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

[Mayo de 2023]

Control de versiones

Versión	Fecha	Control
1	Mayo 2023	✓ Versión inicial

Contenido

1. Introducción

1.1 Antecedentes

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

La seguridad de la información debe establecerse en torno a un conjunto de medidas y procedimientos que tengan como fin la salvaguarda de la información del Grupo y promuevan la voluntad de:

- Asegurar la adecuada protección de la información, desplegando medidas de seguridad que el Grupo CaixaBank debe adoptar para protegerse adecuadamente contra amenazas y riesgos que pudieran impactar sobre la confidencialidad, integridad y disponibilidad de sus sistemas, activos de información o recursos.
- Sistematizar la gestión de la seguridad de la información de manera que ayude en la adecuada toma de decisiones, basadas en riesgos, en situaciones relacionadas con la preservación de la seguridad de la información.
- Establecer para todo el Grupo CaixaBank la función de la seguridad de la información a través de responsabilidades y roles.

1.2 Objetivo

El Grupo CaixaBank, consciente de la importancia que la seguridad en el tratamiento de la información tiene para todo el Grupo, los clientes, los proveedores y, en general, todas las instituciones con las que se mantiene relación, considera fundamental establecer el tipo de tratamiento que debe darse a la información que gestiona, durante todo su ciclo de vida y con el fin de garantizar su confidencialidad, integridad y disponibilidad.

El objetivo de la Política corporativa de seguridad de la información (en adelante la Política) es disponer de los principios corporativos sobre los cuales deberán basarse las actuaciones a realizar en el ámbito de la seguridad de la información, todo ello encaminado a:

- Definir las medidas de índole técnica y organizativa necesarias para mitigar el riesgo sobre la seguridad de la información del Grupo CaixaBank.
- Asegurar la evaluación de las decisiones en materia de seguridad de la información para preservar el equilibrio entre rentabilidad y los riesgos.
- Mantener una gestión adecuada de este riesgo, en consonancia con el Marco de Apetito al Riesgo, cuyo resultado se debe situar en el perfil de riesgo medio-bajo que ha determinado el Consejo de Administración para el Grupo.
- Cumplir los requisitos regulatorios y las expectativas supervisoras.

La Política a la que se refieren los presentes Principios se actualiza en consonancia con las referencias normativas vigentes y las mejores prácticas en la gestión de la seguridad de la información, tanto a nivel nacional como internacional.

2. Ámbito de aplicación

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

3. Estrategia corporativa / Principios generales de la gestión del riesgo de seguridad de la información

La estrategia de seguridad de la información obedece a la necesidad de preservar la confidencialidad, disponibilidad e integridad de la información para la consecución de los objetivos estratégicos del negocio. Con esta premisa, se adopta una estrategia basada en análisis y monitorización periódica de riesgos que, de acuerdo con los umbrales de riesgo establecidos, determinarán su tratamiento.

El análisis y monitorización periódica de riesgos cobra especial relevancia en un entorno en el que emergen nuevas tecnologías que son rápidamente adoptadas por el negocio y la sociedad. Asimismo, se justifica esta aproximación por el incesante número de amenazas que aparecen a diario sobre la tecnología y la información, ya sea vinculado a aspectos novedosos o a través del aprovechamiento de obsolescencias o inadecuado mantenimiento de los entornos.

No se concibe el desarrollo de esta estrategia sin la disposición de un equipo adecuadamente capacitado y formado. Y, dada la complejidad del Grupo, tampoco se concibe el desarrollo de la estrategia sin la constante actualización de conocimientos adquirida a través, tanto de proveedores, como de participaciones en foros nacionales e internacionales y la adopción o alineación con estándares internacionales de reconocido prestigio.

3.1. Principios de la seguridad de la información

Entre los objetivos prioritarios del Grupo figura el garantizar la transparencia, la independencia y su buen gobierno con el fin de salvaguardar los intereses de todos los grupos de interés y contar con su confianza.

Los principios generales son directrices fundamentales relacionadas con la seguridad de la información y deberán estar siempre presentes en cualquier actividad relacionada con la información y los sistemas propiedad del Grupo. A continuación, se enumeran los principios generales:

a) Alineamiento estratégico. El enfoque de la seguridad de la información se mantendrá alineado en todo momento con los objetivos estratégicos del Grupo.

b) Gestión del riesgo. A través de la integración con el marco corporativo de gestión de riesgos, se identificarán, monitorizarán y tratarán los riesgos para situarlos en los niveles aceptables definidos por el Grupo.

c) Proporcionalidad. El despliegue de medidas de protección, detección y recuperación será proporcional a los riesgos, su criticidad, el valor de la información y el coste de las medidas de seguridad definidas.

d) Medidas de seguridad en varios niveles o capas. Se dispondrá de una estrategia de protección constituida por varias capas de seguridad de origen organizativo, lógico y físico, dispuestas de tal manera entre ellas que cuando una falle, permita ganar tiempo para una reacción adecuada frente

a incidentes materializados, se reduzca la probabilidad de que el sistema pueda ser comprometido en todo su conjunto y se minimice el impacto final sobre los sistemas y la información.

e) Características fundamentales de la seguridad de la información. Debido al carácter estratégico de la información del Grupo y la misión de alcanzar los objetivos de negocio, es necesario garantizar su protección sobre la base de los pilares de confidencialidad, integridad y disponibilidad. Se deberá garantizar la confidencialidad de la información según su categorización, de tal manera que solo los usuarios autorizados, tengan acceso a la misma. Deberá asegurarse la integridad de la información, garantizando que los datos no hayan sido manipulados y, por tanto, sean confiables. Por último, se deberá garantizar la disponibilidad de la información, que será la capacidad de permanecer accesible en la ubicación, el momento y la forma en la que los usuarios que estén autorizados lo requieran.

   Del mismo modo y por requerimientos legales y éticos, el Grupo deberá proteger en los mismos términos la información bajo su responsabilidad relativa a clientes, terceros y organismos oficiales.

f) Entrega de valor y mejora continua. A través de la monitorización continua de los riesgos y los controles, se medirá su efectividad para optimizar las inversiones y gasto en materia de seguridad. La monitorización continuada permitirá la captura de riesgos emergentes de seguridad, tanto motivados por la evolución tecnológica como por la propia evolución del Grupo.

g) Seguridad por defecto de los sistemas. Los sistemas y sus datos deberán diseñarse y configurarse con el fin de garantizar un grado suficiente de seguridad alineado con los objetivos estratégicos de negocio.

h) Gestión de los 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 usuario de los sistemas y la información deberá recibir la formación y concienciación necesaria e informada de sus deberes y obligaciones en materia de seguridad de la información. Dicho personal deberá aplicar los principios de seguridad en el desempeño de sus funciones.

i) Profesionalidad. El equipo encargado de gestionar la seguridad de la información estará debidamente capacitado y formado para el desempeño de sus funciones, bajo un proceso de actualización y formación continuada en la materia.

j) Clasificación de la información y de los activos. Los activos se clasificarán a partir de los criterios de seguridad de la información y se asignarán de acuerdo con las funciones a desempeñar y aplicando las medidas de seguridad oportunas.

k) Privilegios, segregación y delegación de funciones. Se deberán minimizar los riesgos derivados de la ausencia de segregación de funciones o incompatibilidades de funciones con roles concretos y la dependencia o sobrecarga unipersonal en funciones críticas.

l) Incidentes de seguridad. Se establecerán mecanismos de detección y reacción frente a 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.

m) Sanciones disciplinarias e incumplimientos. En el ámbito laboral el incumplimiento de la Política de Seguridad podrá ser considerado como una infracción del deber de buena fe contractual, sancionable con las medidas disciplinarias previstas en la legislación y normativa laboral vigente en cada momento, y sin perjuicio del resarcimiento por daños y perjuicios que les pueda reclamar el Grupo.

3.2. Principios de seguridad de la información en relación con los proveedores

En la contratación de proveedores, se deberá asegurar que se trasladan los requisitos que emanen de las políticas corporativas y marcos de relación con proveedores, entre las cuales destacan:

a) Cumplir con la legislación vigente en materia de seguridad de la información en todo momento en los territorios en los que o desde los que el proveedor preste servicio al Grupo y favorecer las prácticas de libre mercado, así como revisar regularmente y mejorar las prácticas de gobierno.

b) 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 todas las actividades sospechosas que se detecten.

c) Fomentar prácticas responsables en materia de seguridad entre los proveedores y su cadena de suministro, a través de cláusulas contractuales y la implantación de mecanismos de supervisión.

El Grupo propagará los principios de la Política corporativa de seguridad de la información a los proveedores, tanto a nivel contractual como a través de la formación y divulgación de estos.

4. Marco de gobierno

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

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

La Política a la que se refieren los presentes Principios se someterá a revisión del Consejo de Administración.

5. Marco de información y reporting

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

Los principales objetivos del marco de información son:

- Proporcionar a los Órganos de Gobierno y a la Alta Dirección, con la antelación suficiente, información exacta, clara y suficiente que facilite la toma de decisiones y permita verificar que se está operando dentro de la tolerancia al riesgo marcada.
- Satisfacer los requerimientos de información de los organismos supervisores.

- Suministrar a los responsables de las distintas áreas, en especial a las áreas gestoras y a las áreas de control, los datos necesarios para poder realizar el control del cumplimiento de la estrategia definida para el Grupo en relación con el de seguridad.

Se facilitará, de forma periódica, la información a los Órganos de Gobierno. Adicionalmente, a demanda de los Órganos de Gobierno, se les proporcionará cualquier monográfico o información solicitada de forma puntual o recurrente en relación con la ciberseguridad en el Grupo CaixaBank.