

itequia

Política de seguretat de la informació

itequia.com



Índex de continguts

Índex de continguts	2
1. Aprovació i entrada en vigor	3
2. Objectius de l'organització.....	3
5. Principis rectors de la política.....	5
6. Abast de certificació.....	6
7. Marc normatiu	6
8. Responsabilitats i organització de la seguretat.....	7
9. Designació i renovació dels rols de seguretat	10
10. Resolució de conflictes	10
11. Gestió del risc	10
12. Recursos	11
13. Dades de caràcter personal	11
14. Desenvolupament de la política de seguretat de la informació.....	12
15. Obligacions del personal.....	12
16. Terceres parts / prestadors de serveis / proveïdors de solucions.....	13
17. Gestió d'incidents de seguretat	14
18. Categoria de seguretat	14
19. Aprovació de la política i entrada en vigor.....	14



1. Aprovació i entrada en vigor

Text aprovat el dia 20/10/2026 per la direcció, d'ara endavant l'empresa.

Aquesta Política de Seguretat de la Informació és vigent des de la data d'aprovació (o de publicació, per a les entitats en què en sigui obligatòria la publicació oficial) i fins que sigui substituïda per una nova Política.

Aquest text deroga l'anterior, que va ser aprovat el dia 22/07/2026 per la direcció de l'empresa.

2. Objectius de l'organització

L'empresa es recolza en els seus sistemes d'informació per assolir els seus objectius estratègics. Per això, la gestió diligent i la protecció d'aquests sistemes són prioritàries. Hem d'aplicar mesures adequades, basades en una avaluació de riscos, per protegir-los de qualsevol incident, intencionat o accidental, que pugui comprometre l'autenticitat, la traçabilitat, la integritat o la confidencialitat de la informació, o la disponibilitat dels serveis.

La seguretat de la informació té com a objectiu primordial garantir l'operativitat contínua de l'empresa, de manera que pugui complir les seves funcions i oferir serveis d'alta qualitat. Per aconseguir-ho, és fonamental adoptar un enfocament preventiu, supervisar activament les operacions diàries i respondre amb agilitat a qualsevol incident.

Els sistemes TIC estan exposats a un panorama d'amenaques dinàmic que podria afectar negativament la confidencialitat, la integritat, la disponibilitat, l'ús previst i el valor de la informació i dels serveis. Per defensar-nos-en eficaçment, cal una estratègia de seguretat adaptable que s'ajusti als canvis de l'entorn. Això implica que cada departament ha d'implementar les mesures de seguretat obligatòries de l'Esquema Nacional de Seguretat (ENS), fer un seguiment constant dels nivells de prestació dels serveis, analitzar les vulnerabilitats detectades i disposar de plans de resposta a incidents per assegurar la continuïtat del negoci.

És imprescindible que la seguretat TIC sigui un pilar fonamental en cada etapa del cicle de vida d'un sistema: des de la seva concepció i desenvolupament fins a la seva adquisició, operació i eventual retirada. Els requisits de seguretat i les necessitats de finançament s'han d'identificar i incorporar en la planificació, així com en les sol·licituds d'ofertes i els plecs de licitació per a projectes que gestionin dades personals, que impliquin la compra de serveis TIC o que afectin els nostres sistemes d'informació.



3. Abast

Aquesta política s'aplica a tots els sistemes d'informació de l'empresa, a les persones que formen part de l'organització i als prestadors de serveis o proveïdors de solucions TIC de l'empresa.

4. Missió

L'entitat ITEQUIA TECHNOLOGY CONSULTING SL, constituïda legalment com a societat limitada amb NIF B75668335, és una entitat de naturalesa PRIVADA la missió principal de la qual és: desenvolupament, explotació i suport de programari i serveis SaaS propis; consultoria, desenvolupament, implementació, explotació i suport de solucions tecnològiques, a mida o basades en productes de tercers; administració i suport tècnic de sistemes, infraestructura i lloc de treball, en entorns cloud i locals.

A l'efecte del compliment de l'Esquema Nacional de Seguretat, l'entitat opera com a prestador de serveis privat.

Els objectius en matèria de seguretat que l'empresa pretén garantir amb aquesta Política són:

- Garantir la confidencialitat, la integritat i l'autenticitat de la informació i la continuïtat en la prestació dels serveis.
- Implementar mesures de seguretat en funció del risc.
- Formar i conscienciar els membres de l'empresa en matèria de seguretat de la informació. Implementar mesures de seguretat que permetin la traçabilitat dels accessos i respectar, entre d'altres, el principi de mínim privilegi, reforçant també el deure de confidencialitat de les persones usuàries pel que fa a la informació que coneixen en l'exercici de les seves funcions.
- Desplegar i controlar la seguretat física, de manera que els actius d'informació es trobin en àrees segures, protegits per controls d'accés, d'acord amb els riscos detectats.
- Establir la seguretat en la gestió de les comunicacions mitjançant els procediments necessaris, de manera que la informació que es transmeti a través de xarxes de comunicacions estigui adequadament protegida.
- Controlar l'adquisició, el desenvolupament i el manteniment dels sistemes d'informació en totes les fases del seu cicle de vida, garantint-ne la seguretat per defecte.
- Controlar el compliment de les mesures de seguretat en la prestació dels serveis, mantenint el control en l'adquisició i la incorporació de nous components del sistema.
- Gestionar els incidents de seguretat per detectar-los, contenir-los, mitigar-los i resoldre'ls correctament, adoptant les mesures necessàries perquè no es tornin a produir.
- Protegir la informació personal, adoptant les mesures tècniques i organitzatives adequades als riscos derivats del tractament, d'acord amb la legislació en matèria de protecció de dades.
- Supervisar de manera continuada el sistema de gestió de la seguretat, millorant-lo i corregint les ineficiències detectades.



5. Principis rectors de la política

- Abast estratègic: la seguretat de la informació ha de comptar amb el compromís i el suport de tots els nivells de l'empresa i s'ha de coordinar i integrar de manera coherent amb la resta d'iniciatives estratègiques.
- Seguretat integral: la seguretat s'entendrà com un procés integral constituït per tots els elements tècnics, humans, materials i organitzatius relacionats amb els sistemes d'informació, i s'evitarà qualsevol actuació puntual o tractament conjuntural. La seguretat de la informació s'ha de considerar part de l'operativa habitual, present i aplicada des del disseny inicial dels sistemes TIC.
- Gestió de la seguretat basada en el risc: la gestió de la seguretat basada en els riscos identificats permetrà mantenir un entorn controlat, minimitzant els riscos fins a nivells acceptables. Les mesures de seguretat s'establiran en funció dels riscos a què estiguin subjectes la informació i els seus sistemes, i seran proporcionals al risc que tracten i hauran d'estar justificades. També es tindran en compte els riscos identificats en el tractament de dades personals.
- Prevenció, detecció, resposta i conservació: amb la implementació d'accions preventives d'incidents, minimitzant les vulnerabilitats detectades, evitant que les amenaces es materialitzin i, quan es produeixin, donant-hi una resposta àgil per restaurar la informació o els serveis prestats, i garantint una conservació segura de la informació.
- Existència de línies de defensa: l'estratègia de seguretat de l'empresa es dissenya i s'implementa en capes de seguretat.
- Vigilància contínua i reavaluació periòdica: l'empresa implementa mitjans per a la detecció i la resposta a activitats o comportaments anòmals, així com altres mitjans que permeten una avaluació continuada de l'estat de seguretat dels actius. També hi haurà un procés de millora contínua per revisar i actualitzar periòdicament les mesures de seguretat, d'acord amb la seva eficàcia i l'evolució dels riscos i dels sistemes de protecció.
- Seguretat per defecte i des del disseny: els sistemes han d'estar dissenyats i configurats per garantir la seguretat per defecte. Els sistemes proporcionaran la funcionalitat mínima necessària per prestar el servei per al qual van ser dissenyats.
- Diferenciació de responsabilitats: en aplicació d'aquest principi, les funcions del Responsable de la Seguretat i del Responsable del Sistema estaran diferenciades.



6. Abast de certificació

Sistema d'informació que dóna suport als serveis de:

- Desenvolupament, explotació i suport de programari i serveis SaaS propis.
- Consultoria, desenvolupament, implementació, explotació i suport de solucions tecnològiques, a mida o basades en productes de tercers.
- Administració i suport tècnic de sistemes, infraestructura i lloc de treball, en entorns cloud i locals.

segons la Declaració d'Aplicabilitat vigent de data 18/09/2026.

7. Marc normatiu

Núm.	Legislació
1	Reglament (UE) 2016/679 del Parlament Europeu i del Consell, de 27 d'abril de 2016, relatiu a la protecció de les persones físiques pel que fa al tractament de dades personals i a la lliure circulació d'aquestes dades i pel qual es deroga la Directiva 95/46/CE (Reglament general de protecció de dades)
2	Llei orgànica 3/2018, de 5 de desembre, de protecció de dades personals i garantia dels drets digitals
3	Llei 34/2002, d'11 de juliol, de serveis de la societat de la informació i de comerç electrònic
4	Reial decret 311/2022, de 3 de maig, pel qual es regula l'Esquema Nacional de Seguretat
5	Reial decret 634/2015, de 10 de juliol, pel qual s'aprova el Reglament de l'impost sobre societats
6	Reial decret legislatiu 2/2015, de 23 d'octubre, pel qual s'aprova el text refós de la Llei de l'Estatut dels treballadors
7	Llei orgànica 10/1995, de 23 de novembre, del Codi penal
8	Llei 25/2007, de 18 d'octubre, de conservació de dades relatives a les comunicacions electròniques i a les xarxes públiques de comunicacions
9	Llei 6/2020, d'11 de novembre, reguladora de determinats aspectes dels serveis electrònics de confiança (deroga la Llei 59/2003)
10	Reial decret legislatiu 1/1996, de 12 d'abril, pel qual s'aprova el text refós de la Llei de propietat intel·lectual, que regularitza, aclareix i harmonitza les disposicions legals vigents sobre la matèria
11	Directiva (UE) 2022/2555 del Parlament Europeu i del Consell, de 14 de desembre de 2022, relativa a les mesures destinades a garantir un elevat nivell comú de ciberseguretat a tota la Unió



12	Reglament (UE) 2024/1689 del Parlament Europeu i del Consell, de 13 de juny de 2024, pel qual s'estableixen normes harmonitzades en matèria d'intel·ligència artificial
----	---

8. Responsabilitats i organització de la seguretat

a. Comitè STIC (Seguretat TIC)

Les activitats TIC es coordinen per mitjà del comitè STIC. Aquest comitè està compost de personal tècnic dels diferents departaments per a la presa de les decisions.

El Comitè de Seguretat TIC estarà format per:

CÀRREC
Direcció
Responsable de la Informació (*)
Responsable del Servei (*)
Responsable de la Seguretat (**)
Responsable del Sistema (**)

(*) Aquestes funcions poden recaure en la mateixa persona.

(**) Aquestes funcions no poden recaure en la mateixa persona.

El director presideix el Comitè STIC i és el principal responsable de:

- Fer servir el vot de qualitat per acordar les decisions oportunes quan no s'arriba a un acord dins de l'equip.
- Implementar, mantenir i millorar el Sistema de Gestió de Seguretat de la Informació (SGSI).
- Assignar els recursos necessaris i aprovar el pressupost.
- Assignar i comunicar els rols, concretament els dels propietaris dels riscos de seguretat de la informació i dels riscos de qualitat.

b. Funcions i responsabilitats

Comitè STIC

- Establir, revisar i aprovar l'abast del SGSI, així com la política de seguretat de la informació.



- Assegurar que les polítiques de seguretat de la informació, els processos, els procediments i les lleis i regulacions reflecteixen els requisits del negoci i estan alineats amb els requeriments de les parts interessades, tant internes com externes.
- Establir, revisar i aprovar els objectius del SGSI i comprovar si estan implementats i mantinguts de manera eficaç.
- Monitorar els canvis importants en la seguretat de la informació.
- Revisar els incidents de seguretat de la informació i acordar les accions necessàries, si escau.
- Aprovar les iniciatives més importants per mantenir la seguretat de la informació i el nivell de qualitat establert.
- Fer revisions per la direcció a intervals planificats.
- Assegurar que el personal és conscient de la importància de complir els requisits de seguretat, els requisits legals i reglamentaris, les obligacions contractuals, els requisits de qualitat, els nivells de qualitat i els acords de nivell de servei.

Responsable de la Informació

- Té la facultat d'establir els requisits de seguretat de la informació gestionada. Si aquesta informació inclou dades de caràcter personal, s'hauran de tenir en compte, a més, els requisits derivats de la legislació corresponent sobre protecció de dades.
- Determina els nivells de seguretat de la informació.

Responsable del Servei

- Té la facultat d'establir els requisits de seguretat dels serveis prestats.
- Determina els nivells de seguretat del servei.

Responsable de Seguretat

Responsable de definir, coordinar i verificar el compliment dels requisits de seguretat de la informació definits d'acord amb els objectius.

Les funcions del Responsable de Seguretat de la Informació són:

- Coordinar i controlar les mesures de seguretat de la informació i de protecció de dades.
- Supervisar la implantació, mantenir, controlar i verificar el compliment de:
 - L'estratègia de seguretat de la informació definida pel Comitè de Seguretat.
 - Les normes i els procediments continguts en la Política de Seguretat de la Informació.
 - Supervisar els incidents de seguretat.

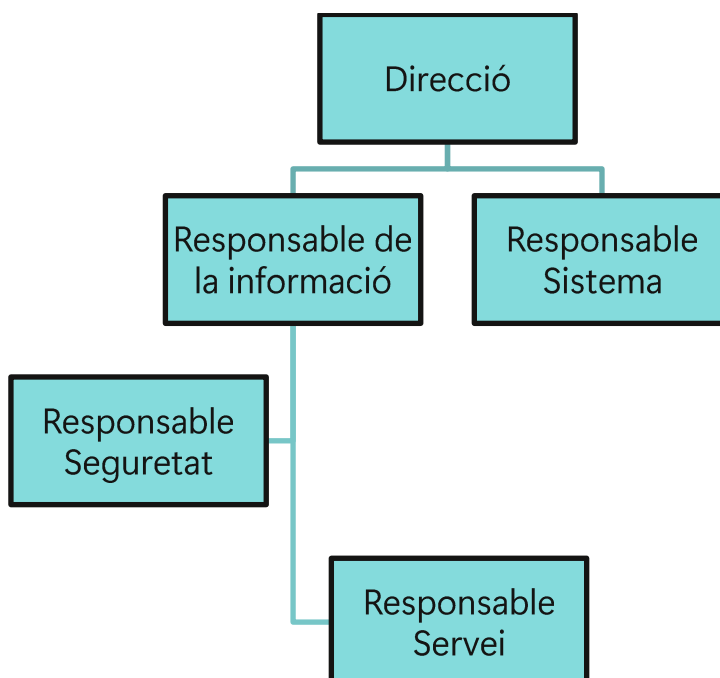


- Difondre entre el personal de l'empresa les normes i els procediments continguts en el sistema de gestió de la seguretat de la informació, així com les funcions i obligacions en matèria de seguretat de la informació.
- Supervisar les auditories internes o externes necessàries per verificar el grau de compliment de la Política de Seguretat, de la normativa que la desenvolupa i de les lleis aplicables en matèria de protecció de dades personals i de seguretat de la informació, i col·laborar-hi.
- Assessorar en matèria de seguretat de la informació les diferents àrees operatives de l'empresa.

Responsable del Sistema

- Desenvolupar, operar i mantenir el sistema d'informació durant tot el seu cicle de vida, incloent-hi les especificacions, la instal·lació i la verificació del seu funcionament correcte.
- Definir la topologia i la gestió del sistema d'informació, establint els criteris d'ús i els serveis disponibles.
- Assegurar-se que les mesures de seguretat s'integren adequadament en el marc general de seguretat.

Dependències dels rols





9. Designació i renovació dels rols de seguretat

La direcció és la màxima responsable de designar els diferents rols de seguretat. Aquesta designació es farà formalment amb l'aprovació d'aquesta política. L'original signat per la direcció l'arxivarà el Responsable de Seguretat.

L'organigrama establert reflectirà aquestes designacions.

La designació es renovarà en els casos següents:

- Baixa a mitjà o llarg termini del personal designat.
- Baixa indefinida del personal a l'empresa.
- Falta de competències.
- Criteri de Direcció atenent a raons de gestió de RH o estratègiques.

10. Resolució de conflictes

En cas de conflicte entre els diferents responsables, el Comitè de Seguretat de la Informació podrà resoldre les discrepàncies.

11. Gestió del risc

Tots els sistemes subjectes a aquesta Política hauran de fer una anàlisi de riscos, en què s'avaluin les amenaces i els riscos a què estan exposats. Aquesta anàlisi es repetirà:

- regularment, almenys una vegada l'any.
- quan es produeixin canvis en la informació gestionada.
- quan es produeixin canvis en els serveis prestats.
- quan es produeixi un incident greu de seguretat.
- quan es notifiquin vulnerabilitats greus.
- quan es produeixin modificacions en l'anàlisi de riscos de protecció de dades o en les avaluacions d'impacte.



Per harmonitzar les anàlisis de riscos, el Comitè de Seguretat de la Informació establirà una valoració de referència per als diferents tipus d'informació gestionats i per als diferents serveis prestats. El Comitè de Seguretat dinamitzarà la disponibilitat de recursos per atendre les necessitats de seguretat dels diferents sistemes i promourà inversions de caràcter horitzontal.

Es tindran en compte els riscos en protecció de dades, amb l'opinió del delegat de protecció de dades, si n'hi ha, i es coordinaran els plans de tractament del risc.

12. Recursos

Per aplicar efectivament la Política de Seguretat de la Informació a l'empresa, la direcció hi destinarà els recursos necessaris per al seu bon desenvolupament, tant en les activitats d'implantació com en les d'operació i millora de la política i dels controls de seguretat de la informació que s'estableixin en cada moment.

La protecció dels actius d'informació de l'empresa i dels seus clients és vital per a l'alineament correcte amb els objectius de negoci. Amb aquesta finalitat, s'ha establert un Sistema de Gestió de Seguretat de la Informació (SGSI) que implementa tots els processos i controls necessaris per establir la manera com es protegeixen els actius d'informació.

El Sistema de Gestió de Seguretat de la Informació s'actualitza i millora contínuament per satisfer les necessitats del negoci, dels clients i de les parts interessades; s'estableixen nous objectius periòdicament i s'avaluen regularment els processos de negoci.

13. Dades de caràcter personal

L'empresa tracta dades de caràcter personal, tal com es descriu en el Registre d'Activitats del Tractament. L'empresa haurà d'avaluar els riscos relacionats amb les dades personals tractades i proposar un pla d'actuació per corregir els riscos que superin el llindar autoritzat.

L'anàlisi de riscos es reavaluarà periòdicament i, en tot cas, quan es detecti un tractament d'alt risc; si escau, s'haurà de fer una avaluació d'impacte. La implementació del pla de tractament del risc es coordinarà amb el de l'ENS, així com la resta de procediments o normes de seguretat amb els derivats de les obligacions en matèria de protecció de dades, especialment en el control dels prestadors de serveis o en la resposta a incidents o bretxes de dades personals.



14. Desenvolupament de la política de seguretat de la informació

Aquesta Política de Seguretat de la Informació complementa altres polítiques de l'empresa en diferents matèries i s'hi integra:

- Política de seguretat (ISO 27001)

Aquesta Política es desenvoluparà per mitjà de normativa de seguretat que tracti aspectes específics. La normativa de seguretat estarà a disposició de tots els membres de l'empresa que l'hagin de conèixer, en particular dels que utilitzin, operin o administrin els sistemes d'informació i comunicacions.

La normativa de seguretat estarà disponible per diversos mitjans a disposició dels usuaris a la intranet de l'empresa.

Els usuaris podran disposar de formació específica sobre seguretat de la informació.

Els proveïdors seran avaluats i haurien de disposar de personal amb la formació adequada als serveis que prestin.

15. Obligacions del personal

Tots els membres de l'empresa tenen l'obligació de conèixer i complir aquesta Política de Seguretat de la Informació i les normes, els procediments o les guies que la desenvolupin. És responsabilitat de l'empresa, a través del Comitè de Seguretat i de l'àrea de personal, disposar els mitjans necessaris perquè la informació arribi a les persones afectades.

Tots els membres de l'empresa assistiran a una sessió de conscienciació en matèria de seguretat de la informació almenys una vegada l'any. S'establirà un programa de conscienciació contínua per atendre tots els membres de l'empresa, en particular els de nova incorporació.

Les persones amb responsabilitat en l'ús, l'operació o l'administració de sistemes TIC rebran formació per al maneig segur dels sistemes en la mesura que la necessitin per fer la seva feina. La formació serà obligatòria abans d'assumir una responsabilitat, tant si es tracta de la primera assignació com d'un canvi de lloc de treball o de responsabilitats.



16. Terceres parts / prestadors de serveis / proveïdors de solucions

Quan l'empresa presti serveis a altres entitats o gestioni informació d'altres entitats, les farà partícips d'aquesta Política de Seguretat de la Informació, sense perjudici de respectar les obligacions de la normativa de protecció de dades si actua com a encarregada del tractament en la prestació d'aquests serveis. S'establiran canals de notificació i de coordinació entre els comitès de seguretat respectius i procediments d'actuació per reaccionar davant d'incidents de seguretat. A més, el Responsable de Seguretat (o la persona en qui delegui) serà el punt de contacte (POC).

Quan l'empresa utilitzi serveis de tercers o cedeixi informació a tercers, els farà partícips d'aquesta Política de Seguretat i de la normativa de seguretat que afecti aquests serveis o aquesta informació, sense perjudici del compliment d'altres obligacions en matèria de protecció de dades. En la contractació de prestadors de serveis o en l'adquisició de productes es tindrà en compte l'obligació de l'adjudicatari de complir l'ENS.

En l'adquisició de drets d'ús d'actius al núvol, es tindran en compte els requisits establerts en les mesures de seguretat de l'annex II i en les guies de desenvolupament.

Aquesta tercera part quedarà subjecta a les obligacions establertes en la normativa esmentada i podrà desenvolupar els seus propis procediments operatius per complir-la, de manera que l'empresa els pugui supervisar o sol·licitar-ne evidències de compliment, fins i tot mitjançant auditories de segona o tercera part. S'establiran procediments específics de notificació i resolució d'incidències, que s'hauran de canalitzar a través del POC dels tercers implicats i, a més, quan afectin dades personals, a través del delegat de protecció de dades. Els tercers garantiran que el seu personal està adequadament conscienciat en matèria de seguretat, almenys al mateix nivell que l'establert en aquesta Política o el que es pugui exigir específicament en el contracte.

Quan algun aspecte de la Política no pugui ser satisfet per un tercer tal com es requereix en els paràgrafs anteriors, el Responsable de la Seguretat emetrà un informe que precisi els riscos en què s'incorre i la manera de tractar-los. Aquest informe l'hauran d'aprovar els responsables de la informació i dels serveis afectats abans de l'inici de la contractació o, si escau, de l'adjudicació. L'informe es traslladarà al representant de l'empresa, que haurà d'autoritzar que continuï la tramitació de la contractació del tercer, assumint els riscos detectats.

Quan l'empresa adquireixi, desenvolupi o implanti un sistema d'intel·ligència artificial, a més de complir el que estableix la normativa vigent en la matèria, haurà de disposar de l'informe del Responsable de la Seguretat, que consultarà el Responsable de la Informació i el del Servei i, quan sigui necessari, el del Sistema. El delegat de protecció de dades també n'haurà d'emetre el seu parer.



17. Gestió d'incidents de seguretat

L'empresa disposarà d'un procediment per a la gestió àgil dels esdeveniments i incidents de seguretat que suposin una amenaça per a la informació i els serveis.

Aquest procediment s'integrarà amb altres procediments relacionats amb els incidents de seguretat d'altres normes sectorials, com la de protecció de dades personals o qualsevol altra que afecti l'organisme, per coordinar la resposta des dels diferents enfocaments i comunicar-ho als diferents organismes de control sense dilacions indegudes i, quan calgui, a les Forces i Cossos de Seguretat de l'Estat o als jutjats.

18. Categoria de seguretat

La categoria de seguretat requerida és MITJANA, dins del marc establert en l'article 40 i els criteris generals prescrits en l'annex I de l'ENS. Alguns dels criteris que determinen aquest nivell són que el procés està totalment definit i que el catàleg de processos es manté actualitzat i garanteix la coherència de les actuacions entre les diferents parts de l'organització.

A més, hi ha normativa establerta i procediments per poder reaccionar davant de qualsevol incident de seguretat, que s'actualitzen i es mantenen regularment. Així mateix, hi ha una alta coordinació entre els departaments i els projectes duts a terme.

El Comitè STIC preveu la possibilitat de modificar el nivell de seguretat requerit.

Els principis de la Política de Seguretat de la Informació són assumits i impulsats per la direcció, que proporciona els mitjans necessaris i dota els treballadors dels recursos suficients per complir-los, i els fa públics a través d'aquesta Política de Seguretat.

19. Aprovació de la política i entrada en vigor

Les modificacions d'aquesta Política que suposin canvis o adaptacions davant d'ineficiències les farà el Comitè de Seguretat de la Informació, que l'haurà de revisar anualment.

En cas que els canvis suposin una modificació substancial o afectin els principis o les responsabilitats designades, el Comitè de Seguretat proposarà els canvis, que haurà d'aprovar, si escau, la persona o l'òrgan amb les competències corresponents.



La substitució de la Política la promourà el Comitè de Seguretat de la Informació i la ratificarà la persona o l'òrgan amb les competències corresponents, i se n'informarà adequadament les persones interessades pels mateixos canals utilitzats per a la seva difusió.

Data: 7/10/2026

Aprovat per la direcció