# Reglament de seguretat de la informació en la utilització de mitjans electrònics de la Universitat de València


VNIVERSITAT DE VALÈNCIA

# Reglament de seguretat de la informació en la utilització de mitjans electrònics de la Universitat de València

## Exposició de motius

## I[1]

Conforme al que es disposa en el Reial decret 311/2022, pel qual es regula l'Esquema Nacional de Seguretat (ENS, d'ara endavant), aquest reglament conté les normes de Seguretat de la Informació que afecten als usuaris dels sistemes d'informació gestionats per la Universitat de València o sota la seua responsabilitat i que es troben afectats per l'abast del ENS. Els seus continguts es basen en les directrius de caràcter més general definides en la Política de Seguretat de la Informació de la Universitat de València.

La finalitat de l'Esquema Nacional de Seguretat és la creació de les condicions necessàries de confiança en l'ús dels mitjans electrònics, a través de mesures per a garantir la seguretat dels sistemes, les dades, les comunicacions, i els serveis electrònics, que permeta als ciutadans i a les Administracions públiques, l'exercici de drets i el compliment de deures a través d'aquests mitjans. Per tant, la Seguretat de la Informació és un esforç conjunt. Requereix la implicació i participació de tots els membres de la Universitat de València que es troben afectats per l'abast del ENS per a l'acompliment del seu treball: PTGAS, PDI i si escau el personal extern vinculat a prestacions de serveis a la Universitat de València. Per açò , cadascun d'ells ha de complir els requeriments del Reglament de Seguretat de la Informació i la seua documentació associada. Els qui deliberadament o per negligència incomplisquen el Reglament de Seguretat podrien estar subjectes a responsabilitat.

El present Reglament fixa les directrius generals per a l'ús adequat dels recursos de tractament d'informació que la Universitat de València posa a la disposició dels seus usuaris per a l'exercici de les seues funcions i que, correlativament, assumeixen les obligacions descrites, comprometent-se a complir amb el que es disposa en els següents epígrafs. El Reglament de Seguretat de la Informació serà mantingut, actualitzat i adequat a les finalitats de la Universitat, alineant-se amb el context de gestió de riscos de la institució.

## II

L'Esquema Nacional de Seguretat defineix un sistema d'informació com un conjunt organitzat de recursos perquè la informació es puga arreplegar, emmagatzemar, processar o tractar, mantenir, usar, compartir, distribuir, posar a disposició, presentar o transmetre.

El bon funcionament de la Universitat depèn en gran manera dels Sistemes d'Informació i de la pròpia informació que en ells s'emmagatzema.

La utilització de recursos tecnològics per al tractament de la informació és essencial i compleix amb una doble finalitat per a la Universitat de València. Primerament, la de facilitar i agilitzar la tramitació de procediments administratius, mitjançant l'ús d'eines informàtiques i aplicacions de gestió. En segon lloc, proporcionar informació completa, homogènia, actualitzada i fiable.

Per açó, la utilització d'equipament informàtic i de comunicacions és actualment una necessitat en qualsevol universitat pública. Aquests mitjans i recursos es posen a la disposició dels usuaris com a instruments de treball per a l'acompliment de la seua activitat professional, raó per la qual

[1] Modificat pel Consell de Govern d'1 de juny de 2021. ACGUV 127/2021. Modificat pel Consell de Govern de 3 d'octubre de 2023. ACGUV 245/2023.

competeix a la Universitat de València determinar les normes, condicions i responsabilitats sota les quals han d'utilitzar-se.

Els Sistemes d'Informació constitueixen elements bàsics per al desenvolupament de les missions encomanades a la Universitat de València, per la qual cosa els usuaris han d'utilitzar aquests recursos de manera que es preserven en tot moment les dimensions de la seguretat sobre les informacions manejades i els serveis prestats: disponibilitat, integritat, confidencialitat, autenticitat i traçabilitat.

La Universitat disposa d'un Sistema de Gestió de Seguretat de la Informació integrat amb el compliment de les obligacions de l'Esquema Nacional de Seguretat. Totes les polítiques i procediments als quals es fa referència en aquest document sobre el Sistema de Gestió de Seguretat de la Informació han sigut revisats, aprovats i impulsats pel Comitè de Gestió i Coordinació de la Seguretat de la Informació de la Universitat de València.

## III

El Reglament de Seguretat de la Informació té com a missió establir objectius de Seguretat de la Informació per a la Universitat, així com protegir els actius d'informació i aconseguir la major eficàcia i seguretat en el seu ús. Aquests objectius inclouen l'adopció d'una sèrie de mesures organitzatives i normes que es presenten en aquest document amb la finalitat de protegir la informació de la Universitat de València. L'objectiu principal del desenvolupament d'aquest Reglament és garantir als usuaris l'accés a la informació amb la quantitat i qualitat que es requereix per a l'acompliment de les seues funcions, així com evitar pèrdues d'informació i accessos no autoritzats a la mateixa.

Per a aconseguir els objectius en matèria de seguretat resulta necessari definir obligacions integrades per un conjunt d'accions positives (deure fer alguna cosa) o omisives (deure abstenir-se de fer). Aquestes obligacions deriven directament de la naturalesa de les tecnologies de la informació que constitueixen la nostra eina natural de treball i no són una altra cosa que l'actualització del deure secret i de preservar la informació administrativa que incumbeix a tot empleat públic.

La seguretat és un instrument al servei de l'organització i de tots els usuaris, capaç de proporcionar confiança en els sistemes, preservar l'exercici de les funcions i responsabilitats pròpies de cada usuari i garantir la qualitat i veracitat de la informació objecte de tractament. Del compliment de la Política i la Normativa de seguretat depèn la garantia dels drets dels ciutadans en la seua relació amb l'Administració.

La seguretat s'articula entorn de cinc grans objectius-principis:

- Confidencialitat: La informació pertanyent a la Universitat de València ha de ser coneguda exclusivament per les persones autoritzades, prèvia identificació, en el moment i pels mitjans habilitats.
- Integritat: La informació de la Universitat de València deu ser completa, exacta i vàlida, sent el seu contingut el facilitat pels afectats sense cap tipus de manipulació.
- Autenticitat: La informació de la Universitat de València és generada per un autor adequadament identificat, la qual cosa inclou el no repudi de la informació introduïda doncs es garanteix que l'emissor de la informació és qui diu ser.
- Disponibilitat: La informació de la Universitat està accessible i utilitzable pels usuaris autoritzats i identificats en tot moment, quedant garantida la seua pròpia persistència davant qualsevol eventualitat.
- Traçabilitat: Suposa que les actuacions d'usuaris autoritzats i identificats es poden rastrejar a posteriori per a definir qui ha accedit o modificat certa informació.

El conjunt d'obligacions que deriven d'aquesta Normativa són funcionals a aquests objectius i es defineixen en directa relació amb els actius protegits i la sensibilitat de la informació objecte de protecció.

## Capítol I. Disposicions generals

**Article 1. Àmbit d'aplicació[2].**

1. Aquest reglament afecta a tots els actius d'informació de la Universitat implicats en l'abast de l'Esquema Nacional de Seguretat, tant a ordinadors personals o servidors, xarxes, aplicacions, sistemes operatius, processos i documentació que pertanyen o són administrats per la Universitat de València.

2. D'acord amb el que disposa la Política de Seguretat de la Informació de la Universitat de València aquesta normativa obliga als usuaris amb accés als recursos informàtics o a la informació que pot ser tractada o extreta del sistema d'informació universitari, als següents serveis que integren i a qualsevol suport que la continga:

   a) Gestió acadèmica (Docència-Estudis):
      • Serveis de Gestió acadèmica
      • Automatrícula
      • Gestió d'actes
      • Gestió de títols
      • Aula virtual
      • Secretaria virtual
      • Portal de l'alumnat
   b) Extensió universitària
   c) Seu electrònica (Sector públic):
      • PTGAS-PDI
      • De investigació
      • De l'estudiantat
      • Serveis a externs
      • Perfil del contractant
   d) Gestió econòmica (Règim Econòmic):
   e) Portal web de la Universitat (Publicacions):
      • Informació administrativa
   f) Sistema de gestió de Recursos Humans (Professorat i PTGAS)
      • Portal de personal
      • Gestió de nòmines.
   g) Biblioteca (Gestió Biblioteca)
   h) Control d´infraestructura i instal·lacions (CPD)

3. Aquest reglament és aplicable i d'obligat compliment per a tots els usuaris dels Sistemes d'Informació de la Universitat de València sota l'àmbit d'aplicació del ENS, d'acord amb la definició de l'apartat anterior. En l'àmbit del present reglament, s'entenen per usuaris dels Sistemes d'Informació sota l'àmbit d'aplicació del ENS:

[2] Modificat pel Consell de Govern d'1 de juny de 2021. ACGUV 127/2021.

a) Els empleats públics de la Universitat de València que requerisquen accedir als Sistemes d'Informació descrits anteriorment per a l'acompliment de les seues funcions.

b) El personal sense vinculació contractual amb la Universitat de València que siga membre de comissions o òrgans relacionats amb aquesta i que manege informació extreta des dels Sistemes d'Informació descrits anteriorment.

c) El personal de prestadors de serveis, entitats col·laboradores o qualsevol un altre amb algun tipus de vinculació amb la Universitat de València quan utilitze o posseïsca accés als Sistemes d'Informació descrits anteriorment.

**Article 2. Classificació de la informació conforme a la seua sensibilitat**

1. La informació de la Universitat de València està classificada en 3 categories depenent del seu grau de confidencialitat. Tot empleat ha de ser conscient d'aquesta classificació:

   a) No classificada: Aquesta informació pot ser compartida sense restriccions. Té caràcter públic.

   b) Restringida: La informació Restringida és sempre per a ús intern i pot ser compartida entre el personal afectat pel present reglament amb competència en el seu tractament. A més, la informació restringida pot ser catalogada com de difusió limitada. En aqueix cas, pot ser compartida també amb tercers interessats com administrats o proveïdors vinculats amb algun tipus de contracte.

   c) Confidencial: Aquesta informació ha de ser únicament compartida entre personal que en virtut de les seues funcions haja de ser coneixedor de la mateixa.

2. Correspon al Comitè de Gestió i Coordinació de la Seguretat de la Informació la classificació de la informació continguda en els Sistemes d'Informació de la Universitat. Com a principi general, la informació es classifica com Restringida. En aquells supòsits en els quals resulte necessària la reclassificació d'algun tipus d'informació o document amb motiu de l'acompliment de les funcions pròpies del servei, aquesta serà decidida pel corresponent Cap de Servei tenint en compte les directrius fixades pel Comitè de Gestió i Coordinació de la Seguretat de la Informació.

3. Es considerarà la informació pública de matèries no classificades com a "ÚS OFICIAL" per a la informació amb algun tipus de restricció en el seu maneig per la seua sensibilitat i confidencialitat.

## Capítol II. Normes de seguretat

**Article 3. Abast.**

1. Les normes de seguretat d'aquest reglament abasten els següents aspectes:

   a) Controls d'accés físic i lògic

   b) Ús, manteniment i destrucció de dispositius o suports que continguen informació protegida

   c) Eixides i entrades de dades

   d) Correu electrònic i xarxa corporativa

   e) Recursos informàtics

   f) Incidències de seguretat

   g) Informació institucional i dades personals

   h) Publicació en web

2. Les normes de seguretat comporten obligacions concretes que hauran de satisfer els usuaris en els termes en què es defineixen en els següents articles d'aquest reglament.
3. Els procediments necessaris per a l'aplicació de les normes i polítiques de seguretat de la Universitat de València seran desenvolupats pel Servei de Ciberseguretat i seran informats pel Comitè de Gestió i Coordinació de la Seguretat de la Informació.

**Article 4. Controls d'accés físic i lògic**

1. L'accés físic a àrees que continguen informació confidencial o restringida només es permet al personal autoritzat pel Responsable de la Unitat de Gestió corresponent, excepte en els supòsits d'urgència o emergència.
2. L'accés als Centres de Processament de dades (CPD) com a les infraestructures de comunicacions de la Universitat de València està restringit al personal del Servei d'Informàtica, en cas de visites externes es realitzaran les mateixes sempre acompanyades per un empleat del Servei d'Informàtica.
3. En cas de ser necessari l'accés a un CPD o a la infraestructura de comunicacions per part de personal no membre del Servei d'Informàtica, el responsable de la visita formalitzarà a través d'una Petició de Servei *"Sol·licitud accés Àrees Segures"* al Responsable de Seguretat, la sol·licitud d'autorització per a aquest accés.
4. Cada usuari podrà accedir exclusivament als recursos i sistemes d'informació autoritzats.
5. L'accés als ordinadors i equips vinculats al lloc de treball ha de realitzar-se amb l'usuari i contrasenya assignat.
6. En cas d'absència del lloc de treball en horari d'oficina, ha de procedir-se al bloqueig de l'ordinador, que en tot cas haurà de produir-se automàticament després de 15 minuts d'inactivitat.
7. En el disseny del lloc de treball s'assegurarà que la pantalla no resulte fàcilment accessible o llegible per a tercers no autoritzats.
8. Ha de procedir-se a apagar l'ordinador fóra de l'horari de treball, així com evitar l'ús del mateix per terceres persones no autoritzades.
9. S'ha de protegir els identificadors d'usuari i contrasenya personal i no revelar-los a ningú. Les contrasenyes no han de ser emmagatzemades en fitxers llegibles, macros, ordinadors sense control d'accés o cap altra manera o lloc on puguen ser accedides per tercers sense autorització.
10. Mai s'han de facilitar les dades d'usuari i contrasenya a terceres persones, encara que es tracte de personal propi de la Universitat.
11. Es procedirà al canvi de contrasenyes quan ho sol·licite el sistema i sempre haurà d'utilitzar contrasenyes segures.
12. En cas d'incidència relacionada amb la contrasenya haurà de notificar-se immediatament a través de el "Procediment de Gestió d'Incidències".
13. L'accés remot (des de fora de la xarxa de la Universitat) als sistemes d'informació haurà de realitzar-se mitjançant una connexió segura. L'usuari aplicarà a l'equip que utilitze les normes de seguretat contingudes en aquest apartat per als equips situats en llocs de la Universitat de València.

**Article 5. Ús, manteniment i destrucció de dispositius o suports que continguen informació protegida**

1. No s'ha de deixar abandonats documents amb informació protegida en la impressora, fax o dispositius similars, o desatesa en el lloc de treball.

2. La impressió o fotocòpia de documents ha de limitar-se únicament aquells que siguen estrictament necessaris i preferiblement a doble cara. Els documents rebutjats, incloses les fotocòpies errònies no podran ser reutilitzats quan continguen dades personals o informació confidencial o restringida havent-se de procedir a la seua immediata destrucció.
3. En el cas de reutilització de documents impresos l'usuari comprovarà prèviament que aquests no contenen dades de caràcter personal, comunicant la incidència en cas contrari.
4. Quan la informació siga qualificada com restringida o confidencial haurà de guardar-se en els llocs designats a aquest efecte pel Responsable de la Unitat de Gestió corresponent, al final de la jornada i, en tot cas, en abandonar el lloc quan la seua conformació no permeta que estiga sota el control d'algun usuari.
5. Abans d'abandonar sales comunes o permetre que alguna persona aliena entre, es netejaran adequadament les pissarres de les sales de reunions o despatxos, cuidant que no quede cap tipus d'informació sensible o que poguera ser reutilitzada.
6. La destrucció de qualsevol tipus de suport automatitzat (CD, DVD, disc dur, memòria usb, etc.) o manual (paper, cintes de vídeo, etc.) es realitzarà de manera que les dades que contenien no siguen recuperables i si escau a través dels procediments establits.
7. No podran donar-se suports informàtics a cap tercer sense que prèviament s'haja realitzat un esborrat complet del mateix.
8. No és possible modificar o afegir components físics (per ex. un disc dur) dels equips informàtics i dispositius de comunicació, excepte autorització expressa del Servei d'Informàtica. En tot cas, aquestes operacions només podran realitzar-se pel personal de suport tècnic autoritzat.
9. Tret que el Comitè de Gestió i Coordinació de la Seguretat de la Informació la Universitat expressament ho autoritze queda prohibit allotjar informació confidencial o restringida pròpia de la Universitat de València en servidors externs en el "núvol" no oferits per la pròpia institució, en particular quan es tracte de dades personals continguts en els sistemes d'informació. En cas de necessitat es farà ús dels espais de disc corporatius (https://disco.uv.es).
10. L'usuari és responsable d'un ús adequat dels dispositius portàtils propietat de la Universitat de València. Ha de mantenir-los sota la seua custòdia i no permetre el seu ús a cap tercer. Si es connecta externament a la Universitat ha de fer-ho sempre mitjançant una connexió segura. Si el dispositiu fos robat o extraviat ha de notificar-se immediatament a la Universitat de València, seguint el "Procediment de Gestió d'Incidències".

**Article 6. Eixides i entrades de dades[3]**

1. Es prohibeix expressament l'ús de suports d'informació extraïble (dispositius d'emmagatzematge USB, memòries flaix, etc.) amb dades confidencials o restringits de la Universitat de València sense autorització del Responsable de la Unitat de Gestió. Es recomana com a procediment adequat a aquesta fi l'ús d'espais de disc corporatiu. Qualsevol informació que siga emmagatzemada en un suport d'informació extraïble haurà de ser emprada exclusivament per a motius de treball, i la informació haurà d'eliminar-se o guardar-se en els llocs designats a aquest efecte.
2. Per a tota entrada i/o eixida d'informació no prevista per les aplicacions corporatives s'ha de sol·licitar autorització formal al Responsable de la Unitat de Gestió que corresponga.

[3] Modificat pel Consell de Govern d'1 de juny de 2021. ACGUV 127/2021.

**Article 7. Correu electrònic i xarxa corporativa**

1. L'ús del correu electrònic per a comunicacions corporatives estarà limitat als comptes de la Universitat, i haurà de complir amb el propòsit de l'acompliment del treballador, sent necessària la inclusió en els missatges de correu sortints de la clàusula relativa a la confidencialitat de les dades i la utilització del contacte de correu electrònic exclusivament per a la fi d'aquest correu.
2. L'accés a informació corporativa es realitzarà a través de la xarxa de dades corporativa. També es realitzarà mitjançant la Intranet, l'accés de la qual estarà limitat als usuaris que hagen d'usar-la mitjançant autenticació per nom d'usuari i contrasenya.
3. L'enviament de dades o informació a tercers (cessió de dades), per mitjà del correu electrònic, transferència FTP o equivalent haurà d'estar autoritzada, pel Responsable de la Unitat de Gestió, per a la finalitat exclusiva per a la qual siga necessari. Quan la informació siga qualificada com a confidencial només serà admissible mitjançant un procediment que impedisca accessos no autoritzats.
4. No han d'obrir-se correus electrònics no sol·licitats, de remitents desconeguts o de remitents coneguts que puguen alçar sospites. Així mateix, no han d'executar-se arxius no confiables.
5. La consulta de comptes de correu personal no corporatiu en l'ordinador del lloc de treball s'haurà de realitzar exclusivament a través de sistemes webmail, amb la cautela de no obrir correus electrònics no sol·licitats, de remitents desconeguts o de remitents coneguts que alcen sospites. Així mateix, no s'han d'executar arxius no confiables.
6. L'usuari es fa responsable dels accessos a Internet que puguen comprometre la seguretat de l'equip.

**Article 8. Recursos informàtics***

1. Tot usuari ha de mantenir actualitzada la seguretat dels sistemes operatius, antivirus i tallafocs (firewalls) del seu equip de treball mitjançant actualitzacions automàtiques i, en tot cas, d'acord amb els procediments establits o amb l'assistència del Centre d'Atenció a l'Usuari de la Universitat (CAU). Els sistemes operatius i aplicacions han de disposar de suport i manteniment per part del fabricant, no permetent-se l'ús de sistemes operatius ni aplicacions que hagen sobrepassat el seu cicle de vida útil fins a un màxim de 18 mesos.
2. Els equips de la Universitat de València connectats a la xarxa cablejada han de tindre instal·lat el programari antivirus proporcionat per la institució, el qual es troba accessible dins del catàleg de programari (https://software.uv.es).
3. L'usuari únicament podrà instal·lar els programes per als quals la Universitat de València tinga llicència d'ús. En particular, els habilitats en el catàleg de programari (https://software.uv.es) de la Universitat de València. No és possible instal·lar programari no autoritzat o sense llicència, ni executar o guardar arxius no confiables.
4. En cas d'incompliment de les obligacions establertes en qualsevol dels apartats anteriors es podrà procedir, com a mesura de prevenció de riscos de seguretat en la informació, a la desconnexió dels dispositius afectats de la xarxa de la Universitat de València. En tot cas, es prestarà suport als usuaris per tal de resoldre la incidència i actualitzar els seus equips.

* Modificat pel Consell de Govern de 3 d'octubre de 2023. ACGUV 245/2023.

**Article 9. Incidències de seguretat**

L'usuari ha de comunicar qualsevol Incidència de Seguretat de la qual tinga coneixement (possible virus, comportaments sospitosos...) seguint el *"Procediment de Gestió d'Incidències"*.

**Article 10. Informació institucional i dades personals**

1. La informació continguda en els Sistemes d'Informació de la Universitat de València és de la seua exclusiva propietat, per la qual cosa els usuaris han d'abstenir-se de comunicar, divulgar, distribuir o posar en coneixement o a l'abast de tercers (externs o interns no autoritzats) aquesta informació, excepte autorització expressa del Comitè de Gestió i Coordinació de la Seguretat de la Informació.
2. Tot usuari (de la Universitat de València o de terceres organitzacions) que, en virtut de la seua activitat professional, poguera tenir accés a dades de caràcter personal, està obligat a guardar secret sobre aquestes i a aplicar les mesures previstes en el document de seguretat. Aquest deure es mantindrà de manera indefinida, fins i tot més enllà de la relació laboral o professional amb la Universitat de València.

**Article 11. Publicació en web**

1. La publicació de continguts en la web de la Universitat de València es limitarà als documents o informacions categoritzats com "No classificats".
2. La informació publicada ha de garantir els principis d'autenticitat i integritat.
3. Els gestors i editors de pàgines web asseguraran la disponibilitat de la informació durant el període previst de vigència de la mateixa procedint a la seua retirada quan es produïsca el venciment.

**Article 12. Gestió del reglament.**

La gestió d'aquest Reglament correspon al Comitè de Gestió i Coordinació de la Seguretat de la Informació, que és competent per a:

a) Interpretar els dubtes que puguen sorgir en la seua aplicació.

b) Verificar la seua efectivitat.

c) Proposar la seua revisió.

**Article 13. Revisió de les normes de seguretat**

1. Anualment, o de manera extraordinària quan existeixen circumstàncies que així ho aconsellen, el Comitè de Gestió i Coordinació de la Seguretat de la Informació revisarà el present Reglament.
2. La revisió s'orientarà tant a la identificació d'oportunitats de millora en la gestió de la seguretat de la informació, com a l'adaptació als canvis en el marc legal, infraestructura tecnològica i qualsevol altre aspecte rellevant.

**Article 14. Divulgació.**

1. El Responsable de Seguretat és la persona encarregada de la difusió de la versió aprovada d'aquest document.

2. Sense perjudici de la competència del Responsable de Seguretat, la Universitat de València mitjançant l'acció dels serveis competents adoptarà les mesures oportunes per difondre aquesta normativa, i per formar i conscienciar els usuaris.

**Article 15. Responsabilitat.**

Tots els usuaris dels sistemes d'informació sota l'abast de l'Esquema Nacional de Seguretat en la Universitat de València estan obligats a complir la present normativa. El seu incompliment genera responsabilitat que se substanciarà conforme al procediment establit a aquest efecte en cada cas.

## Disposició addicional primera

1. Les previsions d'aquesta normativa no són incompatibles amb aquelles obligacions derivades del lloc de treball i d'altres normatives.
2. Es faculta el responsable de seguretat de la Universitat de València per:
    a) Notificar si escau als usuaris instruccions concretes sobre les condicions de compliment de les normes de seguretat.
    b) Establir normes de seguretat addicionals prèvia comunicació al Comitè de Gestió i Coordinació de la Seguretat de la Informació quan ho justifiquen motius d'urgència o necessitat o adoptar aquelles decisions que resulten indispensables per garantir l'objectiu de la seguretat. En aquest cas, regiran de manera provisional tot i incorporant-se a aquesta normativa quan siga revisada.

    c) Definir els procediments de gestió de la seguretat que resulten necessaris per a fer efectives les disposicions d'aquesta normativa. Aquests procediments es notificaran al Comitè de Gestió i Coordinació de la Seguretat de la Informació.

## Disposició addicional segona[4]

En tot allò no previst per aquesta normativa s'aplicarà supletòriament el que disposen les normes reguladores de l'esquema nacional de seguretat; el Reglament (UE) 2016/679 del Parlament i del Consell, relatiu a la protecció de les persones físiques pel que fa al tractament de dades personals i a la lliure circulació d'aquestes dades; la Llei orgànica 3/2018, de protecció de dades de caràcter personal i garantia de drets digitals, i la normativa que la desplega.

## Disposició Final. Entrada en vigor

Aquest reglament es difondrà a tot el personal de la Universitat mitjançant la seua publicació i entrarà en vigor transcorregut un mes natural des de la data d'aprovació pel Consell de Govern de la Universitat.

**Aprovat pel Consell de Govern de 22 de desembre de 2014. ACGUV 227/2014.**

[4] Modificat pel Consell de Govern d'1 de juny de 2021. ACGUV 127/2021.

**Modificat pel Consell de Govern d'1 de juny de 2021. ACGUV 127/2021.**
**Modificat pel Consell de Govern de 3 d'octubre de 2023. ACGUV 245/2023.**

# Reglamento de seguridad de la información en la utilización de medios electrónicos de la Universitat de València


VNIVERSITAT DE VALÈNCIA

# Reglamento de seguridad de la información en la utilización de medios electrónicos de la Universitat de València

## Exposición de motivos

## I[1]

Conforme a lo que se dispone en el Real Decreto 311/2022, por el cual se regula el Esquema Nacional de Seguridad (ENS, de ahora en adelante), este reglamento contiene las normas de Seguridad de la Información que afectan a los usuarios de los sistemas de información gestionados por la Universitat de València o bajo su responsabilidad y que se encuentran afectados por el alcance del ENS. Sus contenidos se basan en las directrices de carácter más general definidas en la Política de Seguridad de la Información de la Universitat de València.

La finalidad del Esquema Nacional de Seguridad es la creación de las condiciones necesarias de confianza en el uso de los medios electrónicos, a través de medidas para garantizar la seguridad de los sistemas, los datos, las comunicaciones, y los servicios electrónicos, que permita a los ciudadanos y a las Administraciones públicas, el ejercicio de derechos y el cumplimiento de deberes a través de estos medios. Por lo tanto, la Seguridad de la Información es un esfuerzo conjunto.

Requiere la implicación y participación de todos los miembros de la Universitat de València que se encuentren afectados por el alcance del ENS para el desempeño de su trabajo: PTGAS, PDI y si procede el personal externo vinculado a prestaciones de servicios en la Universitat de València. Por esto, cada uno de ellos tiene que cumplir los requerimientos del Reglamento de Seguridad de la Información y su documentación asociada. Quienes deliberadamente o por negligencia incumplan el Reglamento de Seguridad podrían estar sujetos a responsabilidad.

El presente Reglamento fija las directrices generales para el uso adecuado de los recursos de tratamiento de información que la Universitat de València pone a disposición de sus usuarios para el ejercicio de sus funciones y que, correlativamente, asumen las obligaciones descritas, comprometiéndose a cumplir con lo dispuesto en los siguientes epígrafes. El Reglamento de Seguridad de la Información será mantenido, actualizado y adecuado a las finalidades de la Universidad, alineándose con el contexto de gestión de riesgos de la institución.

## II

El Esquema Nacional de Seguridad define un sistema de información como un conjunto organizado de recursos para que la información se pueda recoger, almacenar, procesar o tratar, mantener, usar, compartir, distribuir, poner a disposición, presentar o transmitir.

El buen funcionamiento de la Universitat depende en gran medida de los Sistemas de Información y de la propia información que en ellos se almacena.

La utilización de recursos tecnológicos para el tratamiento de la información es esencial y cumple con una doble finalidad para la Universitat de València. Primerament, la de facilitar y agilizar la tramitación de procedimientos administrativos, mediante el uso de herramientas informáticas y aplicaciones de gestión. En segundo lugar, proporcionar información completa, homogénea, actualizada y fiable.

Por ello, la utilización de equipamiento informático y de comunicaciones es actualmente una necesidad en cualquier universidad pública. Estos medios y recursos se ponen a disposición de los

[1] Modificado por el Consejo de Gobierno de 1 de junio de 2021. ACGUV 127/2021. Modificado por el Consejo de Gobierno de 3 de octubre de 2023. ACGUV 245/2023.

usuarios como instrumentos de trabajo para el desempeño de su actividad profesional, razón por la cual compete a la Universitat de València determinar las normas, condiciones y responsabilidades bajo las cuales tienen que utilizarse.

Los Sistemas de Información constituyen elementos básicos para el desarrollo de las misiones encomendadas en la Universitat de València, por lo cual los usuarios tienen que utilizar estos recursos de forma que se preservan en todo momento las dimensiones de la seguridad sobre las informaciones manejadas y los servicios prestados: disponibilidad, integridad, confidencialidad, autenticidad y trazabilidad.

La Universitat dispone de un Sistema de Gestión de Seguridad de la Información integrado con el cumplimiento de las obligaciones del Esquema Nacional de Seguridad. Todas las políticas y procedimientos a los cuales se hace referencia en este documento sobre el Sistema de Gestión de Seguridad de la Información han sido revisados, aprobados e impulsados por el Comité de Gestión y Coordinación de la Seguridad de la Información de la Universitat de València.

## III

El Reglamento de Seguridad de la Información tiene como misión establecer objetivos de Seguridad de la Información para la Universidad, así como proteger los activos de información y conseguir la mayor eficacia y seguridad en su uso. Estos objetivos incluyen la adopción de una serie de medidas organizativas y normas que se presentan en este documento con el fin de proteger la información de la Universitat de València. El objetivo principal del desarrollo de este Reglamento es garantizar a los usuarios el acceso a la información con la cantidad y calidad que se requiere para el desempeño de sus funciones, así como evitar pérdidas de información y accesos no autorizados a la misma.

Para conseguir los objetivos en materia de seguridad resulta necesario definir obligaciones integradas por un conjunto de acciones positivas (deber hacer algo) u omisivas (deber abstenerse de hacer). Estas obligaciones derivan directamente de la naturaleza de las tecnologías de la información que constituyen nuestra herramienta natural de trabajo y no son otra cosa que la actualización del deber secreto y de preservar la información administrativa que incumbe a todo empleado público.

La seguridad es un instrumento al servicio de la organización y de todos los usuarios, capaz de proporcionar confianza en los sistemas, preservar el ejercicio de las funciones y responsabilidades propias de cada usuario y garantizar la calidad y veracidad de la información objeto de tratamiento. Del cumplimiento de la Política y la Normativa de seguridad depende la garantía de los derechos de los ciudadanos en su relación con la Administración.

La seguridad se articula en torno a cinco grandes objetivos-principios:

- Confidencialidad. La información perteneciente a la Universitat de València tiene que ser conocida exclusivamente por las personas autorizadas, previa identificación, en el momento y por los medios habilitados.
- Integridad. La información de la Universitat de València debe de ser completa, exacta y válida, siendo su contenido el facilitado por los afectados sin ningún tipo de manipulación.
- Autenticidad. La información de la Universitat de València es generada por un autor adecuadamente identificado, lo cual incluye el no repudio de la información introducida pues se garantiza que el emisor de la información es quien dice ser.
- Disponibilidad. La información de la Universitat está accesible y utilizable por los usuarios autorizados e identificados en todo momento, quedando garantizada su propia persistencia ante cualquier eventualidad.

- Trazabilidad. Supone que las actuaciones de usuarios autorizados e identificados se pueden rastrear *a posteriori* para definir quién ha accedido o modificado cierta información.

El conjunto de obligaciones que derivan de esta Normativa son funcionales a estos objetivos y se definen en directa relación con los activos protegidos y la sensibilidad de la información objeto de protección.

# Capítulo I. Disposiciones generales

**Artículo 1. Ámbito de aplicación[2].**

1. Este reglamento afecta a todos los activos de información de la Universitat implicados en el alcance del Esquema Nacional de Seguridad, tanto a ordenadores personales o servidores, redes, aplicaciones, sistemas operativos, procesos y documentación que pertenecen o son administrados por la Universitat de València.

2. De acuerdo con lo que dispone la Política de Seguridad de la Información de la Universitat de València, esta normativa obliga a los usuarios con acceso a los recursos informáticos o a la información que puede ser tratada o extraída del siguiente sistema de información universitaria, a los siguientes servicios que integran y a cualquier apoyo que la contenga:

   a) Gestión académica (Docencia-Estudios):
      - Servicios de Gestión académica
      - Automatrícula
      - Gestión de actas
      - Gestión de títulos
      - Aula virtual
      - Secretaría virtual
      - Portal del alumnado

   b) Extensión universitaria

   c) Sede electrónica (Sector público):
      - PTGAS-PDI
      - De investigación
      - Del estudiantado
      - Servicios a externos
      - Perfil del contratante

   d) Gestión económica (Régimen Económico):

   e) Portal web de la Universitat (Publicaciones):
      - Información administrativa

   f) Sistema de gestión de Recursos Humanos (Profesorado y PTGAS)
      - Portal de personal
      - Gestión de nóminas.

   g) Biblioteca (gestión biblioteca)

   h) Control de infraestructura e instalaciones (CPD)

3. Este reglamento es aplicable y de obligado cumplimiento para todos los usuarios de los Sistemas de Información de la Universitat de València bajo el ámbito de aplicación del ENS,

[2] Modificado por el Consejo de Gobierno de 1 de junio de 2021. ACGUV 127/2021.

de acuerdo con la definición del apartado anterior. En el ámbito del presente reglamento, se entienden por usuarios de los Sistemas de Información bajo el ámbito de aplicación del ENS:

a) Los empleados públicos de la Universitat de València que requieran acceder a los Sistemas de Información descritos anteriormente para el desempeño de sus funciones.

b) El personal sin vinculación contractual con la Universitat de València que sea miembro de comisiones u órganos relacionados con esta y que maneje información extraída desde los Sistemas de Información descritos anteriormente.

c) El personal de prestadores de servicios, entidades colaboradoras o cualquier otro con algún tipo de vinculación con la Universitat de València cuando utilice o posea acceso a los Sistemas de Información descritos anteriormente.

**Artículo 2. Clasificación de la información conforme a su sensibilidad**

1. La información de la Universitat de València está clasificada en tres categorías dependiendo de su grado de confidencialidad. Todo empleado tiene que ser consciente de esta clasificación:

   a) No clasificada. Esta información puede ser compartida sin restricciones. Tiene carácter público.

   b) Restringida. La información restringida es siempre para uso interno y puede ser compartida entre el personal afectado por el presente reglamento con competencia en su tratamiento. Además, la información restringida puede ser catalogada como de difusión limitada. En ese caso, puede ser compartida también con terceros interesados como administrados o proveedores vinculados con algún tipo de contrato.

   c) Confidencial. Esta información tiene que ser únicamente compartida entre personal que en virtud de sus funciones tenga que ser conocedor de la misma.

2. Corresponde al Comité de Gestión y Coordinación de la Seguridad de la Información la clasificación de la información contenida en los Sistemas de Información de la Universidad. Como principio general, la información se clasifica como “Restringida”. En aquellos supuestos en los cuales resulte necesaria la reclasificación de algún tipo de información o documento con motivo del desempeño de las funciones propias del servicio, esta será decidida por el correspondiente Jefe de servicio teniendo en cuenta las directrices fijadas por el Comité de Gestión y Coordinación de la Seguridad de la Información.

3. Se considerará la información pública de materias no clasificadas como "USO OFICIAL" para la información con algún tipo de restricción en su manejo por su sensibilidad y confidencialidad.

## Capítulo II. Normas de seguridad

**Artículo 3. Alcance.**

1. Las normas de seguridad de este reglamento alcanzan los siguientes aspectos:

   a) Controles de acceso físico y lógico.

   b) Uso, mantenimiento y destrucción de dispositivos o soportes que contengan información protegida.

   c) Salidas y entradas de datos.

   d) Correo electrónico y red corporativa.

   e) Recursos informáticos.

   f) Incidencias de seguridad.

   g) Información institucional y datos personales.

h) Publicación en web.

2. Les normas de seguridad comportan obligaciones concretas que tendrán que satisfacer los usuarios en los términos en que se definen en los seguientes artículos de este reglamento.
3. Los procedimientos necesarios para la aplicación de las normas y políticas de seguridad de la Universitat de València serán desarrollados por el Servicio de Ciberseguridad y serán informados por el Comité de Gestión y Coordinación de la Seguridad de la Información.

**Artículo 4. Controles de acceso físico y lógico**

1. El acceso físico a áreas que contengan información confidencial o restringida solo se permite al personal autorizado por el Responsable de la Unidad de Gestión correspondiente, excepto en los supuestos de urgencia o emergencia.
2. El acceso a los Centros de Procesamiento de Datos (CPD) como las infraestructuras de comunicaciones de la Universitat de València está restringido al personal del Servicio de Informática, en caso de visitas externas se realizarán siempre acompañadas por un empleado del Servicio de Informática.
3. En caso de ser necesario el acceso a un CPD o a la infraestructura de comunicaciones por parte de personal no miembro del Servicio de Informática, el responsable de la visita formalizará a través de una Petición de Servicio "Solicitud acceso Áreas Seguras" al Responsable de Seguridad, la solicitud de autorización para este acceso.
4. Cada usuario podrá acceder exclusivamente a los recursos y sistemas de información autoritzados.
5. El acceso a los ordenadores y equipos vinculados al puesto de trabajo ha de realitzarse con el usuario y contraseña asignada.
6. En caso de ausencia del puesto de trabajo en horario de oficina, tiene que procederse al bloqueo del ordenador, que en todo caso tendrá que producirse automáticamente después de 15 minutos de inactividad.
7. En el diseño del puesto de trabajo se asegurará que la pantalla no resulte fácilmente accesible o legible para terceros no autorizados.
8. Tiene que procederse a apagar el ordenador fuera del horario de trabajo, así como evitar el uso del mismo por terceras personas no autorizadas.
9. Se tiene que proteger los identificadores de usuario y contraseña personal y no revelarlos a nadie. Las contraseñas no tienen que ser almacenadas en ficheros legibles, macros, ordenadores sin control de acceso o ninguna otra manera o lugar donde puedan ser accedidas por terceros sin autorización.
10. Nunca se tienen que facilitar los datos de usuario y contraseña a terceras personas, aunque se trate de personal propio de la Universitat.
11. Se procederá al cambio de contraseñas cuando lo solicite el sistema y siempre tendrá que utilizar contraseñas seguras.
12. En caso de incidencia relacionada con la contraseña tendrá que notificarse inmediatamente a través del "Procedimiento de Gestión de Incidencias".
13. El acceso remoto (desde fuera de la red de la Universitat) a los sistemas de información tendrá que realizarse mediante una conexión segura. El usuario aplicará al equipo que utiliza las normas de seguridad contenidas en este apartado para los equipos situados en puestos de la Universitat de València.

**Artículo 5. Uso, mantenimiento y destrucción de dispositivos o soportes que contengan información protegida**

1. No se tiene que dejar abandonados documentos con información protegida en la impresora, fax o dispositivos similares, o desatendida en el puesto de trabajo.
2. La impresión o fotocopia de documentos tiene que limitarse únicamente aquellos que sean estrictamente necesarios y preferiblemente a doble cara. Los documentos rechazados, incluidas las fotocopias erróneas no podrán ser reutilizados cuando contengan datos personales o información confidencial o restringida teniéndose que proceder a su inmediata destrucción.
3. En el caso de reutilización de documentos imprimidos, el usuario comprobará previamente que estos no contienen datos de carácter personal, comunicando la incidencia en caso contrario.
4. Cuando la información sea calificada cómo restringida o confidencial tendrá que guardarse en los lugares designados a este efecto por el Responsable de la Unidad de Gestión correspondiente, al final de la jornada y, en todo caso, al abandonar el puesto cuando su conformación no permita que esté bajo el control de algún usuario.
5. Antes de abandonar salas comunes o permitir que alguna persona ajena entre, se limpiarán adecuadamente las pizarras de las salas de reuniones o despachos, cuidando que no quede ningún tipo de información sensible o que pudiera ser reutilizada.
6. La destrucción de cualquier tipo de apoyo automatizado (CD, DVD, disco duro, memoria USB, etc.) o manual (papel, cintas de vídeo, etc.) se realizará de forma que los datos que contenían no sean recuperables y si procede a través de los procedimientos establecidos.
7. No podrán darse soportes informáticos a ningún tercero sin que previamente se haya realizado un borrado completo del mismo.
8. No es posible modificar o añadir componentes físicos (por ej. un disco duro) de los equipos informáticos y dispositivos de comunicación, excepto autorización expresa del Servicio de Informática. En todo caso, estas operaciones sólo podrán realizarse por el personal de apoyo técnico autorizado.
9. Salvo que el Comité de Gestión y Coordinación de la Seguridad de la Información la Universitat expresamente lo autorice, queda prohibido alojar información confidencial o restringida propia de la Universitat de València en servidores externos en la "nube" no ofrecidos por la propia institución, en particular cuando se trate de datos personales contenidos en los sistemas de información. En caso de necesidad se hará uso de los espacios de disco corporativos (https://disco.uv.es).
10. El usuario es responsable de un uso adecuado de los dispositivos portátiles propiedad de la Universitat de València. Tiene que mantenerlos bajo su custodia y no permitir su uso a ningún tercero. Si se conecta externamente a la Universitat tiene que hacerlo siempre mediante una conexión segura. Si el dispositivo fuese robado o extraviado tiene que notificarse inmediatamente a la Universitat de València, siguiendo el "Procedimiento de Gestión de Incidencias".

**Artículo 6. Salidas y entradas de datos[3]**

1. Se prohíbe expresamente el uso de soportes de información extraíble (dispositivos de almacenamiento USB, memorias flash, etc.) con datos confidenciales o restringidos de la Universitat de València sin autorización del Responsable de la Unidad de Gestión. Se recomienda como procedimiento adecuado a este fin el uso de espacios de disco corporativo. Cualquier

[3] Modificado por el Consejo de Gobierno de 1 de junio de 2021. ACGUV 127/2021.

información que sea almacenada en un apoyo de información extraíble tendrá que ser empleada exclusivamente para motivos de trabajo, y la información tendrá que eliminarse o guardarse en los lugares designados a este efecto.

2. Para toda entrada y/o salida de información no prevista por las aplicaciones corporativas se tiene que solicitar autorización formal al Responsable de la Unidad de Gestión que corresponda.

**Artículo 7. Correo electrónico y red corporativa**

1. El uso del correo electrónico para comunicaciones corporativas estará limitado a las cuentas de la Universitat, y tendrá que cumplir con el propósito del desempeño del trabajador, siendo necesaria la inclusión en los mensajes de correo salientes de la cláusula relativa a la confidencialidad de los datos y la utilización del contacto de correo electrónico exclusivamente para el fin de este correo.
2. El acceso a información corporativa se realizará a través de la red de datos corporativa. También se realizará mediante la Intranet, el acceso de la cual estará limitado a los usuarios que tengan que usarla mediante autenticación por nombre de usuario y contraseña.
3. El envío de datos o información a terceros (cesión de datos), por medio del correo electrónico, transferencia FTP o equivalente tendrá que estar autorizada, por el Responsable de la Unidad de Gestión, para la finalidad exclusiva para la cual sea necesario. Cuando la información sea calificada como confidencial sólo será admisible mediante un procedimiento que impida accesos no autorizados
4. No tienen que abrirse correos electrónicos no solicitados, de remitentes desconocidos o de remitentes conocidos que puedan levantar sospechas. Asimismo, no tienen que ejecutarse archivos no confiables.
5. La consulta de cuentas de correo personal no corporativo en el ordenador del puesto de trabajo se tendrá que realizar exclusivamente a través de sistemas webmail, con la cautela de no abrir correos electrónicos no solicitados, de remitentes desconocidos o de remitentes conocidos que levanten sospechas. Asimismo, no se tienen que ejecutar archivos no confiables.
6. El usuario se hace responsable de los accesos a Internet que puedan comprometer la seguridad del equipo.

**Artículo 8. Recursos informáticos***

1. Todo usuario tiene que mantener actualizada la seguridad de los sistemas operativos, antivirus y cortafuegos (*firewalls*) de su equipo de trabajo mediante actualizaciones automáticas y, en todo caso, de acuerdo con los procedimientos establecidos o con la asistencia del Centro de Atención al Usuario de la Universitat (CAU). Los sistemas operativos y aplicaciones han de disponer de soporte y mantenimiento por parte del fabricante, no permitiéndose el uso de sistemas operativos ni aplicaciones que hayan sobrepasado su ciclo de vida útil hasta un máximo de 18 meses.
2. Los equipos de la Universitat de València conectados en la red cableada tienen que tener instalado el *software* antivirus proporcionado por la institución, el cual se encuentra accesible dentro del catálogo de programas (https://software.uv.es).
3. El usuario únicamente podrá instalar los programas para los cuales la Universitat de València tenga licencia de uso. En particular, los habilitados en el catálogo de programas (https://software.uv.es) de la Universitat de València. No es posible instalar programas no autorizados o sin licencia, ni ejecutar o guardar archivos no confiables.

* Modificado por el Consejo de Gobierno de 3 de octubre de 2023. ACGUV 245/2023.

4. En caso de incumplimiento de las obligaciones establecidas en cualquier de los apartados anteriores se podrá proceder, como una medida de prevención de riesgos de seguridad en la información, a la desconexión de los dispositivos afectados de la red de la Universitat de València. En todo caso, se prestará suporte a los usuarios por tal de resolver la incidencia y actualizar sus equipos.

**Artículo 9. Incidencias de seguridad**

El usuario tiene que comunicar cualquier Incidencia de Seguridad de la cual tenga conocimiento (posible virus, comportamientos sospechosos...) siguiendo el "Procedimiento de Gestión de Incidencias".

**Artículo 10. Información institucional y datos personales**

1. La información contenida en los Sistemas de Información de la Universitat de València es de su exclusiva propiedad, por lo cual los usuarios tienen que abstenerse de comunicar, divulgar, distribuir o poner en conocimiento o al alcance de terceros (externos o internos no autorizados) esta información, excepto autorización expresa del Comité de Gestión y Coordinación de la Seguridad de la Información.
2. Todo usuario (de la Universitat de València o de terceras organizaciones) que, en virtud de su actividad profesional, pudiera tener acceso a datos de carácter personal, está obligado a guardar secreto sobre estas y a aplicar las medidas previstas en el documento de seguridad. Este deber se mantendrá de manera indefinida, incluso más allá de la relación laboral o profesional con la Universitat de València.

**Artículo 11. Publicación en web**

1. La publicación de contenidos en la web de la Universitat de València se limitará a los documentos o informaciones categorizados como "No clasificados".
2. La información publicada tiene que garantizar los principios de autenticidad e integridad.
3. Los gestores y editores de páginas web asegurarán la disponibilidad de la información durante el periodo previsto de vigencia de la misma procediendo a su retirada cuando se produzca el vencimiento.

**Artículo 12. Gestión del reglamento.**

La gestión de este Reglamento corresponde al Comité de Gestión y Coordinación de la Seguridad de la Información, que es competente para:

a) Interpretar las dudas que puedan surgir en su aplicación.

b) Verificar su efectividad.

c) Proponer su revisión.

**Artículo 13. Revisión de las normas de seguridad**

1. Anualmente, o de manera extraordinaria cuando existen circunstancias que así lo aconsejan, el Comité de Gestión y Coordinación de la Seguridad de la Información revisará el presente Reglamento.
2. La revisión se orientará tanto a la identificación de oportunidades de mejora en la gestión de la seguridad de la información, como la adaptación a los cambios en el marco legal, infraestructura tecnológica y cualquier otro aspecto relevante.

**Artículo 14. Divulgación**

1. El Responsable de Seguridad es la persona encargada de la difusión de la versión aprobada de este documento.
2. Sin perjuicio de la competencia del Responsable de Seguridad, la Universitat de València mediante la acción de los servicios competentes adoptará las medidas oportunas para difundir esta normativa, y para formar y concienciar los usuarios.

**Artículo 15. Responsabilidad**

Todos los usuarios de los sistemas de información bajo el alcance del Esquema Nacional de Seguridad en la Universitat de València están obligados a cumplir la presente normativa. Su incumplimiento genera responsabilidad que se sustanciará conforme al procedimiento establecido a este efecto en cada caso.

## Disposición adicional primera

1. Las previsiones de esta normativa no son incompatibles con aquellas obligaciones derivadas del puesto de trabajo y otras normativas.
2. Se faculta el responsable de seguridad de la Universitat de València por:
    a) Notificar, si procede, a los usuarios instrucciones concretas sobre las condiciones de cumplimiento de las normas de seguridad.
    b) Establecer normas de seguridad adicionales, previa comunicación al Comité de Gestión y Coordinación de la Seguridad de la Información cuando lo justifican motivos de urgencia o necesidad, o adoptar aquellas decisiones que resultan indispensables para garantizar el objetivo de la seguridad. En este caso, regirán de manera provisional todo e incorporándose a esta normativa cuando sea revisada.
    c) Definir los procedimientos de gestión de la seguridad que resulten necesarios para hacer efectivas las disposiciones de esta normativa. Estos procedimientos se notificarán al Comité de Gestión y Coordinación de la Seguridad de la Información.

## Disposición adicional segunda[4]

En todo aquello no previsto por esta normativa se aplicará supletoriamente lo que disponen las normas reguladoras del Esquema Nacional de Seguridad; el Reglamento (UE) 2016/679 del

[4] Modificado por el Consejo de Gobierno de 1 de junio de 2021. ACGUV 127/2021.

Parlamento y del Consejo, relativo a la protección de las personas físicas en cuanto al tratamiento de datos personales y a la libre circulación de estos datos; la Ley Orgánica 3/2018, de protección de datos de carácter personal y garantía de derechos digitales, y la normativa que la despliega.

## Disposición Final. Entrada en vigor

Este reglamento se difundirá a todo el personal de la Universitat mediante su publicación y entrará en vigor transcurrido un mes natural desde la fecha de aprobación por el Consejo de Gobierno de la Universidad.

**Aprobado por el Consejo de Gobierno de 22 de diciembre de 2014. ACGUV 227/2014.**

**Modificado por el Consejo de Gobierno de 1 de junio de 2021. ACGUV 127/2021.**

**Modificado por el Consejo de Gobierno de 3 de octubre de 2023. ACGUV 245/2023.**