Unió de Federacions
Esportives de Catalunya

Rambla Catalunya, 81 pral. · 08008 Barcelona
Tel. 93 487 45 75 · www.ufec.cat

Política de Seguretat de la Informació

Document d'Ús Públic

Rambla Catalunya, 81 pral. · 08008 Barcelona
Tel. 93 487 45 75 · www.ufec.cat

Control de versions

Data:	Realitzat per:	Versió:	Descripció de la versió:
17/11/2025	Resp. Seguretat	1.0	Data Inicial

Realitzat per:	Revisat per:	Aprovat per:
Resp. Seguretat	Resp. Seguretat	Direcció

Índex

1. Aprovació i Entrada en Vigor
2. Missió de l'organització
3. Abast
4. Objectius
5. Marc normatiu
6. Desenvolupament
7. Organització de seguretat
8. Comitè de Seguretat
9. Gestió de Riscos
10. Gestió de Personal
11. Professionalitat i seguretat dels recursos humans
12. Autorització i control d'accés als Sistemes d'Informació
13. Protecció de les instal·lacions
14. Adquisició de productes
15. Seguretat per defecte
16. Integritat i actualització del sistema
17. Protecció de la informació emmagatzemada i en trànsit
18. Prevenció de sistemes d'informació interconnectats
19. Continuïtat de l'activitat
20. Millora contínua del procés de seguretat

1. Aprovació i Entrada en Vigor

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

2. Missió de l'organització

La Unió de Federacions Esportives de Catalunya i les seves participades, d'ara endavant UFEC, per assolir els seus objectius, assumeix el seu compromís amb la seguretat de la informació, comprometent-se a la gestió adequada d'aquesta, amb la finalitat d'oferir a tots els seus grups d'interès les majors garanties al voltant de la seguretat de la informació utilitzada.

La Unió de Federacions Esportives de Catalunya és un òrgan de solidaritat entre les Federacions esportives catalanes i el conjunt de l'esport a Catalunya. Així mateix, és un òrgan de representació de l'esport a Catalunya i un òrgan de debat i solució de problemes o qüestions interfederatives. Finalment, és un òrgan de formació en ensenyament esportius.

Per aconseguir aquest objecte fundacional, la Unió de Federacions Esportives de Catalunya gestiona instal·lacions esportives municipals, directament o a través de les seves participades, mitjançant concessions administratives públiques.

Aquests sistemes han de ser administrats amb diligència, prenent les mesures adequades per protegir-los davant danys accidentals o deliberats que puguin afectar la disponibilitat, integritat o confidencialitat de la informació tractada o els 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 promptitud als incidents.

Els sistemes TIC han d'estar protegits contra amenaces de ràpida evolució amb potencial per incidir en la confidencialitat, integritat, disponibilitat, ús previst i valor de la informació i els 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 contínua dels serveis.

Això implica que els departaments han d'aplicar les mesures mínimes de seguretat exigides per l'Esquema Nacional de Seguretat, així com realitzar un seguiment continu dels nivells de prestació de serveis, seguir i analitzar les vulnerabilitats reportades, i preparar una resposta efectiva als incidents per garantir la continuïtat dels serveis prestats.

Els diferents departaments han d'assegurar-se 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 i inclosos en la planificació, en la sol·licitud d'ofertes, i en plecs de licitació per a projectes de TIC.

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

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 d'ENS, sense excepcions.

4. Objectius

Per tot l'anteriorment exposat, la Direcció estableix els següents objectius 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 qualsevol desastre físic o contingència que pogués ocórrer i que posés 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 el de complir amb requisits legals aplicables i amb qualssevol altres requisits que subscrivim a més dels compromisos adquirits amb els clients, així com l'actualització contínua dels mateixos. Per a això, el marc legal i regulador en el qual 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, 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 pel qual s'incorporen a l'ordenament jurídic espanyol la Directiva 2014/26/UE del Parlament Europeu i del Consell, de 26 de febrer de 2014, i

la Directiva (UE) 2017/1564 del Parlament Europeu i del Consell, de 13 de setembre de 2017.
- 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 39/2015, d'1 d'octubre, del Procediment Administratiu Comú de les Administracions Públiques.
- Llei 40/2015, d'1 d'octubre, de Règim Jurídic del Sector Públic.

6. Desenvolupament

Per poder aconseguir aquests objectius cal:

- Millorar contínuament el nostre sistema de seguretat de la informació.
- Identificar les amenaces potencials, així com l'impacte en les operacions de negoci que aquestes amenaces, en cas de materialitzar-se, puguin causar.
- Preservar els interessos de les seves principals parts interessades (clients, accionistes, empleats i proveïdors), la reputació, la marca i les activitats de creació de valor.
- Treballar de forma conjunta amb els nostres subministradors i subcontractistes amb la finalitat de millorar la prestació de serveis de TI, la continuïtat dels serveis i la seguretat de la informació, que repercuteixin en una major eficiència de la nostra activitat.
- Avaluar i garantir la competència tècnica del personal, així com assegurar la motivació adequada d'aquest per a la seva participació en la millora contínua dels nostres processos, proporcionant la formació i la comunicació interna adequada perquè desenvolupin bones pràctiques definides en el sistema.
- Garantir el correcte estat de les instal·lacions i l'equipament adequat, de tal forma que estiguin en correspondència amb l'activitat, objectius i metes de l'empresa.
- Garantir una anàlisi de manera contínua de tots els processos rellevants, establint-se les millores pertinents en cada cas, en funció dels resultats obtinguts i dels objectius establerts.
- Estructurar el nostre sistema de gestió de forma que sigui fàcil de comprendre. El nostre sistema de gestió té la següent estructura:

La gestió del nostre sistema s'encomana al Responsable de Sistemes Informàtics i el sistema estarà disponible en el nostre sistema d'informació en un repositori, al qual es pot accedir segons els perfils d'accés concedits segons el nostre procediment en vigor de gestió dels accessos.

La documentació referida a la seguretat del sistema es troba estructurada en carpetes dins del servidor de fitxers de la companyia, dividida en subcarpetes anomenades per punts de norma i marcs d'operació, les quals recullen els diferents procediments, registres i evidències, amb accés restringit per al personal de la companyia, no podent accedir personal extern no autoritzat.

La documentació de seguretat s'estructura en:

- Política de Seguretat.
- Normativa de seguretat: documents que descriuen l'ús d'equips, serveis i instal·lacions. Descriuen el que es considera ús indegut, la responsabilitat del personal respecte al compliment o violació de la normativa, drets, deures i mesures disciplinàries d'acord amb la legislació vigent.
- Documents específics: documentació de seguretat desenvolupada segons les guies CCN-STIC que resultin d'aplicació.
- Procediments de seguretat: documents que detallen com operar els elements del sistema.

Aquesta política es complementa amb la resta de les polítiques, procediments i documents en vigor per desenvolupar el nostre sistema de gestió.

7. Organització de seguretat

La responsabilitat essencial recau sobre la Direcció General de l'organització, ja que aquesta és responsable d'organitzar les funcions i responsabilitats i de facilitar els recursos adequats per aconseguir els objectius de l'ENS. Els directius són també responsables de donar bon exemple seguint les normes de seguretat establertes.

Aquests principis són assumits per la Direcció, qui disposa els mitjans necessaris i dota els seus empleats dels recursos suficients per al seu compliment, plasmant-se i posant-los en públic coneixement a través de la present Política Integrada de Sistemes de Gestió.

Els rols o funcions de seguretat definits són:

Funció	**Deures i responsabilitats**
Responsable de la informació (RIN)	Prendre les decisions relatives a la informació tractada
Responsable dels serveis (RSER)	Coordinar la implantació del sistema Millorar el sistema de forma contínua
Responsable de la seguretat (RSE - CISO)	Determinar la idoneïtat de les mesures tècniques Proporcionar la millor tecnologia per al servei
Responsable del sistema (RSIS)	Coordinar la implantació del sistema Millorar el sistema de forma contínua
Direcció (Secretaria General)	Proporcionar els recursos necessaris per al sistema Liderar el sistema

Aquesta definició de deures i responsabilitats es completa en els perfils de lloc i en els documents del sistema Registre de responsables, rols i responsabilitats.

RESOLUCIÓ DE CONFLICTES

Les diferències de criteris 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.

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 tal forma que totes les decisions més importants relacionades amb la seguretat s'acorden per aquest comitè.

Els membres del comitè de seguretat de la informació són:

- RESPONSABLE DE SEGURETAT
- RESPONSABLE DEL SISTEMA
- RESPONSABLE DEL SERVEI
- RESPONSABLE D'INFORMACIÓ

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 que 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 a aquesta Política d'Organització de la Seguretat.

Aquesta política es complementa amb la resta de les polítiques, procediments i documents en vigor per desenvolupar el nostre sistema de gestió.

9. Gestió de Riscos

Tots els sistemes subjectes a aquesta Política hauran de realitzar una anàlisi de riscos, avaluant les amenaces i els riscos als quals estan exposats.

Aquesta anàlisi es revisa regularment:

- almenys una vegada a l'any;
- quan canviï la informació manejada;
- quan canviïn els serveis prestats;
- quan ocorri un incident greu de seguretat;
- quan es reportin vulnerabilitats greus.

Per a l'harmonització de les anàlisis de riscos, el Comitè de Seguretat TIC establirà una valoració de referència per als diferents tipus d'informació manejats i els

diferents serveis prestats. El Comitè de Seguretat TIC dinamitzarà 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 Anàlisi de Riscos.

10. Gestió de Personal

Tots els membres d'UFEC tenen l'obligació de conèixer i complir aquesta Política de Seguretat de la Informació i la Normativa de Seguretat, sent responsabilitat del Comitè de Seguretat TIC disposar els mitjans necessaris perquè la informació arribi als afectats.

Tots els membres d'UFEC atendran una sessió de conscienciació en matèria de seguretat TIC almenys una vegada a l'any. S'establirà un programa de conscienciació contínua per atendre tots els membres de la UFEC, 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 la necessitin per realitzar la seva feina. La formació serà obligatòria abans d'assumir una responsabilitat, tant si és la seva primera assignació o si es tracta d'un canvi de lloc de treball o de responsabilitats en el mateix.

11. Professionalitat i seguretat dels recursos humans

Aquesta Política s'aplica a tot el personal d'UFEC i el personal extern que realitza tasques dins de l'empresa.

RRHH inclourà funcions de seguretat de la informació en les descripcions dels treballs dels empleats, informarà a tot el personal que contracti les seves obligacions respecte al compliment de la Política de Seguretat de la Informació, gestionarà els Compromisos de Confidencialitat amb el personal i coordinarà les tasques de capacitació dels usuaris respecte a aquesta Política.

- El Responsable de Gestió de la Seguretat (RGS) [CISO], és responsable de monitoritzar, documentar i analitzar els incidents de seguretat reportats, així com de comunicar-se al Comitè de Seguretat de la Informació i als propietaris d'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) [CISO] manegi informes d'incidents i anomalies del sistema. El Comitè també estarà al corrent, supervisarà la investigació, supervisarà l'evolució de la informació i promourà la resolució d'incidents de seguretat de la informació.
- El Responsable de Gestió de la Seguretat (RGS) [CISO] participarà en la preparació del Compromís de Confidencialitat que signaran els empleats i

tercers que exerceixin funcions a UFEC, en l'assessorament sobre les sancions que s'aplicaran per incompliment d'aquesta Política i en el tractament d'incidents de seguretat de la informació.
- Tot el personal d'UFEC és responsable d'informar sobre les debilitats i incidents de seguretat de la informació que es detecten oportunament.

Professionalitat dels recursos humans:

- Determinar la competència necessària del personal per dur a terme la feina que afecta a la Seguretat de la Informació.
- Cal assegurar que les persones siguin competents sobre la base de l'educació, capacitació o experiència adequades.
- Demostrar mitjançant la informació documentada que sigui 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 reclutament del personal i incloure-les en els acords a signar i verificar el seu compliment durant l'acompliment de les tasques de l'empleat.
- Assegurar-se que els usuaris estiguin al corrent de les amenaces i preocupacions de seguretat de la informació i estiguin capacitats per recolzar la Política de Seguretat de la Informació de l'organització en el curs de les seves tasques normals.
- Establir compromisos de confidencialitat amb tot el personal i usuaris fora de les instal·lacions de processament d'informació.
- Establir les eines i mecanismes necessaris per promoure la comunicació de les debilitats de seguretat existents, així com els incidents, amb la finalitat de minimitzar els seus efectes i prevenir la seva reincidència.

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

El control de l'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 a través de tècniques d'autenticació i autorització.
- Controlar la seguretat en la connexió entre la xarxa d'UFEC i altres xarxes públiques o privades.
- Revisar els esdeveniments crítics i les activitats dutes a terme pels usuaris en els sistemes.
- Conscienciar sobre la seva responsabilitat per l'ús de contrasenyes i equips.
- Garantir la seguretat de la informació quan s'utilitzen ordinadors portàtils i ordinadors personals per al treball remot.

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, instal·lacions i informació d'UFEC.
- Protegir l'equip de processament d'informació crític d'UFEC, col·locant-lo en àrees protegides i protegit per un perímetre de seguretat definit, amb les mesures de seguretat i controls d'accés adequats. Així mateix, contemplar la protecció d'aquesta en el seu trasllat i romandre fora de les àrees protegides, per manteniment o altres motius.
- Controlar els factors ambientals que podrien perjudicar el bon funcionament de l'equip de còmput que alberga la informació d'UFEC.
- Implementar mesures per protegir la informació manejada pel personal a les oficines, en el marc normal de les seves tasques habituals.
- Proporcionar protecció proporcional als riscos identificats.

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

El responsable de Gestió de la Seguretat (RGS) [CISO], juntament amb els Titulars de la Informació, segons escaigui, definirà les mesures de seguretat física i ambiental per a la protecció dels actius crítics, sobre la base d'una anàlisi de riscos, i supervisarà la seva 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'UFEC a les àrees restringides sota la seva responsabilitat. Els Propietaris d'Informació autoritzaran formalment la feina fora del lloc amb informació sobre el seu negoci als empleats d'UFEC quan ho considerin apropiat.

Tot el personal d'UFEC és responsable del compliment de la política de pantalla neta i escriptori, per a la protecció de la informació relacionada amb la feina diària a les oficines.

14. Adquisició de productes

Els diferents departaments han d'assegurar-se 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 i inclosos en la planificació, en la sol·licitud d'ofertes, i en plecs de licitació per a projectes de 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.

La política de desenvolupament i adquisició de sistemes d'informació es desenvolupa en el document: Política Adquisició, Desenvolupament i Manteniment de Sistemes.

15. Seguretat per defecte

La Unió de Federacions Esportives de Catalunya considera estratègic per a l'entitat 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, incloent-se la seguretat en les decisions de desenvolupament i/o adquisició i en totes les activitats en explotació establint-se la seguretat com un procés integral i transversal.

16. Integritat i actualització del sistema

La Unió de Federacions Esportives de Catalunya es compromet a garantir la integritat del sistema mitjançant un procés de gestió de canvis que permeti el control de l'actualització dels elements físics o lògics mitjançant l'autorització prèvia a la seva instal·lació en el sistema. Aquesta avaluació serà duta a terme principalment per la direcció de sistemes que avaluarà l'impacte en la seguretat del sistema abans de realitzar els canvis i controlarà de forma documentada aquells canvis que s'avaluïn com 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, a les vulnerabilitats i a les actualitzacions que els afectin, reaccionant amb diligència per gestionar el risc a la vista de l'estat de seguretat d'aquests.

17. Protecció de la informació emmagatzemada i en trànsit

La Unió de Federacions Esportives de Catalunya estableix mesures de protecció per a la Seguretat de la Informació emmagatzemada o en trànsit a través d'entorns insegurs. Tindran la consideració d'entorns insegurs els equips portàtils, assistents personals (PDA), dispositius perifèrics, suports d'informació i comunicacions sobre xarxes obertes o amb xifratge feble.

18. Prevenció de sistemes d'informació interconnectats

La Unió de Federacions Esportives de Catalunya, 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 en la seva totalitat o principalment, per a la prestació de serveis de comunicacions electròniques disponibles per al públic.

Rambla Catalunya, 81 pral. · 08008 Barcelona
Tel. 93 487 45 75 · www.ufec.cat

En tot cas s'analitzaran els riscos derivats de la interconnexió del sistema, a través de xarxes, amb altres sistemes, i es controlarà el seu punt d'unió. Connexions electròniques disponibles per al públic.

19. Continuïtat de l'activitat

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

20. Millora contínua del procés de seguretat

La Unió de Federacions Esportives de Catalunya estableix un procés de millora contínua de la seguretat de la informació aplicant els criteris i metodologia establerta en normes internacionals com ISO 27001.