (virus, inundación, etc.) y la tecnología (fallo generalizado de ordenadores, fallo de tecnología de centros de datos causado por error humano, fallo tecnológico o ataques cibernéticos).
7. Pruebas periódicas de planes de continuidad de negocio (BCP) y recuperación en caso de desastre (DRP) para garantizar que los sistemas y los procesos estén plenamente operativos y actualizados.

5.7 Medidas para garantizar la resiliencia continua de sistemas y servicios (Capítulo 4 del RGPD, Sección 2, Artículo 32.1 (b))

Se aplican las medidas siguientes:

1. Cada aplicación se evalúa en cuanto a riesgos y se asignan los controles y medidas de seguridad adecuados. El software de aplicaciones está sujeto a un estándar de arquitectura y desarrollo interno de SECAPI que se mantiene, comprueba y revisa antes del control de cambios que posibilita el paso a entornos de producción.
2. Se realizan pruebas de DRP y Penetración para garantizar la solidez del entorno de tratamiento de datos.
3. Análisis de seguridad periódicos de la red que identifican los equipos, el software utilizado y cualquier vulnerabilidad. Se elaboran planes de resolución de temas de alta prioridad.
4. Se utiliza una solución de inteligencia para evaluar o analizar los niveles de riesgo.
5. Instalaciones provistas de seguridad frente a robo, incendio, inundación, suministro de emergencia de calefacción y electricidad en las áreas de hardware.
6. Procedimientos de copia de seguridad para recuperar la disponibilidad puntual de Datos Personales.
7. Comprobaciones de la capacidad de recuperación/restablecimiento.

5.8 Medidas de revisión, valoración y evaluación periódica de la eficacia de las medidas técnicas y organizativas (Capítulo 4 del RGPD, Sección 2, Artículo 32.1 (d))

Se aplican las medidas siguientes:

1. Se han diseñado e implementado controles internos para comprobar la eficiencia y eficacia. Son de tres tipos: controles operacionales (nivel 1), controles consolidados (nivel 1 y 2.1) y controles de nivel 3.
2. Se realizan auditorías internas y externas.
3. Se realizan pruebas periódicas de planes de recuperación y continuidad de negocio.
4. El plan de controles del RGPD se aplica con comunicación de información mensual y trimestral.
5. Las medidas técnicas y organizativas se revisan con regularidad.

6 Detalle de medidas técnicas y organizativas de protección específicas

6.1 Medidas de seguridad físicas

6.1.1 Espacio de oficinas de CACEIS

Los edificios y el espacio de oficinas de CACEIS están protegidos 24/7 mediante vídeo vigilancia, detección de intrusiones y rondas nocturnas del personal de Seguridad.

La entrada al edificio requiere autorización previa y un pase de acceso. Las tarjetas de entrada permiten acceso y circulación restringida dentro de los edificios. Todos los empleados reciben una tarjeta. Las visitas reciben un pase de acceso temporal una vez confirmada su identidad y autorizadas por un empleado de CACEIS.

6.1.2 Instalaciones de tratamiento de centros de datos

Las instalaciones de tratamiento de CACEIS se someten a un control riguroso. CACEIS aplica procedimientos formales para el acceso físico a los centros de datos. Los centros de datos se encuentran en instalaciones que requieren acceso con tarjeta electrónica y prueba de identidad. Las listas de acceso se mantienen y se revisan con frecuencia. Los centros de datos de CACEIS requieren operaciones de seguridad *in situ* responsables de controlar y acceder a todas las funciones de seguridad del centro de datos físicos 24 horas al día, 7 días a la semana.

6.2 Gestión y control de autentificaciones

6.2.1 Identificación de usuarios

Se han definido políticas y procedimientos para garantizar la identificación adecuada de usuarios y administradores que acceden a Datos Personales.

CACEIS utiliza un sistema de gestión de identidad y acceso (IAM) centralizado. El sistema se encarga de asignar identidades de usuario, que son únicas para todos los empleados que desean acceder y utilizar cualquier elemento del Sistema de Información de CACEIS. El acceso solo puede producirse a través de un terminal de CACEIS conectado a la red. Se exige una identidad de usuario personal y, como mínimo, una contraseña. Algunas aplicaciones específicas pueden requerir identificación de dos factores.

La Política de Seguridad de la Información de CACES prevé la segregación y distinción de privilegios de las actividades de negocio regulares, por lo que se asigna un ID de usuario específico a las personas designadas. Los privilegios incluyen tareas especiales de administración de sistemas y aplicaciones.

Para garantizar que el ID de usuario siga siendo válido, se llevan a cabo campañas regulares de recertificación y conciliación. Así, los ID que no corresponden a ningún usuario o no son válidos se dan de baja y se eliminan inmediatamente (por ejemplo, desactivación puntual de ID de usuario de empleados que dejan la empresa).

6.2.2 Autentificación

Los controles del sistema de IAM acceden a los sistemas de producción siguiendo unas normas definidas. CACEIS utiliza tecnologías como LDAP, Kerberos y un sistema interno que emplea claves RSA (u otras claves lógicas) que aportan mecanismos de autenticación seguros y flexibles. Esos mecanismos se diseñan de modo que solo concedan derechos de acceso aprobados. Además, la autentificación de sistemas técnicos se controla mediante una plataforma especializada.

La autentificación en CACEIS generalmente requiere una contraseña personal secreta, aunque en algunos casos se emplea autentificación de dos factores mediante tarjetas con chip y token de dispositivos. Las normas y estándares de gestión de contraseñas se rigen por la Política de Seguridad de la Información. Esas normas incluyen restricciones del tipo de reutilización de la contraseña, seguridad de la contraseña y duración de la contraseña. Las normas sobre contraseñas que se indican a continuación se implementan y controlan en el directorio activo de Windows:

- Al menos 12 caracteres según define la Política
- Duración máxima de la contraseña: 90 días
- Bloqueo de cuenta: después de 5 intentos de acceso

6.2.3 Acceso a sistemas de tratamiento de datos

Todos los sistemas de tratamiento de datos (ordenadores de mesa, servidores, etc.) están conectados por una red interna de CACEIS. El acceso a los sistemas de tratamiento solo es posible desde la red de CACEIS.

Los estándares de diseño de la red de CACEIS se basan en los estándares de Crédit Agricole, que siempre están entre los mejores del mercado. La red de

CACEIS está separada física y lógicamente (propósito, riesgo, tecnología) e incorpora tecnología de seguridad que controla, detecta y evita intrusiones (cortafuegos, IDS, IPS y WAF). La redundancia de sistemas y tolerancia de fallos es parte de la arquitectura de red para garantizar que el acceso al tratamiento de datos cumpla los requisitos de los SLA de Negocio.

La configuración de sistemas sigue un principio de «denegación por defecto», lo que significa que las configuraciones de router y cortafuegos se han diseñado para restringir el tráfico de entrada y salida y prohibir cualquier acción que no esté explícitamente permitida. Esos ajustes deniegan por defecto y desde el diseño todos los flujos y comunicaciones no autorizados. Existe un Comité de Aceptación de Cambios (CAB) dedicado a flujos, protocolos y servicios de red. Se aplican controles que monitorizan el cumplimiento de nuestras políticas técnicas.

La monitorización se realiza en tiempo real mediante el monitor CERT de Crédit Agricole 24x7 y el Centro de Operaciones de Seguridad (SOC) de CACEIS. En caso de advertencia de irregularidades, el Director de Seguridad de Tecnología de la Información (ITSO) y el SOC inician respuestas según procedimientos acordados.

6.3 Control de accesos por gestión de autorizaciones

La asignación de accesos se formaliza y se rige por la Política de Control de Accesos de CACEIS (parte de la Política de Seguridad de la Información). El procedimiento operativo estándar (Standard Operating Procedure o SOP) describe el funcionamiento del proceso de gestión, incluida la autorización y atribución de «Acceso».

El acceso se permite solo si existe «necesidad de conocer». La autorización de acceso se realiza mediante flujo de trabajo y se requieren la del responsable y la del propietario de la aplicación, aunque en ocasiones puede exigirse aprobación adicional. La asignación de derechos específicos la gestiona la aplicación y se atribuye una vez autorizada por los responsables.

Los flujos de trabajo de gestión de autorizaciones se realizan dentro del sistema de IAM, donde los derechos se asignan y atribuyen utilizando perfiles de negocio predefinidos. Solo el gestor de perfiles de Negocio puede solicitar un cambio de perfiles de Negocio. Se requiere la aprobación del gestor de perfiles de Negocio, el propietario de la aplicación de negocio y el departamento de Riesgos para asignar un nuevo acceso a un Perfil de Negocio.

El sistema de IAM realiza revocaciones automáticamente. Adicionalmente, el responsable y el propietario de la aplicación llevan a cabo campañas regulares de recertificación para confirmar que la necesidad sigue siendo pertinente.

Los perfiles de negocio y los derechos de acceso asociados se definen para reforzar los principios de «necesidad de conocer», «privilegio menor» y «segregación de funciones». Se llevan a cabo revisiones con el departamento de Riesgos para comprobar posibles combinaciones incorrectas de derechos de acceso.

6.4 Protección de Datos

La Política de Seguridad de la Información de CACEIS define las normas de utilización de medios y uso de los datos. El uso de medios digitales no está permitido. Los puertos USB se bloquean por defecto y las personas físicas pueden solicitar la activación temporal en condiciones estrictas. Para almacenar datos solo pueden utilizarse medios externos aprobados por CACEIS.

6.5 Control de divulgación

6.5.1 Transporte de información y transmisión de datos electrónica

La Política de Seguridad de la Información y los SOP definen medidas de transporte seguras para proteger contra acceso no autorizado y uso indebido.

El transporte físico de información, y en particular de información confidencial y sensible, está restringido. CACEIS utiliza servicios de transporte seguros específicos.

Transferencias electrónicas: CACEIS transfiere la mayor parte de la información por vía electrónica, con conexiones de Internet seguras y transferencia segura de ficheros. Todos los remitentes que intervienen en la transmisión se identifican mediante firma electrónica. Las transmisión de Datos Personales a través de redes externas se realiza utilizando criptografía y protocolos seguros, como TLS, SSH, HTTPS, SFTP e IPSEC. Todas las transmisiones electrónicas de datos se registran y monitorizan.

Se implementan medidas de seguridad para controlar y seguir el flujo de datos de extremo a extremo y en redes externas. Esas medidas incluyen tecnologías de cortafuegos, IDS, IPS y WAF. Un Comité de Aceptación de Cambios se encarga de revisar y planificar flujos, protocolos y servicios de red.

6.5.2 Seguridad de los datos

La Política de Seguridad de la Información y los SOP de CACEIS definen nuestro enfoque para la clasificación de activos, incluidos activos de aplicaciones y activos de datos. La mayoría de los activos se inventarían y clasifican en función de evaluaciones de riesgos que incluyen la evaluación de los axiomas de Seguridad de la información, Confidencialidad, Integridad y Disponibilidad. Este enfoque incluye la clasificación de Datos Personales. El proceso de clasificación de activos es un paso definitivo para garantizar que las medidas de seguridad y los controles se eligen de acuerdo con el grado de criticalidad del activo.

6.5.3 Resiliencia de sistemas y pruebas de penetración

La resiliencia y la solidez de los sistemas son aspectos importantes de los servicios prestados por CACEIS. Para garantizar que cumplan nuestros estándares de Negocio, programamos y realizamos numerosas pruebas de tratamiento de datos a lo largo del año. Esas pruebas incluyen Continuidad del Negocio (BCM) y Recuperación en caso de Desastre (DRP), así como pruebas de Penetración (PEN TEST). El control de cambios es una parte del proceso que asegura la correcta realización de las pruebas antes de entregar los cambios a entornos de producción.

DRP incluye garantizar que los planes se documentan, actualizan y comprueban para una serie de escenarios de desastre definidos. La recuperación de datos incluye nuestra capacidad de restablecer información. Siguiendo la Política de Copia de Seguridad que define las normas y prácticas de copia de seguridad y recuperación de información de forma segura, realizamos pruebas de restablecimiento periódicas.

CACEIS realiza PEN TESTS con carácter regular en nuestra infraestructura crítica para comprobar la seguridad, solidez, resiliencia, rendimiento e impermeabilidad de los sistemas de seguridad desplegados. Además, CACEIS dispone de una herramienta de inteligencia de amenazas que analiza constantemente el estado de su red y su sistema para detectar potenciales violaciones de seguridad.

6.5.4 Ordenadores portátiles y dispositivos móviles

Las medidas de protección de ordenadores portátiles y dispositivos móviles están definidas en la Política de Seguridad de la Información y descritas en las normas y SOP de Seguridad de la Información. El uso de dispositivos móviles (portátiles, smartphones, tablets, etc.) está sujeto a normas particulares. Los usuarios acuerdan respetar estas normas mediante la firma de un documento específico cuando se entrega el dispositivo en cuestión.

La información de los portátiles está protegida por tecnologías de cifrado de disco duro y otras medidas de seguridad gestionadas por una solución MDM (gestión de dispositivos móviles). En caso de robo o pérdida, los datos almacenados en los dispositivos móviles pueden ser eliminados en remoto por CACEIS.

6.5.5 Eliminación de ordenadores utilizados y medios de almacenamiento de datos

CACEIS ha definido e implementado procedimientos adecuados (SOP) para el transporte y la eliminación segura de activos de Tecnología de Información y Comunicación, y los medios de almacenamiento de datos se desechan según la norma de destrucción EN 66399. CACEIS también ha definido e implementado procedimientos adecuados (SOP) para el borrado seguro de datos de los medios de almacenamiento.

6.6 Control de disponibilidad

6.6.1 Instalaciones de seguridad en áreas de hardware (salas de servidores, centro de datos)

Los sistemas de información se alojan en centros de datos de Nivel IV que cumplen con las condiciones de protección y seguridad más exigentes. Los centros de datos de Nivel IV están protegidos contra interrupciones y pérdidas de electricidad y situados en áreas no expuestas a inundaciones o actividad sísmica. Para cumplir esos criterios estrictos, tanto la electricidad como las telecomunicaciones se aseguran mediante numerosas entradas.

6.6.2 Copias de seguridad de los datos

La gestión de copias de seguridad y recuperación de datos se realiza de este modo:

- Se han desarrollado SOP para garantizar que la copia y recuperación de los sistemas se ajusten a requisitos de negocio predefinidos.
- Las copias se realizan diariamente y se reflejan en las instalaciones secundarias.
- Los procedimientos de copia y recuperación se comprueban al menos una vez al año para garantizar que siguen estando plenamente operativos y actualizados.

6.6.3 Precauciones contra desastres

CACEIS tiene en cuenta una serie de escenarios de crisis graves predefinidos de Crédit Agricole y ha puesto en marcha SOP para responder a esos escenarios en caso de desastre.

En cuanto a nuestros centros de datos, cuentan con tolerancia de fallos y son capaces de reabsorber con autonomía una interrupción de sus centros de datos colaboradores y garantizar la continuidad del servicio. Nuestros planes de gestión de crisis aseguran la gestión de la reconexión.

CACEIS realiza varias pruebas cada año para comprobar que las medidas técnicas y organizativas en caso de desastre están operativas. Esas pruebas se realizan bajo el control de la línea de Negocio, que valida sus resultados.

6.7 Huella de auditoría en la instrucción, modificación y borrado de Datos Personales

El acceso a datos (alta, cambios, eliminación) mediante aplicaciones corporativas se registra en las propias aplicaciones. Las aplicaciones disponen de alguna solución de seguimiento realizada por Negocio.

El acceso a Datos Personales por usuarios individuales también se registra y se controla. Así, los casos de acceso a Datos Personales almacenados en aplicaciones se someten a seguimiento y registro (leer, escribir, actualizar, etc.).

Las actividades de administración (por ejemplo, registro de intentos de acceso, excepciones, fallos, etc.) se registran siempre y los registros de eventos se revisan con regularidad. Se aplican medidas específicas cuando resulta adecuado para mitigar cualquier riesgo relacionado con un proceso. El control utiliza el resultado de la monitorización y realiza medidas correctivas para solucionar cualquier incumplimiento de las normas corporativas. El Director de Seguridad de TI de CACEIS es responsable de iniciar el proceso específico.

Para controlar datos no estructurados, CACEIS emplea la solución Varonis, que controla derechos de acceso con directorios compartidos y acceso a esos datos.

6.8 Eliminación de datos y restricciones de tratamiento

La Política de conservación de datos de CACEIS es mantener los datos por un periodo no superior al exigido por ley, normativa o contrato.

6.9 Control de subcontratación

Los servicios correspondientes a criterios predefinidos se someten a un seguimiento acorde con las Directrices de Crédit Agricole sobre servicios esenciales subcontratados predefinidas (OES; PSEE en francés). Se complementan con una Política de externalización de TI específica de CACEIS basada en ISO 37500. Todos los subcontratistas están sujetos a las cláusulas de confidencialidad de CACEIS y a la Política de Seguridad de la Información de CACEIS.

Todos los subcontratistas son evaluados anualmente mediante un cuestionario de cumplimiento o, en algunos casos, con auditorías.