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

[Desembre de 2023]

Control de versions

Versió	Data	Control
1	Abril 2023	✓ Versió inicial
2	21/12/2023	✓ Alineament amb la Política corporativa de seguretat de la informació

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 fi la salvaguarda de la informació del Grup CaixaBank ("d'ara endavant, el Grup") i promoguin la voluntat de:

- Assegurar la protecció adequada de la informació, desplegant mesures de seguretat que el Grup 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 la funció de la seguretat de la informació a través de responsabilitats i rols.

1.2 Objectiu

El Grup, 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.
- 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 Principals generals 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, monitoritzaran i tractaran els riscos per situar-los als nivells acceptables definits pel Grup.

c) Proporcionalitat. El desplegament de mesures de protecció, detecció i recuperació és 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 que quan una falli, permeti guanyar temps per a una reacció adequada davant 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'assolir els objectius de negoci, cal garantir-ne la 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 manera que només els usuaris autoritzats hi tinguin accés. S'haurà d'assegurar la integritat de la informació, garantint que les dades no hagin estat manipulades i, per tant, siguin fiables. Finalment, caldrà garantir la disponibilitat de la informació, que serà la capacitat de romandre accessible a la ubicació, el moment i la forma en què els usuaris que estiguin autoritzats ho requereixin.

   De la mateixa manera i per requeriments legals i ètics, el Grup haurà de protegir en aquests termes la informació sota responsabilitat relativa a clients, tercers i organismes oficials.

f) Lliurament de valor i millora contínua. A través del monitoratge continu i el desenvolupament de revisions i proves per a l'avaluació dels riscos i els controls, se n'ha de mesurar l'efectivitat per optimitzar les inversions i la 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 s'han de dissenyar i configurar per tal de garantir un grau suficient de seguretat alineat amb els objectius estratègics de negoci, mantenint la seva seguretat al llarg de tot el cicle de vida.

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

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

j) Classificació de la informació i dels actius. Els actius d'informació 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) Criticitat de seguretat de la informació. El desenvolupament, la implantació i el manteniment de la Política requereix la formalització d'uns criteris de categorització dels actius del Grup amb l'objectiu d'identificar aquells més prioritaris a l'hora d'abordar la seguretat de la informació. Per això, s'establiran a nivell corporatiu els aspectes i els criteris de seguretat de la informació a ser considerats, per igual i sense excepció, en totes les societats del Grup que estiguin a l'abast d'aquesta Política. El Comitè de Seguretat de la Informació haurà d'aprovar de forma específica una definició de criticitat des de la perspectiva de seguretat de la informació, de manera que es permeti identificar els actius més crítics, i les primeres línies de defensa seran les encarregades de realitzar la classificació per als actius existents.

l) Gestió d'usuaris, privilegis, segregació i delegació de funcions. S'han 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. Així mateix, s'establiran processos per a l'adequada de gestió d'usuaris.

m) Gestió de la seguretat de la informació en proveïdors. En la contractació de proveïdors, cal assegurar que es traslladen tant a nivell contractual com de formació els requisits que emanin de les polítiques corporatives i marcs de relació amb proveïdors. Els principals requisits són: (1) complir amb la legislació vigent en matèria de seguretat de la informació en tot moment als territoris en què 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; (2) establir les mesures necessàries per prevenir i evitar en tot el possible que 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; i (3) fomentar pràctiques responsables en matèria de seguretat entre els proveïdors i la cadena de subministrament, a través de clàusules contractuals i la implantació de mecanismes de supervisió.

n) Incidents de seguretat. S'establiran mecanismes de detecció i reacció davant d'incidents de seguretat que puguin comprometre els sistemes o actius d'informació del Grup. Aquests procediments han de cobrir els mecanismes de detecció, els criteris de classificació, els procediments d'anàlisi i resolució i la comunicació a les parts interessades i han de garantir el registre adequat de l'esdeveniment operacional quan sigui procedent.

o) 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 a la legislació i normativa laboral vigent en cada moment, i sense perjudici del rescabalament per danys i perjudicis que els pugui reclamar el Grup.

4 Marc de govern

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

- Compliment dels principis recollits a la Política a què es refereixen els presents Principis per part de les societats del Grup dins del seu àmbit d'aplicació.
- Supervisió corporativa de l'entitat matriu.
- Alineació d'estratègies entre les societats del Grup, i alhora 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 què es refereixen aquests 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 de la informació.

Els objectius principals del marc d'informació són:

- Proporcionar als Òrgans de Govern i a l'Alta Direcció, amb prou antelació, 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.
- Mantenir informats els accionistes, així com els grups d'interès del Grup en l'àmbit de la seguretat de la informació.
- Subministrar als responsables de les diferents àrees, especialment a les àrees gestores i a les àrees de control, les dades necessàries per poder fer el control del compliment de l'estratègia definida per al Grup en relació amb la de seguretat.
- Satisfer els requeriments d'informació dels organismes supervisors.

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 forma puntual o recurrent en relació amb la ciberseguretat al Grup.