Evolución de la supervisión y la gobernanza de protección de datos frente a los nuevos retos que suponen la IA y las amenazas a la seguridad de la información.

Enero 2026

CaixaBank

Índice

DESCRIPCIÓN DEL CONTEXTO ORGANIZATIVO: Características de la entidad en la que el DPD presta sus servicios, funciones desarrolladas y principales retos de cumplimiento identificados

Pablo Diaz Ortiz, es Delegado de Protección de Datos (en adelante, "**DPD**") de CaixaBank, S.A. Nombrado en 2016 por el Comité de Dirección de la Entidad como delegado de protección de datos corporativo (esto es, de todo el grupo de empresas) de acuerdo con lo dispuesto en la Política Corporativa de Privacidad y Protección de Datos de CaixaBank.

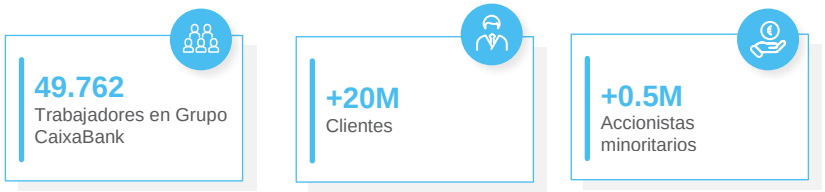
Desde entonces, ejerce este cargo tanto en CaixaBank (entidad de crédito matriz del grupo) como en las sociedades de su grupo empresarial cuyas sedes se encuentran en España) y se detallan en la figura que se muestra a continuación.

Las filiales situadas fuera de España (en gris en la figura), cuentan con delegados de protección de datos propios, que dependen funcionalmente del Delegado de Protección de Datos de CaixaBank, dada su condición de DPD Corporativo.

1.	CaixaBank operational services	8. BuildingCenter	15. Nuevo MicroBANK	22.BPI suisse
2.	CaixaBank Tech	9. Bankia Habitat	16. CBK Titulización	23.OpenWealth
3.	CaixaBank facilities Management	10. Living Center	17.BPI vida e Pensoes	
4.	CaixaBank Payments&Consumer	11. VidaCaixa	18. BPI Gestao de activos	
5.	Facilitea Selectplace	12. VidaCaixa Mediacion	19. CaixaBank AM Luxembourg	
6.	Telefonica Consumer Finance	13. CaixaBank AM	20. Banco BPI	
7.	CaixaBank Equipment Finance	14. Imaginersgen	21. CaixaBank Wealth management Luxembourg	

Por la composición del grupo empresarial respecto del que el DPD presta sus funciones, su actividad se centra en actividades financieras con un modelo de banca universal, aseguradoras, de pagos y crédito al consumo, de inversión financiera e inmobiliarias que ofrecen una propuesta de valor de productos y servicios adaptada para cada segmento, asumiendo la innovación como un reto estratégico y un rasgo diferencial de su cultura.

En cuanto a dimensiones en las que desarrolla su función hay que tener en cuenta que el grupo CaixaBank cuenta con:



En este contexto, los retos estructurales del DPD, son:

1. **Tratamiento masivo de datos financieros y sensibles (en el ámbito asegurador)**: esta circunstancia impacta de manera relevante en el diseño e implantación de las estructuras y procedimientos necesarios para el cumplimiento de los principios de protección de datos y, de manera muy particular, en la privacidad por defecto y desde el diseño y su integración desde el desarrollo tecnológico, en el asesoramiento en las evaluaciones de impacto y el seguimiento de sus planes de acción o a la gestión de incidentes con

afectación datos. También, en la atención de los derechos de los interesados (el 2025, se ha cerrado con la atención de 48.633 ejercicios de derechos en CaixaBank y 55.835 en todo el grupo de empresas).

2. **Implantación de medidas de *"Privacy by Design"* en un ecosistema tecnológico caracterizado por un *core* histórico ("legacy"), con alta complejidad y heterogeneidad:** Sistemas cuyos primeros diseños y funcionales fueron implementados hace décadas y que soportan procesos críticos, cuya evolución o actualización implica intervenciones complejas que comportan el análisis de riesgos muy elevados y necesidades de asesoramiento y supervisión muy relevantes por parte del DPD.

3. **Entorno altamente regulado y multijurisdiccional**: Necesidad de profunda especialización del DPD para la conciliación de las diferentes obligaciones establecidas con carácter adicional a la normativa de protección datos (tales como prevención del blanqueo de capitales, normativa de la CNMV, Banco de España, EBA, PSD2, MiFID II, etc.)

4. **Gestión de cadenas de suministro de alta complejidad:** Gran volumen y heterogeneidad de los proveedores necesarios para el funcionamiento del Grupo, incluyendo proveedores críticos para funciones catalogadas como esenciales e infraestructuras críticas.

5. **Gobernanza de la privacidad en estructuras societarias complejas**: Gran complejidad en el despliegue, mantenimiento y armonización de criterios corporativos tanto en CaixaBank como en el resto de las sociedades del grupo. Y, ello como se puede ver en el grafico anterior, tanto por sus magnitudes (entidades muy relevantes a nivel español) como por la heterogeneidad e idiosincrasia de cada uno de los negocios (negocio asegurador, inmobiliario, financiero).

Adicionalmente, como retos especialmente relevantes en el periodo más reciente hay que señalar, necesariamente, dos:

1) El **impacto de la inteligencia artificial en general y, en particular, de la inteligencia artificial generativa** (en adelante, "IA"), lo que pasa por relevantes necesidades de formación y actualización del DPD y de sus equipos para el correcto entendimiento de estas nuevas y revolucionarias tecnologías. Solo así el DPD y sus equipos pueden ser capaces de detectar, analizar, gestionar y, en su caso, mitigar de los riesgos que, para los derechos fundamentales de los titulares de los datos y, en especial, para el derecho fundamental a la protección de datos, pueden ocasionar.

2) El reto de **seguridad, ciberseguridad y resiliencia en entornos cada vez más digitales**, a los que, sin duda, las tecnologías de inteligencia artificial y sus capacidades añaden cada día más complejidad y sofisticación y, por tanto, mayores riesgos.

OBJETIVOS DEL PROYECTO: metas perseguidas en términos de cumplimiento, cultura de la privacidad o innovación

De acuerdo con el contexto expuesto en el apartado anterior, el **conjunto de actividades** llevadas a cabo por el DPD y su equipo **se encuadran en la promoción e implantación efectiva del cumplimiento normativo** en materia de protección de datos.

En concreto, se centran en abordar y mejorar la gestión de los **riesgos que suponen tanto la IA, como el contexto actual en relación con la seguridad de los datos personales y las amenazas a las que están expuestos**.

Este entorno ha comportado la evolución de los **procesos, procedimientos y metodologías utilizadas para el análisis de los riesgos de la IA para los derechos fundamentales, la mejora en cuanto en la gestión de los incidentes que afectan a datos personales en todo su ciclo de vida y la evolución del modelo de supervisión que opera el DPD**.

Con ello, este DPD presenta al premio de la AEPD las siguientes actuaciones llevadas a cabo, tal y como se irá detallando a lo largo del documento, en el periodo señalado de 16 de octubre de 2024 a el 31 de enero de 2026.

A. Gestión del riesgo de privacidad en el contexto del desarrollo o uso de sistemas de Inteligencia Artificial:

En esta línea de actuación, el DPD se ha centrado en evolucionar el proceso y metodología preexistente en el Grupo para alcanzar:

- **i)** Participación en el análisis de las iniciativas que suponen el desarrollo, o uso, de sistemas de IA desde la concepción del caso de uso (momento muy inicial en el cual se dispone únicamente de una idea);
- **ii)** Identificar de manera muy temprana el tratamiento de datos en el que se ubicará la IA,
- **iii)** Realización *ex ante* de la gestión de riesgos o evaluación de impacto correspondiente; y
- **iv)** Planificación de otros impactos en el marco de cumplimiento (deber información, ejercicio de derechos, medidas técnicas o de seguridad, etc.).

Todo ello, con el objetivo de ser capaz de gestionar, desde la propia concepción de las iniciativas o casos de uso, los riesgos de la IA para los derechos fundamentales, en general, y para el derecho a la protección de datos en particular.

B. Evolución del registro, gestión y seguimiento de las brechas de datos personales y sus planes de acción

En relación con el contexto actual de crecimiento significativo del número e intensidad de los ataques globales, con especial protagonismo del fraude, el *ransomware* o los ataques a las infraestructuras críticas, el DPD durante el 2025 ha tenido como objetivo robustecer el proceso corporativo de gestión de brechas de datos personales, con el objetivo de mejorar el cumplimiento normativo garantizando:

- **i)** La generación de la documentación exhaustiva requerida por el RGPD,
- **ii)** La valoración objetiva del impacto sobre los derechos y libertades de los interesados de las brechas de datos personales,
- **iii)** El establecimiento de un sistema de mejora continua, apoyado en planes de acción verificables y centralizados y
- **iv)** La utilización de una herramienta de soporte única que ofrece un enfoque adaptable y, por tanto, al que pueden sumarse todas las empresas del grupo.

C. Evolución del modelo de supervisión

El modelo de supervisión de (enmarcado en un sistema de tres líneas de defensa, encuadrado en la primera) tiene como objetivo establecer un marco de control corporativo, integral y basado en riesgo que permita evaluar de forma homogénea, objetiva y defendible el cumplimiento de la normativa de protección de datos en todas las entidades del Grupo.

Para ello integra elementos como un radar normativo, un *pre assessment* de riesgo, un modelo de atributos y la monitorización mediante indicadores, orientando la supervisión hacia los ámbitos de mayor exposición a riesgo, asegurando una visión dinámica y actualizada del riesgo.

El modelo busca, además, reforzar la cultura de cumplimiento y la responsabilidad proactiva, mejorar la trazabilidad y la eficiencia en la asignación de recursos, y ofrecer un enfoque adaptable y replicable en distintas organizaciones, consolidando una supervisión más efectiva dentro de la primera línea de defensa.

ACCIONES DESARROLLADAS: actividades, procesos, herramientas, programas formativos, campañas o sistema de gestión implementados

A. Gestión del riesgo de privacidad en el contexto del desarrollo o uso de sistemas de Inteligencia Artificial:

Para al alcanzar las metas señaladas en el apartado anterior en relación con la gestión del riesgo de privacidad, cuando están involucrados sistema de IA, durante el 2025 se han realizado diversas actuaciones que han permitido evolucionar el análisis de los riesgos que pueden provocar estas tecnologías. En concreto:

i. **Incorporación del DPD al proceso creado en la Entidad para la Gobernanza Unificada de Iniciativas de IA** (“**GUIA”**).

Este proceso, constituye el canal único de identificación y evaluación inicial de todas las iniciativas de uso de IA en la entidad y su objetivo, además de la identificación y registro de todas las iniciativas que se plantean con IA, es el análisis y la depuración técnica y de cumplimiento legal de estas, además de guiar al usuario en la ejecución de su caso de uso asegurando la coherencia, el orden y el cumplimiento.

Es en este momento tan inicial, donde se exponen casos de uso, y que es anterior, incluso, a la definición técnica del proyecto, ya se determina por parte del DPD:

a) **La implicación o no del uso de datos personales**

b) **Implicación en el Registro de actividades de tratamiento (RAT):** el DPD determina el tratamiento de los datos en el cual la IA tendrá cabida como activo y si el mismo ya se encuentra en el RAT o debe darse de alta.

c) **Implicación en análisis de riesgos o, en su caso, evaluaciones de impacto en protección de datos**: también aquí el DPD determina las acciones a adoptar para actualizar o iniciar el correspondiente análisis de riesgos o evaluación de impacto.

ii. **Evolución de las estructuras de gobierno de la protección de datos y actualización de procedimientos, políticas y otras normas internas**:

En la gobernanza de la protección de datos diseñada por el DPD en el grupo CaixaBank se distinguen roles y responsabilidades que le permiten asesorar y supervisar, mientras que otros órganos se ocupan de decidir sobre los

fines, medios y los riesgos a asumir derivados de los tratamientos. En este sentido existen:

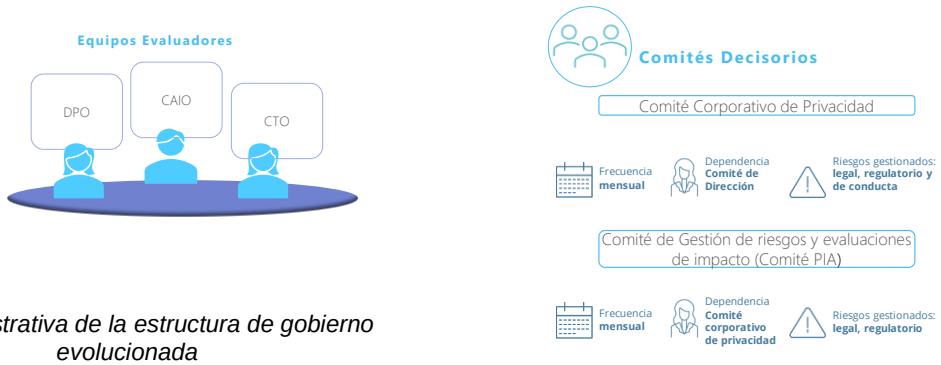


Imagen ilustrativa de la estructura de gobierno evolucionada

Durante el 2025, ha sido necesario adaptar estas estas estructuras, junto con sus políticas, reglamentos o metodologías para garantizar el gobierno de los riesgos de la IA en materia de protección de datos y derechos fundamentales:

a. **Comité Corporativo de Privacidad (Comité de Privacidad)**: se modifica la composición de este comité (órgano decisorio superior en materia de protección de datos que depende directamente del Comité de Dirección), para incorporar la mismo al responsable de Inteligencia Artificial (CAIO).

   Con esta incorporación se alcanza la necesaria coordinación del DPD (visión legal y normativa), del CAIO (visión técnica y estratégica de la IA), del CISO (visión técnica de seguridad) y del CDO (visión calidad del dato) con el objetivo de asegurar el cumplimiento normativo. Ejecutado en julio de 2025.

b. **Comité de Gestión de Riesgos y Evaluaciones de Impacto (Comité PIA)**: se modifica su Reglamento para incorporar entre sus competencias la evaluación del uso ético de los datos y de los componentes de IA. Ejecutado en diciembre de 2024.

c. **Política Corporativa de Privacidad**: texto principal que establece los compromisos en el gobierno de la protección de datos y cuya responsabilidad es del Consejo de Administración. Se actualiza para, entre otros aspectos, incorporar las referencias necesarias para la gestión de los riesgos de la IA y la mejora del *reporting* del DPD al Comité de Dirección y a los órganos de gobierno. Ejecutado en diciembre de 2024.

iii. **Consolidación de los análisis de los riesgos de la IA en la gestión de riesgos y evaluaciones de impacto**:

Con las acciones anteriores, y el modelo de gobierno y gestión de los riesgos de la IA basado en la metodología interna existente, se consolida un sistema en virtud del cual se evalúan los riesgos de la IA de siguiendo el siguiente gráfico, que permite que se desencadenen los flujos para asegurar el cumplimiento normativo:

Gestión de riesgos de privacidad en la IA

Se destaca especialmente:

i. **Análisis del cumplimiento del componente de IA**: aspecto que se realiza a través de los objetivos de control y los controles (144) propuestos por la AEPD en su guía Requisitos para auditorias de tratamientos que incluyen componentes de IA. Dirigido y liderado por el DPD pero ejecutado por los 3 equipos evaluadores: DPD, CISO y CAIO.

ii. **Análisis de los daños y perjuicios del tratamiento para los interesados**: liderado por el letrado que asesora la evaluación de impacto y en el que, si existen componentes de IA, se analizan en particular los riesgos que pueden derivarse del mismo. Este análisis se inspira en los criterios establecidos por la AEPD en su Guía Gestión del riesgos y evaluaciones de impacto, de acuerdo con los gráficos que se muestran a continuación:

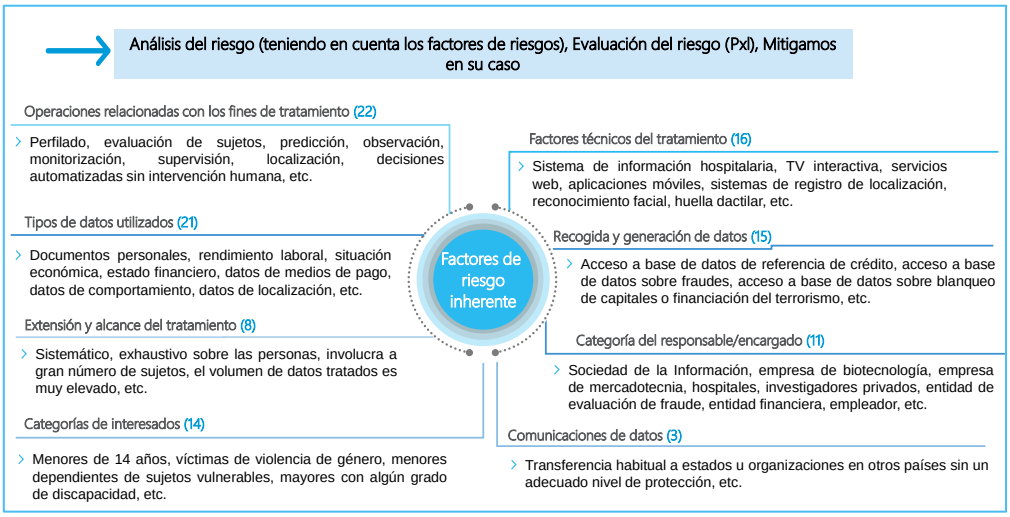


Imagen ilustrativa de los factores de riesgo

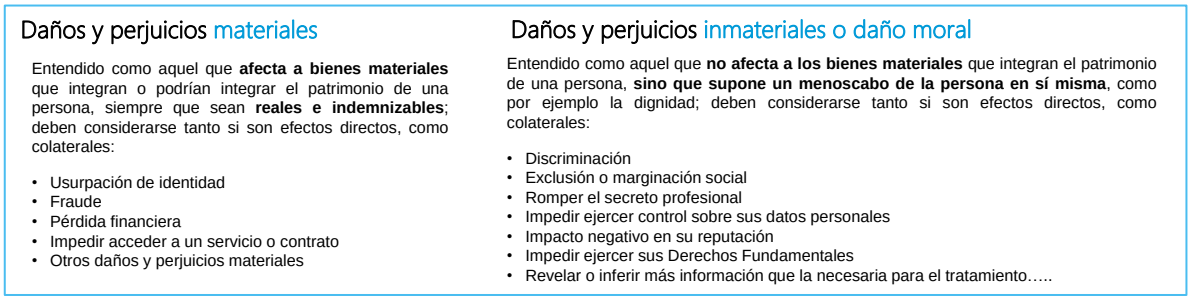


Imagen ilustrativa de ejemplos de daños y perjuicios

iii. **Gestión de los riesgos para los derechos fundamentales**: llegados a este punto el equipo evaluador liderado por el DPD y el letrado identifican los derechos fundamentales que podrían verse afectados por el tratamiento en su conjunto, con especial atención a si están involucrados elementos de IA. La lista de derechos fundamentales se nutre tanto de la Carta de derechos fundamentales de la UE como de la CE. Para cada uno de los derechos impactos se analizan los riesgos y se gestionan a los efectos de mitigarlos con los correspondientes planes de acción.

B. Evolución del registro, gestión y seguimiento de las brechas de datos personales y sus planes de acción

En relación con la mejora del proceso de registro, gestión y seguimiento de las brechas de datos personales y sus planes de acción, las acciones llevadas a cabo se han centrado en la mejora de los procesos incluyendo la implementación de una herramienta centralizada y corporativa que permite el pleno control y seguimiento de todos los sucesos.

Dimensiones de las brechas de datos personales

1. Introducción al modelo corporativo de gestión de brechas impulsado por el DPD

El DPD ha impulsado un modelo de gestión de brechas que va más allá de un simple procedimiento y se convierte en un sistema **preventivo, dinámico y transversal**. Integra en un único circuito la detección temprana, el análisis técnico-jurídico, la mitigación inmediata, la valoración del riesgo y las decisiones sobre notificación y comunicación, junto con un **mecanismo sólido de seguimiento de los planes de acción**.

2. Fase de detección y registro: activación inmediata del circuito

Cualquier empleado puede, y debe, comunicar un indicio de brecha, proceda de observación directa, de avisos clientes, empleados, proveedores o terceros, o de monitorización interna.

El registro se realiza **exclusivamente a través de la herramienta HighQ**, que actúa como **punto único corporativo** y garantiza la trazabilidad desde el primer momento y la activación automática de los equipos especializados.

3. Análisis preliminar y calificación de los sucesos

Tras la comunicación, intervienen de forma coordinada Seguridad de la Información, AJIP y el DPD.

Se determina si existe brecha y su naturaleza (confidencialidad, integridad o disponibilidad).
Esta fase incluye **acciones de contención inmediatas** y la calificación del suceso según las categorías internas (brecha, incidente, suceso sin afectación, no suceso o suceso de tercero).

4. Valoración del riesgo y adopción de decisiones sobre notificación y comunicación

La valoración del riesgo se realiza con una metodología cuantitativa avanzada, inspirada en las recomendaciones de ENISA, la AEPD y el EDPB.

Se analiza qué dimensiones de seguridad se ven afectadas y se aplican variables ponderadas (tipo de datos, afectación, volumen, exposición, consecuencias, etc.).

El resultado orienta las decisiones sobre si es necesario notificar a la autoridad supervisora o a los interesados. Los hallazgos se recogen en informes jurídicos preliminares o finales, actualizándose durante el proceso, si la información evoluciona.

La evaluación se integra en el marco global de riesgos del Grupo para reforzar la privacidad desde el diseño.

5. Gestión integral del incidente y medidas de mitigación inmediatas

Se aplican medidas para contener y corregir la brecha: bloqueo de accesos, recuperación o eliminación de datos, corrección de fallos técnicos, etc.

Cada acción se documenta exhaustivamente para garantizar una trazabilidad completa de la respuesta.

6. Seguimiento de los planes de acción: hito innovador clave del modelo

Cada brecha genera un plan de acción específico, con medidas preventivas y correctoras, responsables, plazos y evidencias.

El seguimiento es continuo y se realiza un control reforzado para garantizar su correcta ejecución.

Una vez implementado y verificado, se cierra mediante un **Informe Jurídico Final**, que alimenta el reporting periódico a comités y órganos de gobierno, impulsando la mejora continua del sistema de privacidad.

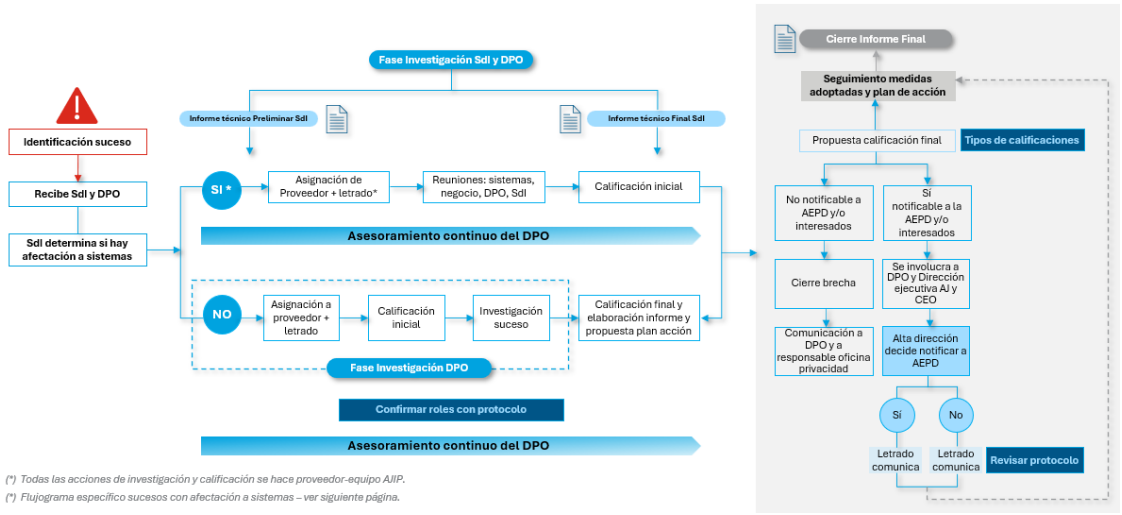


Imagen ilustrativa del flujo de gestión

C. Evolución del modelo de supervisión

En relación con la tercera línea de actuación llevada a cabo por el DPD, relativa al modelo de supervisión, cabe destacar que durante el ejercicio 2025 la función de supervisión consolidó la implementación del modelo que se inició en 2023, estructurado como un **marco de control corporativo,** que integra actividades, procesos, herramientas y gobernanza para garantizar una supervisión basada en riesgo, homogénea y defendible.

Este modelo se articula sobre una metodología que construye un **marco de control integral** compuesto por cuatro elementos principales: (1) radar normativo, (2) *pre assessment* de riesgo, (3) modelo de atributos e (4) indicadores asociados al SGPD.

A través de este marco, la labor de supervisión se desarrolla en base a un proceso estructurado aprobado por los órganos de gobierno de la Entidad:

La metodología se revisa periódicamente con la finalidad de asegurar que el marco se encuentra actualizado y plenamente alineado con la exposición real al riesgo.

El despliegue operativo del Plan de Supervisión en el periodo 2024-2025 ha supuesto la ejecución de distintos ejercicios de supervisión en CaixaBank, S.A.:

- **Ejercicios periódicos**, que abarcaron los dominios del marco de riesgos de privacidad tales como Gobierno y Cumplimiento, Medidas de Seguridad, Accountability, Ejercicio de Derechos, Relación con Supervisores o Evaluaciones de Impacto.
- **Ejercicios extraordinarios**, en los que se revisó por ejemplo el cumplimiento de la Guía de Cookies de la AEPD.
- **Ejercicios recurrentes**, en los que se verificó el cumplimiento del principio de transparencia en los textos informativos alojados en los distintos canales.

CARÁCTER INNOVADOR: uso de tecnologías o metodologías novedosas, mejoras en gobernanza o gestión interna**.**

A. Gestión del riesgo de privacidad en el contexto del desarrollo o uso de sistemas de Inteligencia Artificial:

En cuanto al carácter innovador de las actividades desplegadas en relación con la gestión de los riesgos de la IA en los tratamientos de datos se destacan las siguientes:

i. **Anticipación y participación del DPD desde la concepción de la idea:** el análisis de los riesgos de privacidad comienza desde la fase inicial del proceso GUIA, incluso antes de la definición técnica completa del caso de uso, lo que permite una aproximación preventiva permite identificar tempranamente si la iniciativa utiliza datos personales o si puede generar impactos relevantes sobre los derechos fundamentales de los interesados (habitualmente clientes o empleados de la Entidad), activando desde el primer momento los circuitos de asesoramiento del DPD y las salvaguardas necesarias. De esta manera, la protección de datos por defecto y desde el diseño se garantiza.

ii. **Governance "virtuoso":** los procesos y procedimientos, así como las herramientas que los acompañan guían y desencadenan las acciones que

permiten asegurar el cumplimiento normativo de las iniciativas y la protección de los derechos de los interesados.

B. Evolución del registro, gestión y seguimiento de las brechas de datos personales y sus planes de acción

En relación con el carácter innovador en este apartado, cabe destacar la implantación de la herramienta de gestión HighQ que constituye un proyecto innovador impulsado directamente por el Delegado de Protección de Datos (DPD), quien ha liderado la transformación del proceso de gestión de brechas en un sistema digital, centralizado y plenamente alineado con la responsabilidad proactiva del RGPD y con el Protocolo Corporativo de Brechas del Grupo.

Con este proyecto, HighQ se ha convertido en el punto único corporativo para gestionar todo el ciclo de vida de un incidente: desde la detección y el análisis preliminar hasta la notificación, documentación completa y seguimiento del cierre.

HighQ ha introducido un modelo organizativo basado en automatización, trazabilidad y expediente único, integrando en un mismo entorno la información técnica, jurídica, las comunicaciones internas y los requisitos de documentación exigidos por la AEPD. La innovación más destacada es la gestión inteligente de los planes de acción.

Asimismo, el DPD ha impulsado que HighQ funcione como una plataforma de coordinación corporativa, conectando al Departamento de Seguridad, el Departamento de Sistemas, la Asesoria Jurídica, Auditoría y el Servicio de Atención al Cliente mediante flujos homogéneos y automatizados. Esta orquestación mejora la coherencia del modelo y asegura respuestas rápidas y fundamentadas.

Finalmente, HighQ permite generar un *dashboard* estratégico de indicadores, que proporciona al DPD una visión global y basada en datos del riesgo de privacidad, esencial para la toma de decisiones en comités y para la supervisión continua. En conjunto, HighQ se consolida como el eje tecnológico que potencia el liderazgo del DPD y convierte la gestión de brechas en un proceso estratégico, verificable y orientado a la mejora continua.

Ejemplos de indicadores:

TIPO DE INDICADOR	EJEMPLOS
OPERATIVOS	> Número total de incidentes y brechas confirmadas (mensual y acumulado). > Tiempos medios desde la detección hasta el registro, análisis preliminar y calificación.
RIESGOS	> Tipología predominante de brechas (confidencialidad, integridad, disponibilidad) según la clasificación del Protocolo. > Tipología de datos afectados (datos generales, datos económicos, datos sensibles, etc.).

MEJORA CONTÍNUA	> Reincidencias por proceso/área (indicador clave para propuestas de rediseño). > Evolución de los plazos medios de resolución.

Con ello, HighQ proporciona al DPD una **visión sistémica del riesgo de privacidad**, que refuerza su función de asesoramiento, supervisión y alerta, y transforma la gestión de brechas en un proceso gobernado por datos y orientado a la toma de decisiones estratégicas.

C. Evolución del modelo de supervisión

El carácter innovador del proyecto de consolidación del modelo de supervisión reside en la construcción de un marco de control de privacidad de Primera Línea de Defensa (1LoD) global y más flexible, articulado por distintos elementos interconectados que busca superar las limitaciones de los modelos tradicionales de supervisión basados en revisiones generales, controles cerrados o auditorías reactivas.

El punto de partida de la metodología es un análisis sistemático y exhaustivo de la actividad supervisora: resoluciones sancionadoras de la AEPD y de autoridades europeas, jurisprudencia relevante, guías y directrices del CEPD, así como estudios doctrinales y *papers* especializados. Este análisis se operativiza a través de un **radar normativo** dinámico, que identifica tendencias interpretativas y puntos de foco del supervisor.

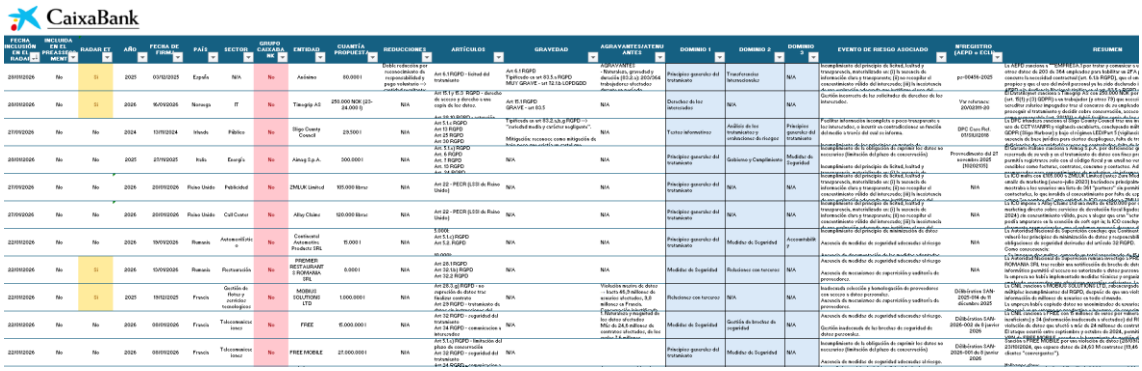


Imagen ilustrativa del Radar Normativo

Cada uno de estos elementos, se asocia a dominios concretos de riesgo dentro de la matriz corporativa de riesgos de privacidad, permitiendo traducir la tendencia regulatoria en un factor objetivo de cálculo del riesgo.

Esta información se integra con otros factores relevantes (historial sancionador, requerimientos de información, volumen de interesados, impacto económico, etc.) para generar un resultado cuantificado (impacto x probabilidad) de **exposición al riesgo por dominio y entidad**, denominado *pre assessment*, que permite traducir resultados numéricos en niveles de exposición comprensibles.

RESULTADO GLOBAL DEL RIESGO INHERENTE POR DOMINIO Y ENTIDAD

DOMINIO/ENTIDAD	CAIXABANK	CPC	CEF	VIDACAIXA	VIDACAIXA MEDIACIÓN	IMAGINERIS	MICROBANK	FACILITEA	BUILDING CENTER	LIVING CENTER	BANKIA HABITAT	CREDIFIMO	OPENWEALTH	CAM	CAIXABANK TITULIZAC	DUALIZA	VOLUNTARIOS	COPS	CFM	CDK TECH	PUERTO TRIANA	SILC	CDK RE WEALTH
Gobierno y Cumplimiento	ALTO	MEDIO-ALTO	MEDIO-BAJO	MEDIO-ALTO	MEDIO-ALTO	MEDIO-ALTO	MEDIO-ALTO	MEDIO-ALTO	MEDIO-ALTO	MEDIO-ALTO	MEDIO-BAJO	MEDIO	MEDIO-BAJO	MEDIO	MEDIO-BAJO	MEDIO-BAJO	MEDIO	MEDIO	MEDIO-BAJO	MEDIO-ALTO	MEDIO-BAJO	MEDIO-BAJO	MEDIO-BAJO
Gestión de brechas de seguridad	MEDIO-ALTO	MEDIO-ALTO	BAJO	MEDIO-ALTO	MEDIO	MEDIO	MEDIO-ALTO	MEDIO-ALTO	MEDIO	MEDIO	BAJO	MEDIO	BAJO	MEDIO	BAJO	BAJO	MEDIO	MEDIO-BAJO	BAJO	MEDIO	BAJO	BAJO	MEDIO-BAJO
Derechos de los interesados	MUY ALTO	MEDIO-ALTO	MEDIO	MEDIO-ALTO	MEDIO-ALTO	MEDIO-ALTO	MEDIO-ALTO	MEDIO-ALTO	MEDIO-ALTO	MEDIO-ALTO	MEDIO	MEDIO-ALTO	MEDIO	MEDIO-ALTO	MEDIO	MEDIO	MEDIO-ALTO	MEDIO	MEDIO	MEDIO-ALTO	MEDIO	MEDIO	MEDIO
Textos Informativos	ALTO	ALTO	MEDIO	ALTO	MEDIO-ALTO	MEDIO-ALTO	ALTO	ALTO	MEDIO-ALTO	MEDIO-ALTO	MEDIO	MEDIO-ALTO	MEDIO	ALTO	MEDIO	MEDIO	MEDIO-ALTO	MEDIO-ALTO	MEDIO	MEDIO-ALTO	MEDIO	MEDIO	MEDIO
Supervisores	ALTO	MEDIO-ALTO	BAJO	MEDIO-ALTO	MEDIO	MEDIO	MEDIO-ALTO	MEDIO-ALTO	MEDIO	MEDIO	BAJO	MEDIO	BAJO	MEDIO	BAJO	BAJO	MEDIO	MEDIO-BAJO	BAJO	MEDIO	BAJO	BAJO	BAJO
Principios Generales del Tratamiento	MUY ALTO	ALTO	MEDIO	ALTO	MEDIO-ALTO	MEDIO-ALTO	ALTO	ALTO	MEDIO-ALTO	MEDIO-ALTO	MEDIO	MEDIO-ALTO	MEDIO	ALTO	MEDIO	MEDIO	MEDIO-ALTO	MEDIO-ALTO	MEDIO	MEDIO-ALTO	MEDIO	MEDIO	MEDIO
[illegible]	MEDIO-ALTO	MEDIO-ALTO	MEDIO-BAJO	MEDIO-ALTO	MEDIO-ALTO	MEDIO-ALTO	MEDIO-ALTO	MEDIO-ALTO	MEDIO-ALTO	MEDIO-ALTO	MEDIO-BAJO	MEDIO	MEDIO-BAJO	MEDIO	MEDIO-BAJO	MEDIO-BAJO	MEDIO	MEDIO	MEDIO-BAJO	MEDIO-ALTO	MEDIO-BAJO	MEDIO-BAJO	MEDIO-BAJO
Relaciones con terceros	MEDIO-ALTO	MEDIO-ALTO	MEDIO-BAJO	MEDIO-ALTO	MEDIO-ALTO	MEDIO-ALTO	MEDIO-ALTO	MEDIO-ALTO	MEDIO-ALTO	MEDIO-ALTO	MEDIO-BAJO	MEDIO	MEDIO-BAJO	MEDIO	MEDIO-BAJO	MEDIO-BAJO	MEDIO	MEDIO	MEDIO-BAJO	MEDIO-ALTO	MEDIO-BAJO	MEDIO-BAJO	MEDIO-BAJO
Análisis de los tratamientos y evaluaciones de riesgo	ALTO	ALTO	MEDIO	ALTO	MEDIO-ALTO	MEDIO-ALTO	MEDIO-ALTO	MEDIO-ALTO	MEDIO-ALTO	MEDIO-ALTO	MEDIO	MEDIO-ALTO	MEDIO	ALTO	MEDIO	MEDIO	MEDIO-ALTO	MEDIO	MEDIO	MEDIO-ALTO	MEDIO	MEDIO	MEDIO
Accountability	MEDIO-ALTO	MEDIO-ALTO	BAJO	MEDIO-ALTO	MEDIO	MEDIO	MEDIO-ALTO	MEDIO-ALTO	MEDIO	MEDIO	BAJO	MEDIO	BAJO	MEDIO	BAJO	BAJO	MEDIO	MEDIO-BAJO	BAJO	MEDIO	BAJO	BAJO	BAJO
Medidas de Seguridad	Resultados de riesgo referenciados con el marco de control de Seguridad de la Información																						
Transferencias Internacionales	MEDIO-ALTO	MEDIO-ALTO	BAJO	MEDIO-ALTO	MEDIO	MEDIO	MEDIO-ALTO	MEDIO-ALTO	MEDIO	MEDIO	BAJO	MEDIO	BAJO	MEDIO	BAJO	BAJO	MEDIO	MEDIO-BAJO	BAJO	MEDIO	BAJO	BAJO	BAJO

Imagen ilustrativa del cálculo preliminar de exposición al riesgo

Este riesgo inherente calculado en el *pre assessment* permite decidir qué supervisar, cuándo y con qué intensidad, centrando la supervisión allí donde la exposición al incumplimiento es mayor.

Este enfoque se completa con un **modelo de atributos (matriz de riesgos y controles)**, que sustituye los controles genéricos y cerrados por controles base adaptables. Los controles no se ejecutan de forma abstracta, sino que se aterrizan en la operación concreta de tratamiento mediante atributos configurados a partir de la actualidad interpretativa extraída del radar. De este modo, el modelo es intrínsecamente escalable, evolutivo y adaptable a cambios normativos o tecnológicos, sin necesidad de redefinir el marco completo.

La automatización parcial de la medición del riesgo, tanto inherente como residual, facilita una monitorización continua del mismo, reduce la subjetividad y genera evidencias auditables del funcionamiento del modelo.

Finalmente, el marco de control se cierra con la **monitorización mediante indicadores**, que permite medir de forma objetiva el riesgo residual en dominios monitorizables y activar supervisiones adicionales cuando los resultados superen los umbrales de riesgo definidos.

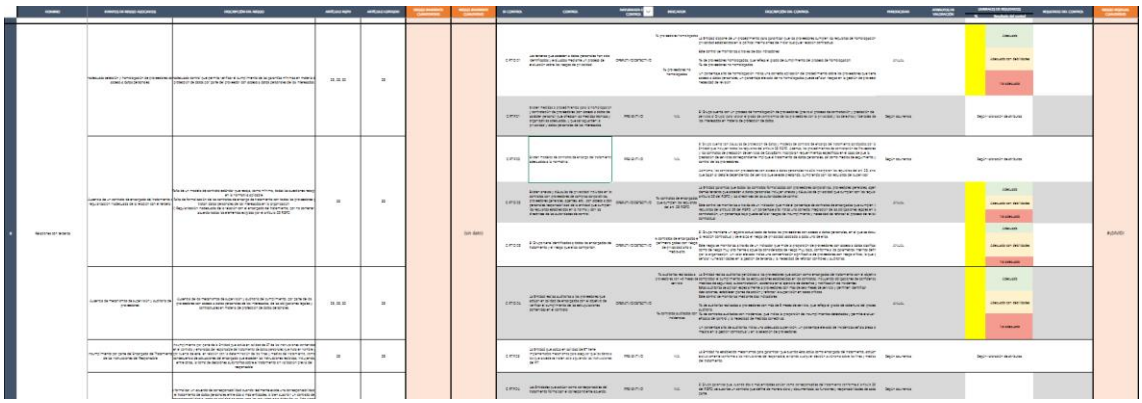


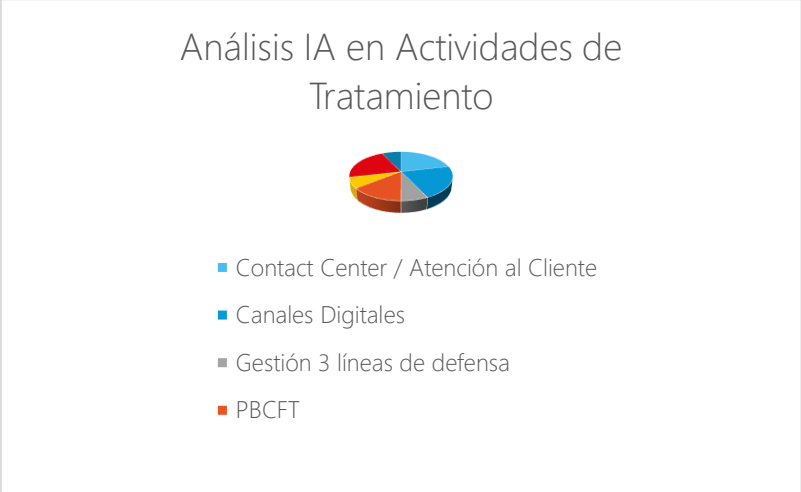
Imagen ilustrativa de la matriz de riesgos y controles con indicadores de riesgo asociados por dominio

RESULTADOS OBTENIDOS: evidencias prácticas del impacto del proyecto (protocolos, auditorías, indicadores de cumplimiento, participación interna, impacto en los interesados).

A. Gestión del riesgo de privacidad en el contexto del desarrollo o uso de sistemas de Inteligencia Artificial

El proceso GUIA, implantado en septiembre de 2025 como mecanismo de preevaluación de casos de uso de IA, ha permitido canalizar y ordenar más de 250 iniciativas desde su creación hasta el 30 de enero de 2026, generando un espacio de trabajo conjunto entre las áreas de negocio, tecnología, riesgos y el DPD, que favorece la detección temprana de riesgos y la mejora de la calidad regulatoria.

En el periodo objeto de valoración para el premio, se han analizado en 14 casos de uso de Inteligencia artificial, que se han incorporado, como activos, en las evaluaciones de impacto de los tratamientos de datos, que se distribuyen de la siguiente manera:



B. Evolución del registro, gestión y seguimiento de las brechas de datos personales y sus planes de acción

La evolución del registro, gestión y seguimiento de brechas de datos personales impulsada mediante la implantación corporativa de **HighQ** como herramienta única y la actualización del **Protocolo Corporativo de Gestión de Brechas**, ha generado resultados verificables que refuerzan la eficacia interna de estos procesos y elevan significativamente la protección de los derechos de los interesados.

En primer lugar, se ha consolidado un **proceso corporativo homogéneo, ágil y completamente documentado**, donde cada incidente se gestiona dentro de un expediente digital único que integra análisis técnicos y jurídicos, valoración de riesgos, medidas de contención y planes de acción, garantizando trazabilidad total y facilitando auditorías internas y externas.

En segundo lugar, la estandarización del proceso ha impulsado una **cultura interna de privacidad más sólida**, gracias a un sistema corporativo que permite que cualquier empleado o proveedor registre incidentes de forma rápida y uniforme. Esto ha mejorado la detección temprana, reforzado la responsabilidad compartida y estandarizado todos los canales de comunicación de brechas.

En tercer lugar, el nuevo modelo ha tenido un impacto directo en el **cumplimiento normativo y la seguridad jurídica**, aplicando de manera sistemática la metodología corporativa de valoración de riesgos, cumpliendo los plazos de notificación de 72 horas a la AEPD y asegurando que se comunican incidentes a los interesados cuando existe un alto riesgo para sus derechos y libertades.

Asimismo, la combinación de HighQ y el Protocolo ha permitido **elevar la protección efectiva de los afectados** gracias a medidas de mitigación inmediatas y registradas en

tiempo real (bloqueo de accesos, borrado de datos erróneos, recuperación de disponibilidad o resolución de fallos técnicos).

Un resultado clave es la **materialización del aprendizaje organizativo**, mediante la implantación de planes de acción verificables, con responsables, plazos y evidencias, cuyo seguimiento semanal garantiza mejoras preventivas y evita reincidencias.

Además, la centralización de la información ha permitido crear un **sistema robusto de indicadores operativos, de riesgo y de mejora continua**, que transforma la gestión de brechas en un proceso analítico y gobernado por datos, facilitando decisiones estratégicas en los diferentes comités corporativos.

Finalmente, el nuevo modelo fortalece la coherencia con las **Evaluaciones de Impacto y la gestión global del riesgo**, al vincular cada brecha con el tratamiento afectado, permitiendo actualizar medidas, revisar PIAs y reforzar el cumplimiento del principio de privacidad desde el diseño continuo.

En conjunto, estos resultados evidencian una evolución profunda hacia un **modelo proactivo, coordinado, trazable y preventivo**, alineado con el RGPD y las mejores prácticas europeas.

C. Evolución del modelo de supervisión

Las funciones de supervisión durante 2024-2025 han derivado en la finalización en CaixaBank, S.A. de los siguientes ejercicios:

- **6 ejercicios de carácter periódico,** en los que se han supervisado la correcta implementación de los controles definidos para mitigar los riesgos de los ámbitos de Gobierno y Cumplimiento, Medidas de Seguridad y *Accountability*;
- **3 ejercicios de carácter extraordinario**, en los que se ha revisado la correcta implementación de los controles dirigidos a asegurar el cumplimiento de la normativa en (i) el uso de cookies, (ii) el proceso de selección de encargados del tratamiento y (iii) en la atención y gestión de derechos de los interesados;
- **3 ejercicios de carácter recurrente**, en los que se ha revisado la correcta implementación de los controles definidos para mitigar el riesgo asociado a eventuales deficiencias de transparencia en la información proporcionada a los interesados sobre el tratamiento de sus datos personales.

Como resultado de la ejecución de los controles asociados, se han identificado un total de 24 planes de acción, de los cuales 21 se encuentran completamente implantados y 3 en curso.

Adicionalmente, el impacto y eficacia el marco de supervisión ha de medirse por la calidad de la evidencia generada y el beneficio directo para la organización y para los interesados.

Así, el proyecto ha aportado resultados tangibles sobre los elementos estructurales del cumplimiento en privacidad:

- Se ha elaborado una metodología objetiva, y homogénea en su aplicación por parte del equipo supervisor, que permite obtener una visión del riesgo por ámbitos y eventos de riesgo.
- Como resultado de los planes de acción definidos, se han revisado y homogeneizado protocolos y procedimientos.
- Se ha reforzado la trazabilidad y documentación, gracias a la configuración de un repositorio único de evidencias, hallazgos y comunicaciones.

IMPACTO Y REPLICABILIDAD: contribución a la cultura institucional de privacidad y posibilidad de reproducir el proyecto en otras entidades

A. Gestión del riesgo de privacidad en el contexto del desarrollo o uso de sistemas de Inteligencia Artificial

La implantación del modelo de gestión del riesgo de privacidad aplicado al desarrollo y uso de sistemas de Inteligencia Artificial ha tenido un impacto directo en la **cultura institucional de privacidad**, consolidando un enfoque preventivo y transversal en todas las áreas implicadas en el ciclo de vida de los casos de uso.

La colaboración estructurada entre la Oficina de IA y el equipo del DPO, sumada a la incorporación expresa del uso ético de los datos y de los componentes de IA en el Comité de Privacidad, ha permitido que la privacidad y los derechos fundamentales se integren de forma sistemática en las decisiones técnicas, jurídicas y de negocio.

Este modelo ha generado un entorno en el que los equipos comprenden, desde fases tempranas, los riesgos asociados a la IA y las medidas necesarias para mitigarlos, reforzando la responsabilidad proactiva y la trazabilidad de las decisiones adoptadas. Adicionalmente ha generado un **entorno de aprendizaje continuo y mutuo que se retroalimenta** con la propia colaboración.

Asimismo, el enfoque aplicado resulta **altamente replicable** en las otras entidades del Grupo, ya que se fundamenta en un conjunto de procesos, criterios de valoración, plantillas, flujos de acompañamiento y órganos de gobierno fácilmente transferibles a organizaciones con estructuras similares.

El uso del análisis IA en las PIAs, la estandarización de los puntos de control y la integración de roles y responsabilidades constituyen elementos metodológicos exportables que pueden adaptarse a distintos sectores. De esta manera, el proyecto no solo eleva el nivel interno de madurez en la gestión del riesgo de privacidad en IA, sino que ofrece un marco práctico y escalable que puede servir de referencia a otras instituciones que busquen implantar un modelo de gobernanza responsable y alineado con los principios de privacidad desde el diseño y respeto a los derechos fundamentales.

B. Evolución del registro, gestión y seguimiento de las brechas de datos personales y sus planes de acción

La actualización del Protocolo Corporativo de Brechas y la implantación de HighQ han generado un impacto profundo en la cultura, organización y gobernanza de la privacidad en CaixaBank. En primer lugar, se ha fortalecido la **cultura institucional de privacidad**, al establecer un procedimiento corporativo obligatorio que utiliza un lenguaje común, fomenta la detección temprana y articula un circuito transversal de colaboración entre todas las áreas implicadas. HighQ se ha convertido en el canal único para registrar incidentes, integrando la gestión de brechas en la operativa diaria de toda la plantilla.

En segundo lugar, el modelo ha tenido un **impacto organizativo significativo**, al consolidar un proceso homogéneo y estructurado para todo el Grupo, con fases estandarizadas, flujos automáticos de comunicación y responsabilidades claras. La herramienta y el Protocolo garantizan coherencia en la valoración del riesgo, uniformidad en los criterios de calificación y cumplimiento riguroso de los plazos legales —incluidas las 72 horas de notificación a la AEPD—, lo que mejora la seguridad jurídica y la protección efectiva de los derechos de los interesados.

Asimismo, HighQ actúa como un **facilitador de la replicabilidad del modelo**, al centralizar en un único expediente digital toda la documentación técnica, jurídica y operativa del incidente, automatizar flujos, integrar otros circuitos (vulneraciones, reclamaciones GDPR/ARCO+) y permitir el seguimiento avanzado de planes de acción con evidencias. Su diseño escalable hace posible adoptar el mismo modelo en filiales o en otras entidades con estructuras complejas.

Finalmente, el Protocolo y HighQ se basan en las **mejores prácticas regulatorias** (RGPD, LOPDGDD, guías del EDPB y de la AEPD), lo que convierte el modelo en plenamente transferible a cualquier organización sujeta al RGPD. En conjunto, la combinación de ambos elementos ha generado un sistema corporativo robusto, preventivo y basado en evidencias, capaz de evolucionar la cultura interna y, al mismo tiempo, convertirse en un estándar replicable para otras entidades que busquen alcanzar un nivel de excelencia en la gestión de brechas.

C. Evolución del modelo de supervisión

El proyecto responde a necesidad de desplegar funciones de supervisión independientes y efectivas (no basadas únicamente en un control formalista) en un contexto organizativo complejo, especialmente cuando los recursos disponibles para la función del Delegado de Protección de Datos son limitados.

El marco implementado constituye una **apuesta estratégica por una cultura de cumplimiento reforzada**, mediante la creación de una función de supervisión interna especializada, estable y metodológicamente avanzada, integrada en la primera línea de defensa. La función no se limita a comprobar la existencia formal de controles, sino que permite **evaluar su adecuación efectiva al riesgo real de incumplimiento**, atendiendo al contexto operativo, a la criticidad del tratamiento y a la evolución de la interpretación normativa por parte de las autoridades de control.

Asimismo, el uso del *pre assessment* y del radar normativo permite **alinear la supervisión con las áreas de mayor exposición**, superando los modelos homogéneos y facilitando una asignación más eficiente de los recursos disponibles. De este modo, la supervisión deja de ser reactiva para convertirse en **selectiva, estratégica y basada en evidencia**, reforzando de forma tangible el principio de responsabilidad proactiva (*accountability*) exigido por el RGPD.

Asimismo, la incorporación sistemática de la **tendencia supervisora y doctrinal** garantiza que los criterios aplicados estén permanentemente actualizados, dando respuesta directa a uno de los retos señalados por la AEPD en sus Memorias: la necesidad de **anticipar riesgos en un entorno normativo y tecnológico en constante evolución**, en lugar de limitarse a corregir incumplimientos una vez materializados (*Agencia Española de Protección de Datos, 2023; 2024*).

En definitiva, permite consolidar una cultura de privacidad que trasciende el cumplimiento formal y se orienta a la prevención efectiva del riesgo de sanción, en línea con las expectativas del supervisor y con las mejores prácticas recogidas en la doctrina especializada.

Valor añadido frente a las prácticas habituales del sector: El sector bancario y asegurador se caracterizan por un alto grado de madurez en materia de control interno, estructurado tradicionalmente en torno a un **modelo de tres líneas de defensa claramente segregadas**. En este esquema, la primera línea se articula de forma descentralizada por áreas y departamentos operativos; la segunda línea asume funciones de definición de marcos, supervisión y control; y la tercera línea ejerce una función de auditoría independiente sobre la eficacia del sistema.

En Privacidad, la primera línea de defensa corresponde a la asesoría jurídica junto con Seguridad de la Información. En este caso, la función del Delegado de Protección de Datos ha conseguido **configurar un equipo especializado dentro de la 1LoD**, no limitado al asesoramiento ex ante, sino capacitado para supervisar la efectiva implementación del asesoramiento en la operativa diaria, desde un enfoque metodológico basado en riesgo.

En este contexto, el valor diferencial del proyecto reside en haber logrado especializar la primera línea de defensa en materia de privacidad, dotándola de una **capacidad supervisora más efectiva**, sin romper el equilibrio propio del modelo de tres líneas ni invadir funciones de control de segundo o tercer nivel.

Encajar un esquema de estas características en un entorno tan regulado, estandarizado y supervisado como el bancario supone una dificultad organizativa y cultural significativa, pero este marco de control demuestra, sin embargo, que es posible evolucionar la primera línea de defensa hacia modelos capaces de integrar criterio jurídico, supervisión basada en riesgo y mejora continua, aportando un **valor añadido real y diferencial.**

Replicabilidad del modelo: El modelo tiene carácter **corporativo y transversal**, aplicable a todas las entidades del Grupo CaixaBank con independencia de su sector, tamaño o grado de madurez en materia de cumplimiento de la normativa de protección de datos.

En este sentido conviene trasladar que, durante 2024-2025, **se han desarrollado en las distintas empresas del Grupo CaixaBank un total de 62 ejercicios de supervisión de carácter periódico**, a través de los cuales se ha verificado la correcta implementación de los controles asociados a distintos ámbitos de riesgo definidos en la matriz corporativa, tales como ejercicio de derechos, formación, relación con supervisores, gobierno y cumplimiento, medidas de seguridad o accountability. En cada empresa, los criterios de evaluación se han adaptado a la naturaleza del riesgo materializado en función del sector y actividad en la que operan.

Estos ejercicios han permitido identificar un total de 323 Planes de Acción de los que 301 se encuentran ya cerrados, y 66 en implementación.

Se trata pues de un modelo basado en atributos y análisis de tendencia, que lo hace fácilmente replicable, y que ha permitido extender la metodología de supervisión al conjunto de empresas del Grupo, ajustando su aplicación al nivel de riesgo y a la naturaleza operativa de cada entidad, incluso operando en sectores diferentes y con niveles de madurez distintos.

Todo ello demuestra que el modelo tiene las características necesarias para ser reproducido en cualquier organización que disponga de un SGPD mínimamente estructurado, sin necesidad de que trate la misma tipología de datos, procesos o riesgos.

PARTICIPACION COMUNITARIA Y PROFESIONAL: COLABORACIÓN EN FOROS, ASOCIACIONES, ACTIVIDADES DE LA COMUNIDAD DE DPD Y DIFUSIÓN DE BUENAS PRÁCTICAS.

Teniendo en cuenta el contexto en el que desarrolla el DPD su función y el periodo establecido, se detallan a continuación los aspectos solicitados llevados a cabo por el DPD y su equipo:

1. **Colaboración en asociaciones de referencia de la privacidad**:

   - **ISMS Fórum**: Participación en las jornadas de:

- 14 de noviembre de 2024: **XXVI Jornada Internacional de SdI**: Mesa redonda de presentación de la **II Edición del Libro Blanco del DPO**. Miembro del equipo del DPO.
- 13 de febrero de 2025**: XXVII Foro de la privacidad del DPI**: mesa redonda ***"Modelo de Evaluación de Impacto en Derechos Fundamentales en IA (FRIA)"***;
- 13 de noviembre de 2025: **XXVII Jornada Internacional de Seguridad de la Información:** participación en dos mesas redondas:
  - **"Privacidad, identidad y pseudonimato: ¿cómo se protege el yo digital?"**
  - **"Retos del DPO: multas, usuario final y brechas"**

• Participación en Guías y publicaciones:

- II Edición del Libro Blanco del Delegado de Protección de Datos (DPO).

- **APEP-IA:** Membresía y participación en el congreso anual. Ponencia sobre las FRIAS.
- **IAPP**: Membresía y Certificado CIPP/E

2. **Colaboración y presencia en asociaciones sectoriales:**
   - **Centro de cooperación interbancaria (CCI)**: miembros participantes en las reuniones sectoriales de privacidad
   - **Confederación Española de Cajas de Ahorros (CECA)**: miembros participantes en las reuniones sectoriales de privacidad
   - **ASNEF**: miembros participantes en las reuniones sectoriales de privacidad
3. **Participación en la red "DPD's en xarxa" de la Autoridad catalana de protección de datos.**
   - Participación en el trabajo: "**Evaluaciones de impacto en derechos fundamentales**" promovida por la APDCAT y liderada por el profesor de la Universidad Politécnica de Turin, Alessandro Mantelero
4. **Participación en acciones de formación/divulgativas:**

   Actualmente el DPD y los miembros de su equipo, imparten los cursos o sesiones formativas siguientes:
   - Programa **INTELIGENCIA ARTIFICIAL, REGULACIÓN Y LEGAL PROMPTING**. Instituto de Empresa (IE)
   - **Curso de preparación de la certificación CDPP** - asignatura práctica sobre el RGPD. Isms Forum.
   - **Máster en protección de datos y Seguridad de la Información (MPDSI).** Universidad complutense de Madrid en colaboración con ISMS Forum.
   - **FRIAS: una aplicación práctica**. APEP
   - **Máster en IA**. Escuela Internacional de Posgrados (EIP)