Principis d'actuació de la política corporativa de seguretat de la informació

[Maig de 2023]

Control de versions

Versió	Data	Control
1	Maig 2023	✓ Versió inicial

Contingut

1. Introducció

1.1 Antecedents

Les tecnologies de la informació i la comunicació (TIC) són, actualment, un recurs clau per al desenvolupament i operació dels serveis bancaris. Les TIC no només són habilitadores en les estratègies de les institucions i formen part de gairebé tots els processos bancaris i canals de distribució, sinó que a més a més executen els controls automatitzats sobre la informació clau (core) del negoci.

La seguretat de la informació s'ha d'establir al voltant d'un conjunt de mesures i procediments que tinguin com a finalitat la salvaguarda de la informació del Grup i promouen la voluntat de:

- Assegurar la protecció adequada de la informació, desplegant mesures de seguretat que el Grup CaixaBank ha d'adoptar per protegir-se adequadament contra amenaces i riscos que poguessin impactar sobre la confidencialitat, integritat i disponibilitat dels seus sistemes, actius d'informació o recursos.
- Sistematitzar la gestió de la seguretat de la informació de manera que ajudi en la presa de decisions adequada, basades en riscos, en situacions relacionades amb la preservació de la seguretat de la informació.
- Establir per a tot el Grup CaixaBank la funció de la seguretat de la informació mitjançant responsabilitats i rols.

1.2 Objectiu

El Grup CaixaBank, conscient de la importància que la seguretat en el tractament de la informació té per a tot el Grup, els clients, els proveïdors i, en general, totes les institucions amb què es manté relació, considera fonamental establir el tipus de tractament que s'ha de donar a la informació que gestiona, durant tot el cicle de vida i per tal de garantir-ne la confidencialitat, integritat i disponibilitat.

L'objectiu de la Política corporativa de seguretat de la informació (d'ara endavant la Política) és disposar dels principis corporatius sobre els quals s'hauran de basar les actuacions a realitzar en l'àmbit de la seguretat de la informació, tot encaminat a:

- Definir les mesures tècniques i organitzatives necessàries per mitigar el risc sobre la seguretat de la informació del Grup CaixaBank.
- Assegurar l'avaluació de les decisions en matèria de seguretat de la informació per preservar l'equilibri entre rendibilitat i els riscos.
- Mantenir una gestió adequada d'aquest risc, d'acord amb el Marc d'Apetit al Risc, el resultat del qual s'ha de situar al perfil de risc mitjà-baix que ha determinat el Consell d'Administració per al Grup.
- Complir els requisits reguladors i les expectatives supervisores.

La Política a què es refereixen aquests Principis s'actualitza d'acord amb les referències normatives vigents i les millors pràctiques en la gestió de la seguretat de la informació, tant a nivell nacional com internacional.

2. Àmbit d'aplicació

La Política a què es refereixen aquests Principis té caràcter corporatiu i està alineada amb la Política corporativa de gestió del risc tecnològic. Al seu abast hi ha CaixaBank i totes les seves societats dependents (aquelles en què la matriu exerceixi una posició de control).

3. Estratègia corporativa / Principis generals de la gestió del risc de seguretat de la informació

L'estratègia de seguretat de la informació obeeix a la necessitat de preservar la confidencialitat, la disponibilitat i la integritat de la informació per a la consecució dels objectius estratègics del negoci. Amb aquesta premissa, s'adopta una estratègia basada en anàlisi i monitorització periòdica de riscos que, d'acord amb els llindars de risc establerts, en determinaran el tractament.

L'anàlisi i monitorització periòdica de riscos adquireix una rellevància especial en un entorn en què emergeixen noves tecnologies que són ràpidament adoptades pel negoci i la societat. Així mateix, es justifica aquesta aproximació per l'incessant nombre d'amenaces que apareixen diàriament sobre la tecnologia i la informació, ja sigui vinculat a aspectes nous o a través de l'aprofitament d'obsolescències o manteniment inadequat dels entorns.

No es concep el desenvolupament d'aquesta estratègia sense la disposició d'un equip adequadament capacitat i format. I, atesa la complexitat del Grup, tampoc no es concep el desenvolupament de l'estratègia sense la constant actualització de coneixements adquirida a través, tant de proveïdors, com de participacions en fòrums nacionals i internacionals i l'adopció o l'alineació amb estàndards internacionals de reconegut prestigi.

3.1 Principis de la seguretat de la informació

Entre els objectius prioritaris del Grup figura garantir la transparència, la independència i el bon govern per tal de salvaguardar els interessos de tots els grups d'interès i comptar amb la seva confiança.

Els principis generals són directrius fonamentals relacionades amb la seguretat de la informació i han de ser sempre presents en qualsevol activitat relacionada amb la informació i els sistemes propietat del Grup. A continuació, s'enumeren els principis generals:

a) Alineament estratègic. L'enfocament de la seguretat de la informació es mantindrà alineat en tot moment amb els objectius estratègics del Grup.

b) Gestió del risc. A través de la integració amb el marc corporatiu de gestió de riscos, s'identificaran, monitoraran i tractaran els riscos per a situar-los en els nivells acceptables definits pel Grup.

c) Proporcionalitat. El desplegament de mesures de protecció, detecció i recuperació serà proporcional als riscos, la seva criticitat, el valor de la informació i el cost de les mesures de seguretat definides.

d) Mesures de seguretat en diversos nivells o capes. Es disposarà d'una estratègia de protecció constituïda per diverses capes de seguretat d'origen organitzatiu, lògic i físic, disposades de tal manera entre elles que quan una falli, permeti guanyar temps per a una reacció adequada enfront d'incidents materialitzats, es redueixi la probabilitat que el sistema pugui ser compromès en tot el seu conjunt i es minimitzi l'impacte final sobre els sistemes i la informació.

e) Característiques fonamentals de la seguretat de la informació. A causa del caràcter estratègic de la informació del Grup i la missió d'aconseguir els objectius de negoci, és necessari garantir la seva protecció sobre la base dels pilars de confidencialitat, integritat i disponibilitat. S'haurà de garantir la confidencialitat de la informació segons la seva categorització, de tal manera que només els usuaris autoritzats, tinguin accés a aquesta. Haurà d'assegurar-se la integritat de la informació, garantint que les dades no hagin estat manipulats i, per tant, siguin de confiança. Finalment, s'haurà de garantir la disponibilitat de la informació, que serà la capacitat de romandre accessible en la ubicació, el moment i la forma en la qual els usuaris que estiguin autoritzats el requereixin.
   De la mateixa manera i per requeriments legals i ètics, el Grup haurà de protegir en els mateixos termes la informació sota la seva responsabilitat relativa a clients, tercers i organismes oficials.

f) Lliurament de valor i millora contínua. A través del monitoratge continu dels riscos i els controls, es mesurarà la seva efectivitat per a optimitzar les inversions i despesa en matèria de seguretat. El monitoratge continuat permetrà la captura de riscos emergents de seguretat, tant motivats per l'evolució tecnològica com per la pròpia evolució del Grup.

g) Seguretat per defecte dels sistemes. Els sistemes i les seves dades hauran de dissenyar-se i configurar-se amb la finalitat de garantir un grau suficient de seguretat alineat amb els objectius estratègics de negoci.

h) Gestió dels recursos humans i tècnics. El procés de seguretat de la informació ha de considerar-se com un procés format per persones, elements tècnics, materials i organitzatius. El personal usuari dels sistemes i la informació haurà de rebre la formació i conscienciació necessària i informada dels seus deures i obligacions en matèria de seguretat de la informació. Aquest personal haurà d'aplicar els principis de seguretat en l'acompliment de les seves funcions.

i) Professionalitat. L'equip encarregat de gestionar la seguretat de la informació estarà degudament capacitat i format per a l'acompliment de les seves funcions, sota un procés d'actualització i formació continuada en la matèria.

j) Classificació de la informació i dels actius. Els actius es classificaran a partir dels criteris de seguretat de la informació i s'assignaran d'acord amb les funcions a exercir i aplicant les mesures de seguretat oportunes.

k) Privilegis, segregació i delegació de funcions. S'hauran de minimitzar els riscos derivats de l'absència de segregació de funcions o incompatibilitats de funcions amb rols concrets i la dependència o sobrecàrrega unipersonal en funcions crítiques.

l) Incidents de seguretat. S'establiran mecanismes de detecció i reacció enfront d'incidents de seguretat que puguin comprometre els sistemes o actius d'informació del Grup. Aquests procediments cobriran els mecanismes de detecció, els criteris de classificació, els procediments d'anàlisis i resolució i la comunicació a les parts interessades.

m) Sancions disciplinàries i incompliments. En l'àmbit laboral l'incompliment de la Política de Seguretat podrà ser considerat com una infracció del deure de bona fe contractual, sancionable amb les mesures disciplinàries previstes en la legislació i normativa laboral vigent a cada moment, i sense perjudici del rescabalament per danys i perjudicis que els pugui reclamar el Grup.

3.2 Principis de seguretat de la informació en relació amb els proveïdors

En la contractació de proveïdors, s'haurà d'assegurar que es traslladen els requisits que emanin de les polítiques corporatives i marcs de relació amb proveïdors, entre les quals destaquen:

a) Complir amb la legislació vigent en matèria de seguretat de la informació en tot moment en els territoris en els quals o des dels quals el proveïdor presti servei al Grup i afavorir les pràctiques de lliure mercat, així com revisar regularment i millorar les pràctiques de govern.

b) Establir les mesures necessàries per a prevenir i evitar en tan possible com la informació i els sistemes del Grup puguin ser utilitzats per a la pràctica de conductes il·lícites i revisar-les periòdicament, col·laborar activament amb els reguladors i les forces de seguretat i comunicar totes les activitats sospitoses que es detectin.

c) Fomentar pràctiques responsables en matèria de seguretat entre els proveïdors i la seva cadena de subministrament, a través de clàusules contractuals i la implantació de mecanismes de supervisió.

El Grup propagarà els principis de la Política corporativa de seguretat de la informació als proveïdors, tant a nivell contractual com a través de la formació i divulgació d'aquests.

4. Marc de govern

Els pilars sobre els quals s'assenteixi el marc de govern del risc associat a la seguretat de la informació en el Grup CaixaBank són:

- Compliment dels principis recollits en la Política a la qual es refereixen els presents Principis per part de les societats del Grup CaixaBank dins del seu àmbit d'aplicació.
- Supervisió corporativa de l'entitat matriu.
- Alineació d'estratègies entre les societats del Grup, i al seu torn alineació amb les millors pràctiques, amb les expectatives supervisores i amb la regulació vigent.
- Implicació màxima dels òrgans de govern i direcció de les societats del Grup.
- Marc de control intern basat en el model de Tres Línies de Defensa que garanteix l'estricta segregació de funcions i l'existència de diverses capes de control independent.

La Política a la qual es refereixen els presents Principis se sotmetrà a revisió del Consell d'Administració.

5. Marc d'informació i reporting

L'establiment d'un marc d'informació adequat és fonamental per a la gestió dels riscos de seguretat.

Els principals objectius del marc d'informació són:

- Proporcionar als Òrgans de Govern i a l'Alta Direcció, amb l'antelació suficient, informació exacta, clara i suficient que faciliti la presa de decisions i permeti verificar que s'està operant dins de la tolerància al risc marcada.
- Satisfer els requeriments d'informació dels organismes supervisors.

- Subministrar als responsables de les diferents àrees, especialment a les àrees gestores i a les àrees de control, les dades necessàries per a poder realitzar el control del compliment de l'estratègia definida per al Grup en relació amb el de seguretat.

Es facilitarà, de manera periòdica, la informació als Òrgans de Govern. Addicionalment, a demanda dels Òrgans de Govern, se'ls proporcionarà qualsevol monogràfic o informació sol·licitada de manera puntual o recurrent en relació amb la ciberseguretat en el Grup CaixaBank.