POLÍTICA DE SEGURETAT DE LA INFORMACIÓ

Fundació General de la Universitat de València

VNIVERSITAT DE VALÈNCIA
Fundació General

ÍNDEX

1. APROVACIÓ I ENTRADA EN VIGOR

Text aprovat el dia 15 de juliol de 2025 per la Vicepresidència Executiva de la Fundació General de la Umniversitat de València. Aquesta política de seguretat de la informació serà efectiva des d'aquesta data i fins que siga reemplaçada per una de nova.

2. INTRODUCCIÓ

La Fundació General de la Universitat de València (FGUV) depén dels sistemes de les tecnologies d'informació i la comunicació (TIC) per aconseguir els seus objectius. Aquests sistemes s'han de de tractar amb diligència prenent les mesures adequades per a protegir-los de danys accidentals o deliberats que puguen afectar la disponibilitat, la integritat o la confidencialitat de la informació tractada o els serveis prestats.

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

Els sistemes de les TIC han d'estar protegits d'amenaces d'evolució ràpida amb potencial per a afectar la confidencialitat, la integritat, la disponibilitat, l'ús previst i el valor de la informació i dels serveis. Per defensar-se d'aquestes amenaces es requereix una estratègia que s'adapte als canvis de les condicions de l'entorn i 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, fer un seguiment continu dels graus de prestació de serveis, atendre i analitzar les vulnerabilitats que es comuniquen i preparar una resposta efectiva per als incidents per garantir la continuïtat dels serveis prestats.

L'organització s'ha de cerciorar que la seguretat de les TIC és una part integral de cada etapa del cicle de vida del sistema, des de la seua concepció fins a la retirada del servei, passant per les decisions sobre desenvolupament o adquisició i les activitats d'explotació. Els requisits de seguretat i les necessitats de finançament s'han d'identificar i incloure en la planificació, en la sol·licitud d'ofertes i en els plecs de licitació per a projectes de TIC.

L'organització ha d'estar preparada per a prevenir, detectar, reaccionar i recuperar-se d'incidents, d'acord amb l'article 8 de l'ENS.

2.1. Prevenció

L'organització ha d'evitar, o almenys prevenir en la mesura que siga possible, que la informació o els serveis es vegen perjudicats per incidents de seguretat. Per a això s'han d'adoptar les mesures mínimes de seguretat determinades per l'ENS, així com controls addicionals identificats a través d'una avaluació d'amenaces i riscos. Aquests controls, així com els papers i les responsabilitats sobre seguretat de tot el personal han d'estar clarament definits i documentats.

Per garantir el compliment de la política l'organització ha de:

- Tenir autoritzats els sistemes abans d'entrar en operació.
- Avaluar regularment la seguretat, inclosos els canvis de configuració rutinaris.
- Sol·licitar la revisió periòdica per part de tercers amb la finalitat d'obtenir una avaluació independent.

2.2. Detecció

Atés que els serveis es poden degradar ràpidament a causa dels incidents de tot tipus, que van des d'una simple desacceleració, fins a la seua detenció, s'han de monitorar les operacions de forma contínua per detectar anomalies en la prestació dels serveis i actuar en conseqüència, segons estableix l'article 10 de l'ENS.

El monitoratge és especialment rellevant quan s'estableixen línies de defensa d'acord amb l'article 9 de l'ENS. S'establiran mecanismes de detecció, anàlisi i comuniccaicó que arriben als responsables regularment i quan es produïsca una desviació significativa dels paràmetres que s'hagen preestablert com a normals.

2.3. Resposta

L'organització ha de:

- Establir mecanismes per a respondre eficaçment als incidents de seguretat.
- Establir un punt de contacte per a les comunicacions sobre incidents en altres departaments o organismes.

- Establir protocols per a l'intercanvi d'informació sobre l'incident. Això inclou comunicacions en ambdós sentits, amb els equips de resposta en cas d'emergències (CERT).

2.4. Recuperació

Les mesures per a donar resposta s'adoptaran en temps oportú i estaran orientades a la restauració de la informació i els serveis afectats per un incident de seguretat.

El sistema d'informació garantirà la conservació de les dades i de la informació en suport electrònic.

D'igual manera, el sistema mantindrà disponibles els serveis durant tot el cicle vital de la informació digital a través d'una concepció i uns procediments que siguen la base per a la preservació de la informació.

3. ABAST

Aquesta política s'aplicarà a tots els sistemes de les TIC i a tots els membres de l'organització.

4. MISSIÓ

La FGUV, de conformitat amb el que disposa l'article 8 dels seus Estatuts, té la missió fonamental de cooperar per al compliment dels fins de la Universitat de València. Aquesta és una tasca que realitza mitjançant l'encàrrec de gestió que fa la Universitat de València, que desenvolupa a través de tres grans àrees d'actuació: cultura i formació, serveis universitaris i solidaritat, i dels seus serveis generals.

L'experiència i el coneixement de l'entorn sociocultural, formatiu i docent, així com de l'àmbit de la cooperació universitària per al desenvolupament proporcionen a la FGUV les eines necessàries per a configurar-se com un pont entre la Universitat de València i la societat per a la transferència, la divulgació, la difusió, la democratització cultural, la formació i la solidaritat.

5. NORMATIVA

Les principals normatives aplicables a la FGUV són les següents:

- Lleis 8/1998, de 9 de desembre, de la Generalitat Valenciana, de fundacions de la Comunitat Valenciana.
- Decret 68/2011, de 27 de maig, del Consell, pel qual s'aprova el reglament de les fundacions de la Comunitat Valenciana.
- Llei 9/2017, de 8 de novembre, de contractes del sector públic, per la qual es transposen a l'ordenament jurídic espanyol les directrius del Parlament Europeu i del Consell 2014/23/UE i 2014/24/UE, de 26 de febrer de 2014.
- Llei 19/2013, de 9 de desembre, de transparència, accés a la informació pública i bon govern.
- Llei 38/2003, de 17 de novembre, general de subvencions.
- Llei orgànica 3/2018, de 5 de desembre, de protecció de dades personals i garantia dels drets digitals.
- Reglament (UE) 2016/679, del Parlament Europeu i del Consell, de 27 d'abril de 2016, per a la protecció de les persones físiques quant al tractament de les dades personals i a la lliure circulació d'aquestes, pel qual es deroga la directriu 95/46/CE, del reglament general de protecció de dades.
- Reial decret 311/2022, de 3 de maig, pel qual es regula l'Esquema Nacional de Seguretat.
- Llei 10/2010, de 28 d'abril, de prevenció del blanqueig de capitals i del finançament del terrorisme.
- Llei 34/2002, d'11 de juliol, de serveis de la societat de la informació i de comerç electrònic.
- Reial decret legislatiu 1/2007, de 16 de novembre, pel qual s'aprova el text refós de la *Llei general dels consumidors i usuaris* i altres lleis complementàries
- Reial decret legislatiu 1/1996, de 12 d'abril, pel qual s'aprova el text refós de la *Llei de propietat intel·lectual* i es regularitzen, aclareixen i harmonitzen les disposicions legals vigents sobre la matèria.
- Llei 53/1984, de 26 de desembre, d'incompatibilitats del personal al servei de les administracions públiques.

- Llei 6/2020, d'11 de novembre, de regulació de determinats aspectes dels serveis electrònics de confiança.

6. ORGANITZACIÓ DE LA SEGURETAT

6.1. Comitè

La seguretat de la informació i de les TIC estarà coordinada pel Comitè de Seguretat, que estarà format per:

- La Gerencia de la FGUV.
- La persona responsable del departament dadministració de la FGUV.
- La persona responsable del departament jurídic de la FGUV.
- Una persona técnic/a del departament jurídic de la FGUV.
- El/la delegat per a la protecció de les dades de carácter personal de la Universitat de València i de les seues fundaciones depenents.
- La persona responsable de la seguretat de la informació de la FGUV.
- La persona responsable de sistemes de la FGUV.

El responsable de la seguretat serà el secretari del Comitè de Seguretat i com a tal tindrà les funcions següents:

- Convocar les reunions del Comitè de Seguretat.
- Preparar els assumptes que s'hagen de tractar en les reunions del Comitè i aportar la informació puntual per a la presa de decisions.
- Ser el responsable de l'execució, directa o delegada, de les decisions del Comitè.

El Comitè de Seguretat informarà a la Vicepresidència Executiva.

Haurà d'obtenir regularment l'assessorament tècnic o extern pertinent per a la presa de decisions i s'assessorarà sobre els problemes sobre els quals haja de decidir o donar una opinió.

6.2. Papers: funcions i responsabilitats

1. El responsable de la informació

El paper de responsable de la informació, a causa de la naturalesa, la grandària i els recursos disponibles de l'organització recaurà en el Comitè de Seguretat. Si procedira, es detallaria el nomenament de responsables delegats de seguretat i les funcions que se'ls delegarien.

Funcions del responsable de la informació:

a. Determinar els requisits de seguretat de la informació tractada segons els paràmetres de l'annex I de l'ENS.

b. Acceptar els nivells de risc residual que afecten la informació.

2. El responsable del servei

El Comitè de Seguretat assumirà el paper de responsable del servei i es responsabilitza d'alinear totes les activitats de l'organització en matèria de seguretat, entre les qual destaquen la seguretat física (seguretat de les instal·lacions), la seguretat de la informació, la seguretat i la conformitat legal, i els plans de contingència.

Funcions del responsable del servei:

a. Determinar els requisits de seguretat dels serveis prestats, segons els paràmetres de l'annex I de l'ENS.
b. Coordinar les funcions de seguretat de l'organització.
c. Vetlar pel compliment de la normativa d'aplicació legal, reguladora i sectorial.
d. Vetlar per l'alineament de les activitats de seguretat i els objectius de l'organització.
e. Acceptar els nivells de risc residual que afecten el servei i la informació.
f. Aprovar les mesures de seguretat.
g. Aprovar les mesures tècniques del sistema abans de posar-les en pràctica.

3. El responsable de la seguretat

El responsable de la seguretat (de l'ENS) és designat pel direcgtor de l'organització, segons el procediment establert en aquest document, en l'apartat sobre procediments de designació.

Funcions del responsable de seguretat:

Ha de planificar el que s'ha de fer en matèria de seguretat i supervisar que s'haja fet adequadament.

Les funcions essencials del responsable de la seguretat són:

a. Determinar les decisions de seguretat pertinents per satisfer els requisits establerts pels responsables de la informació i el servei.
b. Mantenir la seguretat de la informació manejada i dels serveis prestats pels sistemes d'informació.
c. Promoure la formació i la conscienciació en matèria de seguretat de la informació.
d. Fer de secretari del Comitè de Seguretat.

4. El responsable del sistema

El responsable del sistema s'encarrega de la part operativa del sistema d'informació d'acord amb les mesures de seguretat determinades pel responsable de la seguretat

Funcions del responsable del sistema:

a. Desenvolupar, operar i mantenir el sistema d'informació durant tot el seu cicle de vida, incloses les seues especificacions, la instal·lació i la verificació del seu correcte funcionament.

b. Suspendre l'accés a la informació o la prestació del servei si té coneixement que hi ha deficiències greus de seguretat.

c. Definir la topologia i la gestió del sistema d'informació i establir els criteris d'ús i els serveis disponibles en aquest.

d. Cerciorar-se que les mesures de seguretat s'integren adequadament en el marc general de seguretat.

e. Complir les funcions de l'administrador de la seguretat del sistema.

f. Encarregar-se de la gestió, la configuració i l'actualització, si és el cas, del "hardware" i el "software" dels mecanismes i els serveis de seguretat.

g. Monitorar l'estat de seguretat due donen les eines de gestió de d'esdeveniments de seguretat i els mecanismes d'auditoria tècnica.

6.3. Procediments de designació

Les responsabilitats i les funcions indicades en aquesta política de seguretat es compliran per la definició de diferents papers que s'han vinculat a elles. Serà competència de la Vicepresidència Executiva designar la persona, el comitè o l'entitat que jugue un paper determinat i precisar les seues funcions i responsabilitats en el marc establert per aquesta política.

Els papers de seguretat es revisaran en el cas que existisca una vacant, que s'haurà de cobrir en el termini adequat seguint el mateix procediment.

6.4. Política de seguretat de la informació

El Comitè de Seguretat tindrà la missió de revisar anualment la política seguretat de la informació i proposar la revisió o el seu manteniment. La política l'aprovarà La Vicepresidència Executiva i la difondrà la Gerència perquè la coneguen tot els afectats.

7. DADES DE CARÀCTER PERSONAL

La FGUV tracta dades de caràcter personal. El document de seguretat al qual tindran accés només els qui estiguen autoritzats recollirà els fitxers afectats i els responsables corresponents. Tots els sistemes d'informació de la FGUV s'ajustaran als graus de seguretat requerits per la normativa per a la naturalesa i la finalitat de les dades de caràcter personal recollits en el document de seguretat indicat.

8. GESTIÓ DE RISCOS

L'organització haurà de fer una anàlisi de riscos de tots els sistemes i avaluar les amenaces i els riscos als quals estiguen exposats. Aquesta anàlisi es farà:

- Regularment almenys una vegada cada any.
- Quan canvie la informació manejada.
- Quan canvien els serveis prestats.
- Quan ocórrega un incident greu de seguretat.
- Quan es comuniquen vulnerabilitats greus.

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

Es prestarà especial atenció a l'anàlisi dels riscos que es deriven del tractament de les dades personals.

9. DESENVOLUPAMENT DE LA POLÍITCA DE SEGURETAT DE LA INFORMACIÓ

El objectius d'aquesta política de seguretat s'assoliran mitjançant el desenvolupament de la documentació que componen les normes i procediments de seguretat associats al compliment de l'Esquema Nacional de Seguretat. Per a la seua organització s'ha establert una norma per a la gestió de la documentació que fixa les directrius per a l'organització, la gestió i l'accés.

La revisió anual d'aquesta política correspon al Comitè de Seguretat de la Informació que, en cas que siga necessari, proposarà millores d'aquesta perquè les aprove el mateix òrgan que l'aprovà inicialment.

Aquesta política de seguretat de la informació complementa la política de seguretat en diferents matèries:

- Normes d'ús personal dels recursos informàtics i telemàtics de la Universitat de València.
- Anàlisi de riscos realitzats.

- Avaluacions d'impacte.
- Normativa de seguretat.

Aquesta política es desenvoluparan per mitjà de la normativa de seguretat que afronte aspectes específics. La normativa de seguretat estarà a la disposició de tots els membres de l'organització que necessiten conèixer-la, en particular dels qui utilitzen, operen o administren els sistemes d'informació i comunicació. La normativa de seguretat estarà disponible en la intranet.

10. OBLIGACIONS DEL PERSONAL

Tots els membres de la FGUV tindran l'obligació de conèixer i complir aquesta política de seguretat de la informació i la normativa de seguretat. Serà responsabilitat del Comitè de Seguretat disposar els mitjans necessaris perquè la informació arribe als afectats.

Tots els membres de la FGUV assistiran a una sessió de conscienciació sobre seguretat de les TIC en el moment de la incorporació. A més, s'establirà un programa de conscienciació contínua per atendre a tots els membres de la FGUV.

Els qui tinguen responsabilitats sobre l'ús, l'operació o l'administració de sistemes de TIC rebran formació per al maneig segur dels sistemes en la mesura en què la necessiten per a fer el seu treball. La formació serà obligatòria abans d'assumir una responsabilitat, tant si es tracta de la primera assignació com si es tracta d'un canvi de lloc de treball o de responsabilitats en aquest.

11. TERCERES PARTS

Quan la FGUV preste serveis a altres organismes o manege informació d'altres organismes se'ls farà partícips d'aquesta política de seguretat de la informació i s'establiran canals per a comunicar i coordinar els respectius comitès de seguretat i els procediments adequats per a adoptar les mesures adequades davant d'incidents de seguretat.

Quan la FGUV utilitze serveis de tercers o els cedisca informació es faran es faran partícips d'aqueta política de seguretat i de la normativa de seguretat que concerneix aquests serveis o a aquesta informació. El tercer de què es tracte quedarà subjecte a les obligacions establertes en aquesta normativa i podrà desenvolupar els seus propis procediments operatius per complir-la. S'establiran procediments específics de comunicació i resolució d'incidències. Es garantirà que el personal dels tercers estiga adequadament conscienciat en matèria de seguretat, almenys amb el mateix nivwll que l'establert en aquesta política.

Quan un tercer no puga complir aquesta política en algun dels seus aspectes segons es requereix en els paràgrafs anteriors, el responsable de seguretat haurà de fer un informe en què precise els riscos que puga haver-hi i la forma de tractar-los. Es requerirà l'aprovació d'aquest informe per part dels responsables de la informació i els serveis afectats abans de seguir endavant.

L´original està signat per la Vicepresidenta Executiva en data 15/07/2025