# Política de seguretat de la informació de la UOC

**Document aprovat pel Consell de Direcció de la UOC el dia 20 de desembre de 2021**

# Índex

# 1. Principis

La seguretat de la informació té com a objectiu reduir, fins a un nivell que resulti acceptable, els riscos als quals està sotmesa la informació, els sistemes i els serveis que donen suport a l'activitat universitària. Aquest nivell acceptable ha de respondre a una valoració conjunta de la gravetat de les amenaces, els recursos disponibles, el respecte als drets individuals i el compliment normatiu. Només els òrgans de direcció de la Universitat Oberta de Catalunya (UOC) tenen les competències necessàries per establir aquest nivell, ordenar les actuacions necessàries en matèria de seguretat de la informació i habilitar els mitjans per portar-les a terme.

La política de seguretat de la UOC es defineix basant-se en els següents principis bàsics que s'han de desenvolupar:

a) Organització i implantació del procés de seguretat.
b) Anàlisi i gestió dels riscos.
c) Gestió del personal.
d) Professionalitat.
e) Autorització i control dels accessos.
f) Protecció de les instal·lacions.
g) Adquisició de productes.
h) Seguretat per defecte.
i) Integritat i actualització del sistema.
j) Protecció de la informació emmagatzemada i en trànsit.
k) Prevenció davant altres sistemes d'informació interconnectats.
l) Registre d'activitat.
m) Incidents de seguretat.
n) Continuïtat de l'activitat.
o) Millora contínua del procés de seguretat.

# 2. Objecte

L'objecte de la política de seguretat és fixar el marc d'actuació necessari per protegir els sistemes d'informació, d'amenaces internes i externes, deliberades o accidentals, amb el fi d'assegurar el compliment dels principis bàsics de confidencialitat, integritat i disponibilitat de la informació.

En aquest sentit, resulta imprescindible establir, en la política de seguretat de la informació, una organització que garanteixi la correcta distribució de tasques i responsabilitats.

# 3. Àmbit d'aplicació subjectiu

Aquesta política de seguretat cal aplicar-la a tota la informació que es genera a conseqüència de les activitats acadèmiques, de recerca, de gestió o de difusió, tant a la Fundació per a la Universitat Oberta de Catalunya (FUOC) com a la resta d'empreses del grup (en endavant, "el grup" o "el grup empresarial"), així com als tractaments dels quals pugui ser objecte, independentment que aquests siguin manuals o automatitzats i que inclogui o no dades de caràcter personal, i afecta tots els membres de l'organització, sense excepcions.

# 4. Assignació de rols i responsabilitats

A continuació, es detallen els rols i les responsabilitats de cadascuna de les àrees de la UOC implicades en la seguretat de la informació. Cal especificar, doncs, que l'àmbit d'actuació de les àrees següents va més enllà de la Fundació, ja que la seva funció té abast a la totalitat d'empreses del Grup.

## 4.1. Responsable del servei

La persona responsable de servei té les funcions següents:

1. Responsabilitzar-se de la prestació de serveis basats en sistemes de la informació de la Universitat.
2. Vetllar per la seguretat dels actius, en cada dimensió de seguretat, segons els criteris marcats pel Comitè de Seguretat de la Informació de la UOC, amb l'assessorament de la persona responsable de seguretat de la informació i de la persona responsable de la tecnologia de la informació.
3. Garantir la prestació del servei en condicions òptimes de disponibilitat, accessibilitat o interoperabilitat

La funció de la persona responsable del servei de la UOC recau en el gerent de la FUOC, que la té delegada al vicegerent d'Operacions.

## 4.2. Responsables funcionals dels sistemes d'informació

Les persones responsables funcionals dels sistemes d'informació tenen les funcions següents en l'àmbit de la seguretat de la informació:

1. Classificar la informació de la qual són responsables segons la criticitat que aquesta tingui per a la companyia en termes de confidencialitat, privadesa, integritat, continuïtat, autenticitat, no repudi, traçabilitat i impacte mediàtic.

2. Determinar la categoria dels sistemes d'informació utilitzant com a marc de referència l'establert en l'annex I del Reial decret 3/2010, de 8 de gener, que regula l'Esquema Nacional de Seguretat.

3. Tenir coneixement de la normativa general o sectorial aplicable a la informació de la qual són responsables, inclosa la normativa vigent en matèria de protecció de dades de caràcter personal.

4. Vetllar per la seguretat dels actius corresponents al procés dels quals són responsables, en cada dimensió de seguretat, confidencialitat, disponibilitat i integritat, segons els criteris marcats pel Comitè de Seguretat de la Informació de la UOC, amb l'assessorament de la persona responsable de seguretat de la informació.

5. Determinar l'ús, els accessos i els privilegis dels sistemes que estan sota el seu àmbit de responsabilitat.

6. Vetllar per la inclusió de clàusules sobre seguretat en els contractes amb terceres parts i perquè es compleixin.

7. Col·laborar a fer revisions i auditories de seguretat de la informació.

La funció de les persones responsables funcionals dels sistemes d'informació de la UOC la desenvolupen les persones responsables de procés definides en el Mapa de processos del sistema de gestió interna de qualitat de la UOC.

## 4.3. Responsable de seguretat de la informació

La persona responsable de seguretat té l'obligació de vetllar per la seguretat de la informació i dels serveis prestats pels sistemes d'informació, i dirigir el sistema de gestió

de la seguretat de la informació d'acord amb el que s'estableix en aquesta política. Té les funcions següents:

1. Elaborar, promoure i mantenir una política de seguretat de la informació.
2. Desenvolupar, amb el suport de les unitats corresponents, el marc normatiu de seguretat i controlar-ne el compliment.
3. Fixar objectius de seguretat i planificar-ne l'execució.
4. Planificar les auditories necessàries per garantir el compliment de la legalitat vigent i el cicle de vida del sistema de gestió de la seguretat de la informació.
5. Analitzar els riscos que afronta la UOC en el marc de seguretat de la informació i prendre decisions sobre la manera de tractar-los.
6. És responsable de l'elaboració i seguiment del Pla de seguretat.
7. Promoure l'adequació a les normatives.
8. Vetllar perquè s'estableixin els mecanismes de continuïtat de les activitats davant d'incidents de seguretat.
9. Fer seguiment de les incidències de seguretat i escalar-les al Comitè de Seguretat si correspon.
10. Supervisar l'eficàcia de les mesures de seguretat establertes per protegir la informació i garantir la disponibilitat i el correcte funcionament dels serveis prestats pels sistemes d'informació.
11. Proposar la implantació d'eines i controls de seguretat de la informació i definir el quadre de comandament de la seguretat.
12. Promoure la formació i conscienciació dels treballadors i treballadores de la UOC en la seguretat de la informació dins del seu àmbit de responsabilitat.
13. Ésser l'interlocutor o interlocutora oficial en comunicacions amb altres entitats en aquesta matèria.

La funció de responsable de seguretat de la informació l'exerceix la persona que té assignada la responsabilitat de direcció de l'Oficina de Seguretat de la Informació.

## 4.4. Responsable tècnic del servei de ciberseguretat

La persona responsable del servei de ciberseguretat té les funcions següents:

1. Dirigir i coordinar el servei d'operació de la seguretat que monitoritza, aixeca alertes i investiga possibles incidents de seguretat.
2. Coordinar les activitats relacionades amb la detecció, l'anàlisi i la gestió de vulnerabilitats.
3. Estar alerta dels canvis de la tecnologia de què disposa la UOC i de les conseqüències d'aquests canvis, i proposar les mesures oportunes.
4. Informar i retre comptes a la persona responsable de seguretat de la informació en matèria de seguretat de la informació.
5. Redactar els procediments d'actuació en l'ús dels serveis tecnologies de la informació i la comunicació (TIC) relacionats amb la seguretat.

6. Coordinar l'elaboració d'informes tècnics en cas d'incidències de seguretat molt greus.
7. Responsabilitzar-se de l'execució regular de verificacions de seguretat i, si cal, proposar mesures correctores.
8. Col·laborar en l'elaboració i el seguiment del Pla de seguretat.
9. Elaborar els requisits de formació i qualificació d'administradors, operadors i usuaris, juntament amb la persona responsable del sistema.
10. Identificar les tasques d'administració i operació que garanteixin la satisfacció dels criteris i requisits de segregació de tasques imposades pel Comitè de Seguretat de la Informació.
11. Responsabilitzar-se de coordinar la resposta davant d'incidents de seguretat que desbordin els casos previstos i procedimentats, i de coordinar la investigació forense relacionada amb incidents considerats rellevants.

La funció de responsable tècnic del servei de ciberseguretat l'exerceix la persona dins de l'Oficina de Seguretat de la Informació designada per la persona responsable de seguretat.

## 4.5. Responsable del sistema

La persona responsable del sistema té les funcions següents en relació amb la seguretat de la informació:

1. Garantir el desenvolupament, l'operació i el manteniment del sistema durant tot el seu cicle de vida, de les seves especificacions, instal·lació i verificació del seu correcte funcionament.
2. Aplicar la política de seguretat corresponent a la connexió o desconnexió d'equips.
3. Assegurar l'aprovació dels canvis que afectin la seguretat del sistema.
4. Garantir la implantació de les mesures específiques de seguretat del sistema i assegurar-se que aquestes s'integrin adequadament dins del marc general de seguretat.
5. Vetllar per la implantació de la configuració autoritzada de maquinari i programari per utilitzar en el sistema.
6. Dur a terme el preceptiu procés d'anàlisi i gestió de riscos en el sistema.
7. Vetllar pel compliment de les obligacions en matèria de seguretat de cada entitat involucrada en el manteniment, operació, explotació, implantació i supervisió del sistema.
8. Dotar els recursos necessaris per investigar els incidents de seguretat que afecten el sistema i, si escau, comunicació a la persona responsable de seguretat de la informació o a qui aquesta determini.
9. Establir plans de contingència i emergència segons les directrius establertes als plans de continuïtat, i portar a terme exercicis freqüents perquè el personal es familiaritzi amb aquests.

10. Vetllar perquè els projectes TIC incorporin els principis de protecció de dades i de seguretat de la informació en el disseny i per defecte.

A més, la persona responsable del sistema pot acordar la suspensió del maneig d'una certa informació o la prestació d'un cert servei si és informada de deficiències greus de seguretat que puguin afectar la satisfacció dels requisits establerts. Aquesta decisió ha de ser acordada amb les persones responsables de la informació afectada i del servei afectat, així com amb la persona responsable de seguretat de la informació, abans de ser executada.

La funció de responsable del sistema l'exerceix la persona que té assignada la responsabilitat de direcció de la tecnologia de la informació a la UOC, és a dir, el director o directora de l'Àrea de Tecnologia.

## 4.6. Plantilla de la UOC

Les persones que treballen a la UOC, personal empleat i personal eventual que utilitza els sistemes i aplicacions de la UOC, tenen les funcions següents en l'àmbit de la seguretat de la informació:

1. Responsabilitzar-se del correcte tractament de les dades personals dins del seu àmbit d'activitat.
2. Relacionar-se amb les TIC per complir les seves obligacions laborals.
3. Conscienciar-se en la seguretat de les TIC pel manteniment de la seguretat del sistema.
4. Estar informades de les seves obligacions i responsabilitats i haver estat correctament instruïdes per a les tasques que realitzen. A l'efecte tindran a la seva disposició les normes d'ús dels mitjans tecnològics i de la informació i rebran la formació adient en cada moment, atenent a les seves responsabilitats.
5. Ésser responsables de conèixer els procediments de la seva competència.
6. Ésser responsables d'informar de qualsevol incident de seguretat que sigui observat durant la realització de la seva activitat laboral diària.

# 5. Organització de la seguretat

La UOC disposarà d'una estructura de supervisió i coordinació de la seguretat que serà la responsable d'establir i aprovar els requisits de seguretat per al sistema, a més de verificar i supervisar la correcta implementació i manteniment d'aquests requisits. Aquesta estructura està formada pels òrgans següents:

## 5.1. Consell de Direcció de la Universitat

Funcions:

- Ésser el responsable que la UOC aconsegueixi els seus objectius de seguretat

TIC a curt, mitjà i llarg termini.
- Donar suport explícitament i amb notorietat de les activitats de seguretat TIC a la UOC.
- Expressar les seves inquietuds quant a la seguretat de la informació al Comitè de Seguretat de la Informació.
- Aprovar la política de seguretat de la UOC.
- Delegar el seguiment de la seguretat en el Comitè de Seguretat de la Informació.

## 5.2. Comitè de Seguretat de la Informació

Funcions:
- Revisa la política de seguretat de la informació i proposa que el Consell de Direcció l'aprovi.
- Aprovar les normatives associades a la política de seguretat de la informació.
- Divulgar la política i les normatives de seguretat de la UOC.
- Aprovar del Pla director de seguretat.
- Vetllar per obtenir els recursos necessaris per a l'assoliment dels nivells de seguretat establerts.
- Seguir periòdicament (dos cops l'any) els objectius de seguretat marcats per l'any en curs.

El Comitè de Seguretat es reunirà de manera ordinària dues vegades l'any, una el primer semestre i una el segon, i, de manera extraordinària, tantes vegades com faci falta, a instància del seu president o presidenta o de la persona responsable de seguretat de la informació.

Formaran part d'aquest comitè les següents figures/persones:

President o presidenta: director o directora general de la FUOC i gerent o gerenta de la Universitat.

Secretari o secretària: persona responsable de la seguretat de la informació.

Membres:
- Director o directora general de la FUOC i gerent o gerenta de la Universitat
- Vicerector o vicerectora de Docència i Aprenentatge
- Vicerector o vicerectora de Planificació Estratègica i Recerca
- Vicegerent o vicegerenta de Recursos i Finances
- Vicegerent o vicegerenta d'Operacions
- Secretari o secretària general
- Director o directora de l'Àrea de Tecnologia
- Responsable de la seguretat de la informació
- Director o directora de l'Assessoria Jurídica
- Delegat o delegada de protecció de dades

# 6. Desenvolupament

## 6.1. Dimensions de la seguretat

La UOC depèn dels sistemes TIC per assolir els seus objectius. Aquests sistemes han de ser administrats amb diligència, prenent les mesures adequades per protegir enfront de 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 confidencialitat, disponibilitat i integritat de la informació i la prestació continuada dels serveis, actuant preventivament, supervisant l'activitat diària i reaccionant amb prestesa 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, cal una estratègia que s'adapti als canvis en les condicions de l'entorn per garantir la prestació contínua dels serveis, 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.

Les diferents àrees i estudis de la UOC s'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 plecs de licitació per a projectes de TIC.

Les àrees i els estudis de la UOC han d'estar preparats per prevenir accidents, detectar-los, reaccionar-hi i recuperar-se'n.

### 6.1.1. Prevenció

Les àrees i els estudis de la UOC han d'evitar, o almenys prevenir en la mesura del possible, que la informació o els serveis es vegin perjudicats per incidents de seguretat. Per això els departaments han d'implementar les mesures de seguretat adequades, així com qualsevol control addicional identificat per mitjà d'una avaluació d'amenaces i riscos que es consideri adient. Aquests controls, i els rols i les responsabilitats de seguretat de tot el personal, han d'estar clarament definits i documentats.
Per garantir el compliment de la política han de:

- Autoritzar expressament la correcció dels sistemes i la seva configuració, i cal presentar uns controls de seguretat adients abans d'entrar en operació.

- Avaluar regularment la seguretat, incloent-hi avaluacions dels canvis de configuració, que afectin la seguretat, realitzats de forma rutinària.
- Determinar la revisió periòdica per part de tercers amb la finalitat d'obtenir una avaluació independent.

### 6.1.2. Detecció

Atès que els serveis es poden degradar ràpidament a causa d'incidents, que van des d'una simple desacceleració fins a la seva detenció, s'han d'establir mesures per monitorar l'operació de manera contínua per detectar anomalies en els nivells de prestació dels serveis i actuar en conseqüència.

El monitoratge és especialment rellevant quan s'estableixen línies de defensa en la seguretat del sistema en estudi. S'establiran mecanismes de detecció, anàlisi i informe que arribin a les persones responsables regularment i quan es produeix una desviació significativa dels paràmetres que s'hagin preestablert com a normals.

### 6.1.3. Resposta

Els departaments de la UOC han de:

- Establir mecanismes per respondre eficaçment als incidents de seguretat (bé directament o bé mitjançant entitats centrades en aquesta resposta a incidents).
- Designar un punt de contacte per a les comunicacions pel que fa a incidents detectats en altres departaments o en altres organismes que puguin tenir impacte.
- Establir protocols per a l'intercanvi d'informació relacionada amb l'incident amb les entitats que puguin participar en activitats de suport i assistència.

### 6.1.4. Recuperació

Per garantir la disponibilitat dels serveis crítics, els departaments de la UOC han de desenvolupar plans de continuïtat dels sistemes TIC com a part del seu pla general de continuïtat de negoci i activitats de recuperació.

Un pla de continuïtat del negoci ha de permetre:

- Mantenir el nivell de servei dins els límits definits.
- Minimitzar el període de recuperació.
- Recuperar la situació inicial prèvia a un incident.
- Analitzar els resultats i els motius dels incidents.
- Minimitzar l'impacte d'un incident en l'activitat de l'organització.

En cas que els incidents de seguretat hagin pogut tenir impacte en els serveis o els actius de l'organització, caldrà determinar en el pla de continuïtat les actuacions i els protocols que cal seguir per tal de permetre la recuperació i continuació dels serveis implicats.

# 6.2. Principis de la seguretat de la informació

El sistema de gestió de la seguretat de la informació és l'instrument del qual es dota la UOC per garantir la integritat, confidencialitat i disponibilitat de la informació que tracta, així com per garantir la traçabilitat de les accions que es porten a terme sobre aquesta. Aquest sistema ha d'estar sotmès a monitoratge, control i millora contínua per tal de mantenir-ne l'eficàcia davant la constant evolució de les amenaces i dels sistemes tècnics de protecció.

El sistema de gestió de la seguretat de la informació està constituït per un conjunt de documents (protocols, normatives i procediments), que desenvolupen els principis que han de regir l'aplicació d'aquesta política.

## 6.2.1. Gestió de riscos

L'anàlisi i la gestió de riscos són parts essencials del procés de seguretat i s'han de mantenir permanentment actualitzades. La gestió de riscos ha de permetre el manteniment d'un entorn controlat, que minimitzi els riscos fins a nivells acceptables i que involucri els òrgans de direcció de la UOC en l'acceptació d'un determinat risc residual.

L'anàlisi i la gestió de riscos s'ha de fer conforme a eines i metodologies habitualment acceptades i han d'estar presents en totes les fases del cicle de vida de les aplicacions i dels serveis i sistemes que donen suport al tractament de la informació. La selecció i l'aplicació dels controls de seguretat, així com l'avaluació de la seva eficàcia, s'han de tenir en compte durant el disseny, la construcció, la contractació, l'adquisició, l'explotació i la terminació o cancel·lació de les aplicacions, els serveis i els sistemes mencionats.

La persona responsable de la seguretat de la informació ha d'elaborar un informe anual sobre l'estat de la seguretat, els riscos previsibles i els plans d'actuació recomanats.

## 6.2.2. Classificació de la informació

Els actius d'informació que es tracten han d'estar inventariats i classificats. Aquesta classificació s'ha de fer tenint en compte requeriments legals, el seu valor, la seva sensibilitat i la seva criticitat per l'organització. El nivell de protecció i les mesures de seguretat que s'han d'aplicar a la informació s'han de basar en la seva classificació.

## 6.2.3. Planificació i coordinació

Periòdicament la UOC ha de definir un conjunt d'objectius de seguretat, que han d'incloure una descripció de les línies d'actuació previstes, els projectes en què es concreten, els objectius que s'han d'assolir i els indicadors de compliment i progrés

corresponents. Aquests objectius han de prendre en consideració els resultats de les auditories i de l'anàlisi de riscos.

L'esquema organitzatiu de la seguretat de la informació inclou els òrgans de coordinació i decisió necessaris per a l'aplicació i el control de les mesures de seguretat.

### 6.2.4. Accés a la informació

Les persones que tracten informació de la UOC que no tingui caràcter públic han d'estar degudament acreditades per unes credencials electròniques personals i intransferibles.

Els privilegis d'accés a la informació s'han de limitar als estrictament imprescindibles per al desenvolupament de les funcions de cadascú.

### 6.2.5. Registre d'activitat

Les actuacions de les persones, com que formen part de tractaments d'informació, s'han d'enregistrar a aplicació de les exigències legals de traçabilitat o per verificar el compliment d'aquesta política.

### 6.2.6. Confidencialitat i deure de secret

Les persones que tracten informació de la UOC que no tingui caràcter públic han de guardar, per un temps indefinit, la màxima reserva i no divulgar ni utilitzar directament ni mitjançant terceres persones o empreses les dades, els documents, les metodologies, les contrasenyes, les anàlisis, els programes i altra informació a la qual tinguin accés durant la seva relació laboral amb la FUOC i amb empreses que pertanyen al Grup, tant en suport material com electrònic. Aquesta obligació continuarà vigent un cop extingit el contracte laboral.
En el cas de l'activitat de recerca, les dades tractades es podran divulgar convenientment anonimitzades.

### 6.2.7. Instal·lacions i equipament

Les infraestructures informàtiques i de comunicacions que no formen part dels llocs de treball s'han d'ubicar en àrees aïllades, d'accés restringit i suficientment protegides.

### 6.2.8. Protecció de la informació no automatitzada

La informació en suport no electrònic s'ha de protegir amb el mateix nivell de seguretat que la que hagi estat sotmesa a tractament automatitzat.

# 7. Directrius de seguretat de la informació

- **Salvaguarda d'interessos**, entesa com que qualsevol acció o mesura implementada en matèria de seguretat de la informació ha de salvaguardar els interessos de la comunitat UOC (estudiantat, professorat, personal investigador i treballadores i treballadors) i ha de permetre el compliment de les seves obligacions.
- **Proporcionalitat i gestió del risc**, entesos com que cal aplicar mesures de protecció de la informació per garantir-ne la disponibilitat, confidencialitat, privacitat i integritat segons el principi de proporcionalitat, de manera que les mesures adoptades per protegir la informació siguin fruit d'una anàlisi del risc existent i de l'impacte per part de la UOC en cas que aquest risc es materialitzés.
- **Assumpció de riscos**, entesa com que l'assumpció de riscos en matèria de seguretat de la informació ha de ser aprovada per un nivell directiu adequat, que serà més alt segons major sigui l'impacte màxim del risc. Aquest nivell directiu de risc ha de tenir competència sobre l'àmbit afectat en cas de materialització del risc.
- **Continuïtat del negoci**, entesa com que cal desenvolupar plans de continuïtat del negoci d'acord amb el resultat d'una anàlisi del risc per assegurar la continuïtat dels processos crítics.
- **Propietat i classificació de la informació**, enteses com que tota informació ha de tenir una persona propietària responsable de classificar-la en funció del seu valor i els requeriments legals existents, controlar el seu cicle de vida i autoritzar-ne l'accés.
- **Accés d'acord amb el principi de necessitat**, entès com que només es facilita accés a la informació a les persones que en tinguin una necessitat legítima per al desenvolupament de les seves funcions.
- **Responsabilitat i qualitat**, enteses com que la informació proporcionada a través de mitjans electrònics ha d'estar protegida adientment per garantir-ne la veracitat i l'autenticitat.
- **Compliment normatiu**, entès com que cal donar compliment a la legislació i al marc normatiu de referència vigent en matèria de seguretat de la informació.
- **Relació amb tercers**, entesa com que cal adoptar les mesures necessàries per garantir la seguretat de la informació en la relació amb terceres parts. En concret, els contractes inclouran clàusules que obliguin l'empresa contractista i, si s'escau, subcontractada a aplicar les mesures de seguretat de la informació que corresponguin en aplicació d'aquesta política, a complir o desenvolupar els procediments de seguretat de la informació necessaris i a complir altres polítiques de la UOC que puguin ser aplicables a l'empresa, el servei o el personal extern que presta el servei. El contracte ha de recollir la possibilitat de realitzar auditories per part de la UOC, i de penalitzar el prestador de serveis en cas d'incompliment.
- **Divulgació**, entesa com que es duran a terme accions de formació i conscienciació de tots els usuaris i usuàries en matèria de seguretat de la informació, i de comunicació de responsabilitats, obligacions i pautes de comportament ètic, així com dels procediments establerts per la notificació

d'incidències.

- **Ús legítim**, entès com que cal assegurar-se que tots els actius d'informació, siguin llogats, cedits, compartits o propietat de la UOC, siguin per a l'ús exclusiu en les activitats i els objectius previstos i legítims de la UOC, i que no es permeti cap ús privat o per a qualsevol altre objectiu.
- **Disponibilitat de recursos**, entesa com que s'establirà l'estructura de gestió i s'assignaran els recursos necessaris per garantir i controlar la correcta implantació de la seguretat de la informació.
- **Segregació de funcions**, entesa com que l'assignació de funcions i responsabilitats es farà respectant sempre que sigui possible el principi de segregació de funcions (les operacions d'alt risc no haurien de poder ser realitzades de principi a fi per una sola persona).
- **Seguiment continuat**, entès com que es farà un seguiment continuat del sistema de gestió de la seguretat de la informació i dels indicadors que se'n derivin, i es realitzaran auditories regulars dels sistemes per garantir l'aplicació dels controls i mesures de seguretat de la informació establerts, i detectar possibles vulnerabilitats o mancances.

# 8. Desenvolupament de la política de seguretat de la informació

La política de seguretat es desenvoluparà mitjançant normes, procediments, guies i documents de suport de seguretat per cada especificitat.

Aquests recursos s'aniran actualitzant periòdicament i es divulgaran i comunicaran tal com s'explica en el punt 10 del present document.

# 9. Revisió o control de compliment

La persona responsable de seguretat de la informació realitzarà revisions o controls periòdics de verificació de l'aplicació i el compliment de la política de seguretat, així com del marc normatiu que la desenvolupa. Des del Comitè de Seguretat es realitzaran controls de compliment de la política de seguretat, i també s'identificarà i es mantindrà actualitzada la relació de requisits legals, organitzatius i tècnics que li siguin aplicables en matèria de seguretat de la informació.

Aquestes revisions tindran caràcter anual o es duran a terme quan es produeixin canvis significatius de la política de seguretat o del marc normatiu.

# 10. Divulgació i comunicació

Una vegada aprovada la present política de seguretat, així com la normativa que la complementi, es posarà a disposició de tots els subjectes afectats per aquesta segons l'àmbit d'aplicació. Així mateix, els documents esmentats estaran disponibles a la intranet de la UOC. Per difondre i donar a conèixer la política de seguretat i la normativa complementària, es realitzaran píndoles de formació. L'assistència a les sessions de formació és de caràcter obligatori.
En els contractes, llicències i acords subscrits amb tercers per part de la FUOC s'inclourà el deure de compliment de la legislació vigent en matèria de seguretat, així com la legislació aplicable en matèria de propietat intel·lectual i de protecció de dades i qualsevol altra normativa aplicable. S'informarà els diferents proveïdors, en el moment de la contractació, de l'existència de la política de seguretat a la qual resten subjectes.

# 11. Aprovació de la política

L'aprovació d'aquesta política s'ha dut a terme de conformitat amb el que preveu la política de rols i responsabilitats en l'aprovació de normativa interna de la UOC.

# 12. Confidencialitat

Totes les normes, els procediments i els documents aprovats internament són propietat de la UOC i no es poden utilitzar amb finalitats diferents d'aquelles per a les quals s'han lliurat ni es poden transmetre o comunicar a persones alienes als interessos de la UOC.

Signatura,

# Annex 1. Marc legal i normatiu

Per complir amb les obligacions relatives a la seguretat de la informació, el marc legal i estratègic de la present política està format principalment per les següents directives, lleis orgàniques, lleis, reials decrets, pactes i normatives internes:

- 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 les transaccions electròniques en el mercat interior i pel qual es deroga la Directiva 1999/93/CE.
- Reglament (UE) 2016/679 del Parlament Europeu i del Consell, de 27 d'abril de 2016, relatiu a la protecció de les persones físiques sobre el tractament de dades personals i la lliure circulació d'aquestes dades i pel qual es deroga la Directiva 95/46/CE (Reglament general de protecció de dades).
- Directiva (UE) 2016/1148 del Parlament Europeu i del Consell, de 6 de juliol de 2016, relativa a les mesures destinades a garantir un elevat nivell comú de seguretat de les xarxes i sistemes d'informació a la Unió.
- Llei orgànica 3/2018, de 5 de desembre, de protecció de dades personals i garantia dels drets digitals.
- Llei orgànica 15/1999, de 13 de desembre, de protecció de dades de caràcter personal.
- Reial decret 1720/2007, de 21 de desembre, pel qual s'aprova el Reglament de desenvolupament de la Llei orgànica 15/1999, de 13 de desembre, de protecció de dades de caràcter personal.
- Reial decret legislatiu 1/1996, de 12 d'abril, pel qual s'aprova el text refós de la Llei de propietat intel·lectual.
- Llei 34/2002, d'11 de juliol, de serveis de la societat de la informació i de comerç electrònic.
- Llei 19/2014, de 29 de desembre, de transparència, accés a la informació pública i bon govern.
- Així com la resta de normativa aplicable a la UOC en matèria de seguretat de la informació.

# Annex 2. Quadre de versions

| Versió | Data | Canvi | Motiu del canvi |
|---|---|---|---|
| 1 | 30/06/2016 | Creació. | |
| 2 | 01/07/2021 | La totalitat de la política. | Adequació a la nova realitat de la institució i al marc legal vigent. |
| 3 | 21/01/2022 | Canvi en l'apartat 5.2. | Canvi en la composició del Comitè. |