# 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

Conforme al que es disposa en el Reial decret 3/2010, de 8 de gener, pel qual es regula l'Esquema Nacional de Seguretat en l'àmbit de l'Administració Electrònica (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: PAS, 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 agilitar 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 açò, 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 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.**

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 dels següents sistemes d'informació, als serveis que integren i a qualsevol suport que la continga:

a) Gestió acadèmica:

- Serveis de gestió acadèmica
- Serveis de préstecs bibliotecaris

b) Gestió d'automatrícula (subsistema de gestió acadèmica):

- Servei d'automatrícula
- Servei d'admissió a la Universitat

c) Gestió d'actes (subsistema de gestió acadèmica):

- Servei d'actes d'avaluació
- Gestió de títols (subsistema de gestió acadèmica):
- Serveis de sol·licitud i emissió de títols

d) Seu electrònica:

- Serveis per a PAS-PDI
- Serveis vinculats a la investigació
- Serveis per a estudiants
- Serveis a externs

e) Gestió econòmica:

- Serveis de contractació administrativa

f) Sistema de docència virtual:

- Aula Virtual

g) Portal web de la Universitat:

- Serveis d'informació administrativa

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:

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.

## 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 D'informàtica 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 (http://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**

1. Es prohibeix expressament l'eixida 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.

**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).

2. 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 (http://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.

**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 relevant.

**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

En tot allò no previst per aquesta normativa s'aplicarà supletòriament el que disposen les normes reguladores de l'esquema nacional de seguretat i el Títol VIII del Reial decret 1720/2007, de 21 de desembre, pel qual s'aprova el Reglament de desplegament de la Llei orgànica 15/1999, de 13 de desembre, de protecció de dades de caràcter personal.

## 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.**