



Principios de actuación de la política corporativa de seguridad de la información

25 de septiembre de 2025

Control de versiones

Versión	Fecha	Control
1	Abril 2023	✓ Versión inicial
2	21/12/2023 Consejo de Administración	✓ Alineación con la Política de seguridad de la información corporativa
3	19/12/2024 Consejo de Administración	✓ Alineación con la Política de seguridad de la información corporativa. ✓ Actualización del apartado 3. Principios generales de seguridad de la información.
4	25/09/2025 Consejo de Administración	✓ Actualización del apartado: 3 principios generales para la gestión del riesgo de seguridad de la información.

Contenido

1	Inicio	4
1.1	Antecedentes	4
1.2	Objetivo	4
2	Rango de aplicación	5
3	Principios generales de Seguridad de la Información	6
4	Marco de gobierno	8
5	Marco de información y reporting	9

1 Inicio

1.1 Antecedentes

Las tecnologías de la información y comunicación (TIC) son un recurso clave para el desarrollo y operación de los servicios bancarios. Las TIC no solo son útiles en las estrategias de las instituciones y forman parte de casi todos los procesos bancarios y canales de distribución, sino que también ejecutan los controles automatizados sobre la información clave (*core*) del *negocio*.

La seguridad de la información debe estar basada en un conjunto de medidas y procedimientos que tienen como objetivo proteger la información del Grupo CaixaBank y promueven la voluntad de:

- Asegurar la protección adecuada de la información mediante medidas de seguridad que el Grupo debe tomar para protegerse adecuadamente contra amenazas y riesgos que puedan afectar la confidencialidad, integridad y disponibilidad de sus sistemas, activos de información o recursos.
- Sistematizar la gestión de la seguridad de la información para ayudar en la toma de decisiones adecuadas, basadas en riesgos, en situaciones relacionadas con la preservación de la información.
- Establecer la función de seguridad de la información para todo el Grupo a través de responsabilidades y roles.

1.2 Objetivo

El Grupo entiende lo importante que es la seguridad en el tratamiento de la información para todo el Grupo, los clientes, los proveedores y, en general, todas las instituciones con las que mantiene relación. Ha considerado fundamental fijar el tipo de tratamiento que debe darse a la información que maneja, a lo largo de su ciclo de vida y para asegurar su confidencialidad, integridad, disponibilidad y autenticidad, así como la de los datos y activos de información y las TIC.

El objetivo de la Política corporativa de seguridad de la información es tener los principios corporativos sobre los que se deben basar las acciones a hacer en el ámbito de la seguridad de la información. Todo ello orientado a:

- Definir las medidas técnicas y organizativas necesarias para mitigar el riesgo sobre la seguridad de la información del Grupo.
- Asegurar la evaluación de las decisiones sobre seguridad de la información para mantener el equilibrio entre rentabilidad y riesgos.
- Mantener una gestión adecuada de este riesgo, de acuerdo con el Marco de Apetito al Riesgo, cuyo resultado debe situarse en el perfil de riesgo medio-bajo que ha determinado el Consejo de Administración para el Grupo.
- Cumplir con los requisitos regulatorios y las expectativas de los supervisores.

La Política a la que se refieren estos Principios se actualiza de acuerdo con las leyes vigentes y las mejores prácticas en la gestión de la seguridad de la información, tanto a nivel nacional como internacional.

2 Rango de aplicación

La Política a la que se refieren estos Principios es de carácter corporativo y está alineada con la Política corporativa de gestión del riesgo tecnológico. En su alcance están CaixaBank y todas sus sociedades dependientes (aquellas en las que la matriz ejerce una posición de control).

3 Principios generales de Seguridad de la Información

Los objetivos principales del Grupo son asegurar la transparencia, la independencia y el buen gobierno para proteger los intereses de todos los grupos interesados y contar con su confianza.

Los principios generales son pautas fundamentales sobre la seguridad de la información y deben estar presentes en cualquier actividad relacionada con la información y los sistemas propiedad del Grupo. A continuación, se presentan los principios generales:

- a) Alineación estratégica. El enfoque de la seguridad de la información se mantendrá en línea con los objetivos estratégicos del Grupo en todo momento.
- b) La gestión del riesgo. Al integrarse con el marco corporativo de gestión de riesgos, se identificarán, supervisarán y tratarán los riesgos para ubicarlos en los niveles aceptables definidos por el Grupo.
- c) La proporcionalidad. El despliegue de medidas de protección, detección y recuperación estará en proporción con los riesgos, su importancia, el valor de la información y el coste de las medidas de seguridad definidas.
- d) Medidas de seguridad en varios niveles o capas. Tendrá una estrategia de protección formada por varias capas de seguridad de origen organizativo, lógico y físico, dispuestas de tal manera entre ellas que cuando una falla, permita ganar tiempo para una reacción adecuada frente a incidentes materializados, reduce la probabilidad de que el sistema pueda ser comprometido en su conjunto y minimiza el impacto final en los sistemas y la información.

En relación con la seguridad física, se aplicarán los controles definidos en la Política corporativa de gestión de la seguridad física. Esta política establece el marco de acción sobre los accesos físicos en CPD y edificios singulares, excluyendo oficinas y otras instalaciones no críticas, así como aspectos de seguridad ambiental, cuya gestión corresponde a otras funciones corporativas.

- e) Características fundamentales de la seguridad de la información. Debido a la importancia de la información del Grupo y a su misión de lograr los objetivos de negocio, es importante asegurar su protección sobre la base de los pilares de disponibilidad, autenticidad, integridad o confidencialidad de los datos almacenados, transmitidos o tratados, o de los servicios ofrecidos por dichos sistemas de redes e información o accesibles a través de ellos. Se debe asegurar que la información sea confidencial según su clasificación, de manera que solo los usuarios autorizados puedan acceder a ella. Se debe asegurar la integridad de la información, asegurándose de que los datos no hayan sido manipulados y por lo tanto sean confiables. Se debe asegurar la autenticidad de las operaciones realizadas estableciendo mecanismos para confirmar su origen. Finalmente, se debe asegurar la disponibilidad de la información, que será la capacidad de permanecer accesible en el lugar, el momento y la forma que los usuarios autorizados lo requieran.

Del mismo modo, por requisitos legales y éticos, el Grupo debe proteger en estos términos la información bajo su responsabilidad relativa a clientes, terceros y organismos oficiales.

- f) Entrega de valor y mejora continua. Mediante el seguimiento continuo y la realización de revisiones y pruebas de seguridad para la evaluación de riesgos y controles, así como de resistencia periódica frente a los principales escenarios de riesgo, se medirá su efectividad para optimizar las inversiones y gasto en seguridad. El desarrollo de pruebas y el seguimiento continuo permitirá la captura de riesgos de seguridad emergentes, tanto por la evolución tecnológica como por la evolución del Grupo.

- g) Seguridad por defecto de los sistemas. Los sistemas de redes e información y sus datos deben ser diseñados y configurados para asegurar un grado suficiente de Seguridad alineado con los objetivos estratégicos del negocio, manteniéndolo seguro a lo largo de su ciclo de vida.
- h) Gestión de recursos humanos y técnicos. El proceso de seguridad de la información debe considerarse como un proceso formado por personas, elementos técnicos, materiales y organizativos. El personal que use los sistemas y la información debe recibir la formación necesaria y ser informado sobre sus deberes y obligaciones en materia de seguridad de la información que provienen de esta política. Este personal debe aplicar los principios de seguridad en el desempeño de sus funciones.
- i) La profesionalidad. El equipo encargado de gestionar la seguridad de la información estará capacitado para hacer sus funciones, siguiendo un proceso de actualización y formación continua en la materia.
- j) Clasificación de la información y de los activos. Los activos de información se clasificarán según los criterios de seguridad de la información y se asignarán según las funciones a cumplir y aplicando las medidas de seguridad oportunas.
- k) Criticidad de seguridad de la información. Para desarrollar, implementar y mantener la Política, se deben clasificar los activos del Grupo para identificar los más importantes en la seguridad de la información. Para ello, se establecerán a nivel corporativo los aspectos y criterios de seguridad de la información a considerar, igual y sin excepción, en todas las empresas del Grupo que estén dentro del alcance de esta Política. El Comité de Seguridad de la Información debe aprobar específicamente una definición de importancia desde el punto de vista de la seguridad de la información para identificar los activos más críticos. Las primeras líneas de defensa son las encargadas de hacer la clasificación para los activos existentes.
- l) Gestión de usuarios, privilegios, segregación y delegación de funciones. Se deben minimizar los riesgos derivados de la falta de segregación de funciones o incompatibilidades de funciones con roles concretos y la dependencia o sobrecarga de unipersonal en funciones críticas. También se establecerán procesos para la correcta gestión de los usuarios.
- m) Gestión de la seguridad de la información en proveedores. En la contratación de proveedores, se debe asegurar que se trasladan a nivel contractual y de formación los requisitos que provienen de las políticas corporativas y marcos de relación con proveedores. Los principales requisitos son: (1) cumplir con la legislación vigente sobre seguridad de la información en todo momento en los territorios donde el proveedor presta servicio al Grupo y promover las prácticas de libre mercado, así como revisar regularmente y mejorar las prácticas de gobierno; (2) establecer las medidas necesarias para prevenir y evitar en todo lo posible que la información y los sistemas del Grupo puedan ser utilizados para la práctica de conductas ilícitas y revisarlas periódicamente; colaborar activamente con los reguladores y las fuerzas de seguridad y comunicar cualquier actividad sospechosa que se detecte; y (3) fomentar prácticas responsables en materia de seguridad entre los proveedores y su cadena de suministro, mediante cláusulas contractuales y la implementación de mecanismos de supervisión.
- n) Incidentes de seguridad. Se establecerán mecanismos de detección y reacción ante Incidentes de seguridad que puedan comprometer los sistemas o activos de información del Grupo. Estos procedimientos cubrirán los mecanismos de detección, los criterios de clasificación, los procedimientos de análisis y resolución y la comunicación a las partes interesadas asegurándose de que el evento operativo se registre correctamente cuando sea necesario.
- o) Sanciones disciplinarias e incumplimientos. En el ámbito laboral, el incumplimiento de la Política de Seguridad puede considerarse como una infracción del deber de buena fe contractual, que puede ser castigada con las medidas disciplinarias previstas en la legislación laboral vigente en cada momento, y sin perjuicio del pago de daños y perjuicios que pueda reclamar el Grupo.

4 Marco de gobierno

Los pilares sobre los que se basa el marco de gobierno del riesgo asociado a la seguridad de la información en el Grupo son:

- Cumplimiento de los Principios mencionados en la Política por las empresas del Grupo dentro de su ámbito de aplicación.
- Supervisión corporativa de la entidad matriz.
- Alineación de estrategias entre las empresas del Grupo y alineación con las mejores prácticas, con las expectativas de los supervisores y con la regulación vigente.
- La participación máxima de los órganos de gobierno y dirección de las sociedades del Grupo.
- Marco de control interno basado en el modelo de Tres Líneas de Defensa que asegura la estricta separación de funciones y la existencia de varias capas de control independiente.

La Política a la que se refieren estos Principios será revisada por el Consejo de Administración.

5 Marco de información y reporting

El establecimiento de un marco de información adecuado es fundamental para gestionar los riesgos de seguridad de la información.

Los principales objetivos del marco de información son:

- Dar a los Órganos de Gobierno y a la Alta Dirección información precisa, clara y suficiente para facilitar la toma de decisiones y comprobar que se está operando dentro de la tolerancia al riesgo marcada.
- Satisfacer los requisitos de información de los organismos supervisores.
- Mantener informados a los accionistas y a los grupos de interés del Grupo CaixaBank en la seguridad de la información.
- Dar a los responsables de las áreas, especialmente a las áreas gestoras y a las áreas de control, los datos necesarios para controlar el cumplimiento de la estrategia definida para el Grupo en relación con la seguridad de la información.

Se proporcionará información regularmente a los Órganos de Gobierno. Además, a petición de los Órganos del Gobierno, se les proporcionará cualquier monográfico o información solicitada de manera puntual o recurrente en relación con la ciberseguridad en el Grupo.