



Política de Seguretat de la Informació

Esquema Nacional de Seguridad

Data: 20/01/2026

Versió 0.1

Ús de la informació Interna

iqembu: proximitat igualtat i equip	POLÍTICA DE SEGURETAT DE LA INFORMACIÓ	20/01/2026 Pàgina 2 de 12
Classificació: Interna		Versió 0.1

Índex

1. Aprovació i entrada en vigor.....	4
2. Missió de l'organització.....	4
3. Abast	4
4. Objectius.....	5
5. Marc normatiu.....	5
6. Desenvolupament.....	6
7. Organització de seguretat.....	6
8. Comitè de Seguretat.....	7
9. Gestió de riscos.....	7
10. Gestió de personal.....	8
11. Professionalitat i seguretat dels recursos humans.....	8
12. Autorització i control d'accés als Sistemes d'Informació	9
13. Protecció de les instal·lacions.....	10
14. Adquisició de productes	10
21. Millora contínua del procés de seguretat	12

iqembu proximitat igualtat i equip	POLÍTICA DE SEGURETAT DE LA INFORMACIÓ	20/01/2026 Pàgina 3 de 12
Classificació: Interna		Versió 0.1

Control de Versions

Versió	Autor	Revisió	Aprovat	Data	Descripció
0.1	Responsable de Seguretat		Direcció	20/01/2026	Versió inicial

	POLÍTICA DE SEGURETAT DE LA INFORMACIÓ	20/01/2026 Pàgina 4 de 12
Classificació: Interna		Versió 0.1

1. Aprovació i entrada en vigor

Aquesta Política de Seguretat de la Informació és efectiva des de la data de signatura i fins que sigui substituïda per una nova Política.

2. Missió de l'organització

IQEMBU és una empresa dedicada a la gestió de projectes en l'àmbit sociocultural, la cultura de proximitat, l'educació i el lleure, així com a la consultoria i l'assessorament especialitzats en grups socials.

IQEMBU, per assolir els seus objectius, assumeix el compromís amb la seguretat de la informació, compromentent-se amb la seva adequada gestió, amb la finalitat d'oferir a tots els seus grups d'interès les màximes garanties en relació amb la seguretat de la informació utilitzada.

Aquests sistemes han de ser administrats amb diligència, adoptant les mesures adequades per protegir-los davant de danys accidentals o deliberats que puguin afectar la disponibilitat, integritat o confidencialitat de la informació tractada o dels serveis prestats.

L'objectiu de la seguretat de la informació és garantir la qualitat de la informació i la prestació continuada dels serveis, actuant preventivament, supervisant l'activitat diària i reaccionant amb celeritat davant dels incidents.

Els sistemes TIC han d'estar protegits contra amenaces d'evolució ràpida amb potencial d'incidir en la confidencialitat, integritat, disponibilitat, ús previst i valor de la informació i dels serveis. Per defensar-se d'aquestes amenaces, es requereix una estratègia que s'adapti als canvis en les condicions de l'entorn per garantir la prestació continuada dels serveis. Això implica que els departaments han d'aplicar les mesures mínimes de seguretat exigides per l'Esquema Nacional de Seguretat, així com fer un seguiment continu dels nivells de prestació dels serveis, seguir i analitzar les vulnerabilitats reportades i preparar una resposta efectiva davant dels incidents per garantir la continuïtat dels serveis prestats.

Els diferents departaments han d'assegurar que la seguretat TIC és una part integral de cada etapa del cicle de vida del sistema, des de la seva concepció fins a la seva retirada de servei, passant per les decisions de desenvolupament o adquisició i les activitats d'explotació. Els requisits de seguretat i les necessitats de finançament han de ser identificats, tant per als productes que desenvolupa i els seus serveis associats com pel que fa al programari base adquirit de tercers.

Els departaments han d'estar preparats per prevenir, detectar, reaccionar i recuperar-se d'incidents, d'acord amb l'article 8 de l'ENS (article 8. Prevenció, detecció, resposta i conservació).

3. Abast

iqembu: proximitat igualtat i equip	POLÍTICA DE SEGURETAT DE LA INFORMACIÓ	20/01/2026 Pàgina 5 de 12
Classificació: Interna		Versió 0.1

Aquesta política s'aplica a tots els sistemes TIC de l'entitat i a tots els membres de l'organització implicats en serveis i projectes destinats al sector públic que requereixin l'aplicació de l'ENS, sense excepcions.

4. Objectius

Per tot el que s'ha exposat anteriorment, la Direcció estableix els objectius següents de seguretat de la informació:

- Proporcionar un marc per augmentar la capacitat de resistència o resiliència per donar una resposta eficaç.
- Assegurar la recuperació ràpida i eficient dels serveis davant de qualsevol desastre físic o contingència que pugui produir-se i que posi en risc la continuïtat de les operacions.
- Prevenir incidents de seguretat de la informació en la mesura que sigui tècnica i econòmicament viable així com mitigar els riscos de seguretat de la informació generats per les nostres activitats.
- Garantir la confidencialitat, integritat, disponibilitat, autenticitat i traçabilitat de la informació.

5. Marc normatiu

Un dels objectius ha de ser complir els requisits legals aplicables i qualsevol altre requisit que subscrivim, a més dels compromisos adquirits amb els clients, així com la seva actualització contínua. Amb aquesta finalitat, el marc legal i regulador en què desenvolupem les nostres activitats és:

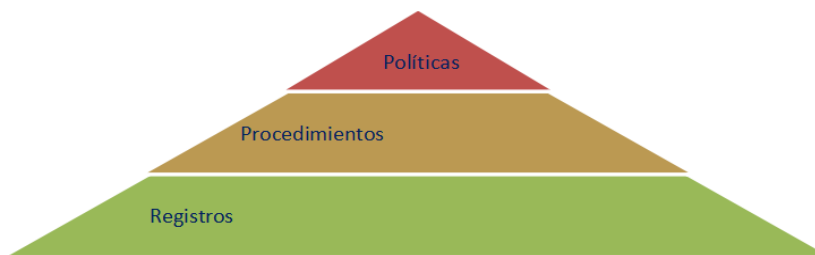
- REGLAMENT (UE) 2016/679 DEL PARLAMENT EUROPEU I DEL CONSELL de 27 d'abril de 2016 relatiu a la protecció de les persones físiques pel que fa al tractament de dades personals i a la lliure circulació d'aquestes dades.
- Llei orgànica 3/2018, de 5 de desembre, de protecció de dades personals i garantia dels drets digitals.
- Reial decret legislatiu 1/1996, de 12 d'abril, pel qual s'aprova el text refós de la Llei de propietat intel·lectual.
- Llei 2/2019, d'1 de març, per la qual es modifica el text refós de la Llei de propietat intel·lectual, aprovat pel Reial decret legislatiu 1/1996, de 12 d'abril, i s'incorporen a l'ordenament jurídic espanyol la Directiva 2014/26/UE i la Directiva (UE) 2017/1564.
- Reial decret 311/2022, de 3 de maig, pel qual es regula l'Esquema Nacional de Seguretat.
- Llei 34/2002, d'11 de juliol, de serveis de la societat de la informació i de comerç electrònic (LSSI).
- Llei 40/2015, d'1 d'octubre, de règim jurídic del sector públic.
- Llei 39/2015, d'1 d'octubre, del procediment administratiu comú de les administracions públiques.
- Resolucions de la Secretaria d'Estat de Funció Pública relatives a les Instruccions Tècniques de Seguretat de l'ENS (informe de l'estat de la seguretat, conformitat amb l'ENS, auditoria i notificació d'incidentes).
- REGLAMENT (UE) núm. 910/2014 del Parlament Europeu i del Consell, de 23 de juliol de 2014, relatiu a la identificació electrònica i els serveis de confiança per a les transaccions electròniques al mercat interior.

iqembu: proximitat igualtat i equip	POLÍTICA DE SEGURETAT DE LA INFORMACIÓ	20/01/2026 Pàgina 6 de 12
Classificació: Interna		Versió 0.1

6. Desenvolupament

Per assolir aquests objectius és necessari:

- Millorar contínuament el nostre sistema de seguretat de la informació.
- Identificar les amenaces potencials i l'impacte en les operacions de negoci que puguin causar.
- Preservar els interessos de les parts interessades principals (clients, accionistes, empleats i proveïdors), la reputació, la marca i les activitats de creació de valor.
- Treballar conjuntament amb els nostres subministradors i subcontractistes per millorar la prestació de serveis TIC, la continuïtat dels serveis i la seguretat de la informació.
- Avaluar i garantir la competència tècnica del personal i assegurar-ne la motivació, proporcionant la formació i la comunicació interna adequades.
- Garantir el correcte estat de les instal·lacions i l'equipament adequat.
- Garantir l'anàlisi contínua de tots els processos rellevants i establir les millores pertinents.
- Estructurar el sistema de gestió de manera que sigui fàcil de comprendre. Té la següent estructura:



La gestió del sistema s'encomana al Responsable de Sistemes Informàtics i estarà disponible en el sistema d'informació en un repositori accessible segons els perfils d'accés definits.

7. Organització de seguretat

La responsabilitat essencial recau en la Direcció General, responsable d'organitzar funcions i responsabilitats i facilitar els recursos adequats per assolir els objectius de l'ENS. Els directius també han de donar exemple complint les normes de seguretat establertes.

Aquests principis són assumits per la Direcció, que disposa els mitjans necessaris i dota el personal dels recursos suficients, fent-los públics mitjançant aquesta Política.

Rols de seguretat definits:

- Responsable de la informació (RINFO): decisions relatives a la informació tractada.
- Responsable dels serveis (RSER): coordinació de la implantació i millora contínua.
- Responsable de la seguretat (RSEG): idoneïtat de mesures tècniques i tecnologia.
- Responsable del sistema (RSIS): coordinació de la implantació i millora contínua.

iqembu: proximitat igualtat i equip	POLÍTICA DE SEGURETAT DE LA INFORMACIÓ	20/01/2026 Pàgina 7 de 12
Classificació: Interna		Versió 0.1

- Direcció: recursos necessaris i lideratge del sistema.

Aquesta definició es completa als perfils de lloc i al registre de responsables, rols i responsabilitats.

8. Comitè de Seguretat

El procediment per a la seva designació i renovació serà la ratificació en el Comitè de Seguretat.

El comitè per a la gestió i coordinació de la seguretat és l'òrgan amb major responsabilitat dins del sistema de gestió de seguretat de la informació, de manera que totes les decisions més importants relacionades amb la seguretat s'acorden en aquest comitè. Els membres del Comitè de Seguretat de la Informació són:

- Responsable de la Informació
- Responsable dels Serveis
- Responsable de la Seguretat
- Responsable del Sistema
- Direcció de l'empresa (socis-administradors)

Aquests membres són designats pel comitè, únic òrgan que pot nomenar-los, renovar-los i cessar-los.

El Comitè de Seguretat és un òrgan autònom, executiu i amb autonomia per a la presa de decisions, i no ha de subordinar la seva activitat a cap altre element de la nostra empresa.

L'organització de la seguretat de la informació es desenvolupa en el document complementari; entre les seves funcions es destaca la de vetllar per l'ENS i, entre les seves tasques principals, sobresurt la resolució de conflictes, ja que les diferències de criteri que poguessin derivar en un conflicte es tractaran en el si del Comitè de Seguretat i prevaldrà, en tot cas, el criteri de la Direcció General.

L'organització de la seguretat de la informació es desenvolupa en el document complementari a aquesta Política d'Organització de la Seguretat. Aquesta política es complementa amb la resta de polítiques, procediments i documents vigents per desenvolupar el nostre sistema de gestió.

9. Gestió de riscos

Tots els sistemes subjectes a aquesta Política han de realitzar una anàlisi de riscos, avaluant les amenaces i els riscos als quals estan exposats. Aquesta anàlisi es revisa regularment:

com a mínim un cop l'any;

- quan canviï la informació gestionada;
- quan canviïn els serveis prestats;
- quan es produeixi un incident greu de seguretat;
- quan es reportin vulnerabilitats greus.

iqembu: proximitat igualtat i equip	POLÍTICA DE SEGURETAT DE LA INFORMACIÓ	20/01/2026 Pàgina 8 de 12
Classificació: Interna		Versió 0.1

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

Per a la realització de l'anàlisi de riscos es tindrà en compte la metodologia d'anàlisi de riscos desenvolupada en el procediment d'Anàlisi de Riscos.

10. Gestió de personal

Tots els membres d'IQEMBU tenen l'obligació de conèixer i complir aquesta Política de Seguretat de la Informació i la Normativa de Seguretat, i és responsabilitat del Comitè de Seguretat TIC disposar dels mitjans necessaris perquè la informació arribi a les persones afectades.

Tots els membres d'IQEMBU assistiran a una sessió de conscienciació en matèria de seguretat TIC com a mínim un cop l'any. S'establirà un programa de conscienciació continuada per atendre tots els membres d'IQEMBU, en particular els de nova incorporació.

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

11. Professionalitat i seguretat dels recursos humans

Aquesta Política s'aplica a tot el personal d'IQEMBU i al personal extern que realitza tasques dins de l'empresa. RRHH inclourà funcions de seguretat de la informació en les descripcions dels llocs de treball, informará tot el personal contractat de les seves obligacions pel que fa al compliment de la Política de Seguretat de la Informació, gestionarà els Compromisos de Confidencialitat amb el personal i coordinarà les tasques de capaciació dels usuaris respecte d'aquesta Política.

El Responsable de Gestió de la Seguretat (RGS) és responsable de monitorar, documentar i analitzar els incidents de seguretat reportats, així com de comunicar-se amb el Comitè de Seguretat de la Informació i amb els propietaris de la informació.

El Comitè de Seguretat de la Informació serà responsable d'implementar els mitjans i canals necessaris perquè el Responsable de Gestió de la Seguretat (RGS) gestioni informes d'incidentes i anomalies del sistema. El Comitè també n'estarà al corrent, supervisarà la investigació, l'evolució de la informació i promourà la resolució dels incidents de seguretat de la informació.

iqembu: proximitat igualtat i equip	POLÍTICA DE SEGURETAT DE LA INFORMACIÓ	20/01/2026 Pàgina 9 de 12
Classificació: Interna		Versió 0.1

El Responsable de Gestió de la Seguretat (RGS) participarà en la preparació del Compromís de Confidencialitat que signaran els empleats i tercers que exerceixin funcions a IQEMBU, en l'assessorament sobre les sancions aplicables per incompliment d'aquesta Política i en el tractament d'incidents de seguretat de la informació.

Tot el personal d'IQEMBU és responsable d'informar sobre les debilitats i incidents de seguretat de la informació que es detectin oportunament.

Professionalitat dels recursos humans:

- Determinar la competència necessària del personal per dur a terme la feina que afecta la Seguretat de la Informació.
- Cal assegurar que les persones siguin competents sobre la base d'una educació, capacitació o experiència adequades.
- Demostrar, mitjançant la informació documentada necessària, la competència del personal en matèria de Seguretat de la Informació.

Els objectius de controlar la seguretat del personal són:

- Reduir els riscos d'error humà, posada en marxa d'irregularitats, ús indegut d'instal·lacions i recursos, i maneig no autoritzat de la informació.
- Explicar les responsabilitats de seguretat en l'etapa de selecció i incloure-les en els acords a signar, i verificar-ne el compliment durant l'exercici de les tasques.
- Assegurar que els usuaris siguin conscients de les amenaces i preocupacions de seguretat de la informació i estiguin capacitats per donar suport a la Política de Seguretat de la Informació en el desenvolupament de les seves tasques habituals.
- Establir compromisos de confidencialitat amb tot el personal i amb usuaris fora de les instal·lacions de processament d'informació.
- Establir eines i mecanismes per promoure la comunicació de debilitats de seguretat existents i d'incidents, amb la finalitat de minimitzar-ne els efectes i prevenir-ne la reincidència.

12. Autorització i control d'accés als Sistemes d'Informació

El control d'accés als sistemes d'informació té per objectiu:

- Evitar l'accés no autoritzat a sistemes d'informació, bases de dades i serveis d'informació.
- Implementar la seguretat en l'accés dels usuaris mitjançant tècniques d'autenticació i autorització.
- Controlar la seguretat en la connexió entre la xarxa d'IQEMBU i altres xarxes públiques o privades.
- Revisar els esdeveniments crítics i les activitats realitzades pels usuaris en els sistemes.
- Conscienciar sobre la responsabilitat en l'ús de contrasenyes i equips.
- Garantir la seguretat de la informació quan s'utilitzen ordinadors portàtils i ordinadors personals per al treball remot.

iqembu: proximitat igualtat i equip	POLÍTICA DE SEGURETAT DE LA INFORMACIÓ	20/01/2026 Pàgina 10 de 12
Classificació: Interna		Versió 0.1

13. Protecció de les instal·lacions

Els objectius d'aquesta política en matèria de protecció de les instal·lacions són: prevenir l'accés no autoritzat, danys i interferències a la seu, les instal·lacions i la informació d'IQEMBU.

- Protegir l'equip crític de processament d'informació d'IQEMBU, ubicant-lo en àrees protegides i dins d'un perímetre de seguretat definit, amb mesures de seguretat i controls d'accés adequats. Així mateix, contemplar la seva protecció durant el trasllat i quan romangui fora de les àrees protegides per manteniment o altres motius.
- Controlar els factors ambientals que podrien perjudicar el bon funcionament dels equips informàtics que allotgen la informació d'IQEMBU.
- Implementar mesures per protegir la informació gestionada pel personal a les oficines, en el marc normal de les seves tasques habituals.
- Proporcionar una protecció proporcional als riscos identificats.

Aquesta Política s'aplica a tots els recursos físics relacionats amb els sistemes d'informació d'IQEMBU: instal·lacions, equips, cablejat, expedients, mitjans d'emmagatzematge, etc.

El Responsable de Gestió de la Seguretat (RGS), juntament amb els titulars de la informació, si escau, definirà les mesures de seguretat física i ambiental per protegir els actius crítics sobre la base d'una anàlisi de riscos i en supervisarà l'aplicació. També verificarà el compliment de les disposicions de seguretat física i mediambiental.

Els responsables dels diferents departaments definiran els nivells d'accés físic del personal d'IQEMBU a les àrees restringides sota la seva responsabilitat. Els propietaris de la informació autoritzaran formalment el treball fora del lloc amb informació del negoci als empleats d'IQEMBU quan ho considerin oportú.

Tot el personal d'IQEMBU és responsable del compliment de la política de pantalla neta i escriptori net, per protegir la informació relacionada amb el treball diari a les oficines.

14. Adquisició de productes

Els diferents departaments han d'assegurar que la seguretat TIC és una part integral de cada etapa del cicle de vida del sistema, des de la concepció fins a la retirada de servei, passant per les decisions de desenvolupament o adquisició i les activitats d'explotació. Els requisits de seguretat i les necessitats de finançament han de ser identificats i inclosos en la planificació, en la sol·licitud d'ofertes i en els plecs de licitació per a projectes TIC.

D'altra banda, es tindrà en compte la seguretat de la informació en l'adquisició i manteniment dels sistemes d'informació, limitant i gestionant el canvi.

iqembu: proximitat igualtat i equip	POLÍTICA DE SEGURETAT DE LA INFORMACIÓ	20/01/2026 Pàgina 11 de 12
Classificació: Interna		Versió 0.1

15. Seguretat per defecte

IQEMBU considera estratègic que els processos integrin la seguretat de la informació com a part del seu cicle de vida. Els sistemes d'informació i els serveis han d'incloure la seguretat per defecte des de la seva creació fins a la seva retirada, incorporant la seguretat en les decisions de desenvolupament i/o adquisició i en totes les activitats d'exploració, establint-la com un procés integral i transversal.

16. Integritat i actualització del sistema

IQEMBU es compromet a garantir la integritat del sistema mitjançant un procés de gestió de canvis que permeti controlar l'actualització dels elements físics o lògics mitjançant autorització prèvia a la seva instal·lació al sistema. Aquesta avaluació serà duta a terme principalment per la direcció tècnica, que valorarà l'impacte en la seguretat del sistema abans de fer els canvis i controlarà documentalment aquells canvis que es considerin importants o amb implicacions en la seguretat dels sistemes.

Mitjançant revisions periòdiques de seguretat s'avaluarà l'estat de seguretat dels sistemes, en relació amb les especificacions dels fabricants, les vulnerabilitats i les actualitzacions que els afectin, reaccionant amb diligència per gestionar el risc a la vista del seu estat de seguretat.

17. Protecció de la informació emmagatzemada i en trànsit

IQEMBU estableix mesures de protecció per a la Seguretat de la Informació emmagatzemada o en trànsit a través d'entorns insegurs. Es consideraran entorns insegurs els equips portàtils, dispositius perifèrics, suports d'informació i comunicacions sobre xarxes obertes o amb xifrat feble.

18. Prevenció de sistemes d'informació interconnectats

IQEMBU estableix mesures de protecció per a la Seguretat de la Informació especialment per protegir el perímetre, en particular si es connecta a xarxes públiques, especialment si s'utilitzen totalment o principalment per a la prestació de serveis de comunicacions electròniques disponibles per al públic.

En tot cas, s'analitzaran els riscos derivats de la interconnexió del sistema, a través de xarxes, amb altres sistemes, i se'n controlarà el punt d'unió.

19. Registres d'activitat

IQEMBU registrarà les activitats dels usuaris, retenint la informació necessària per monitorar, analitzar, investigar i documentar activitats indegudes o no autoritzades, permetent identificar en cada moment la persona que actua.

Els objectius principals de la gestió d'incidents són:

	POLÍTICA DE SEGURETAT DE LA INFORMACIÓ	20/01/2026 Pàgina 12 de 12
Classificació: Interna		Versió 0.1

- Establir un sistema de detecció i reacció davant codi maliciós.
- Disposar de procediments de gestió d'incidents de seguretat i de debilitats detectades en els elements del sistema d'informació.

Aquests procediments cobriran mecanismes de detecció, criteris de classificació, procediments d'anàlisi i resolució, així com els canals de comunicació a les parts interessades i el registre de les actuacions.

- Aquest registre s'utilitza per a la millora contínua de la seguretat del sistema.
- Garantir que els serveis TIC tornin a tenir un rendiment òptim.
- Reduir els possibles riscos i impactes que pugui causar l'incident.
- Vetllar per la integritat dels sistemes en cas d'un incident de seguretat.
- Comunicar l'impacte d'un incident tan aviat com es detecti per activar l'alarma i posar en pràctica un pla de comunicació empresarial adequat.
- Promoure l'eficiència empresarial.

20. Continuïtat de l'activitat

IQEMBU, amb l'objectiu de garantir la continuïtat de les activitats, estableix mesures perquè els sistemes disposin de còpies de seguretat i estableix els mecanismes necessaris per garantir la continuïtat de les operacions en cas de pèrdua dels mitjans habituals de treball.

21. Millora contínua del procés de seguretat

IQEMBU estableix un procés de millora contínua de la seguretat de la informació aplicant els criteris i la metodologia establerta a l'Esquema Nacional de Seguretat.

Barcelona, 22 de gener de 2026

Direcció General