



VNIVERSITAT  
DE VALÈNCIA

# **Reglament de seguretat de la informació en la utilització de mitjans electrònics de la Universitat de València (ACGUV 245/2023)**

Comentaris a les normes establides en el Reglament

1. Introducció al Reglament
2. Normes de seguretat
  - Controls d'accés físic i lògic.
  - Ús, manteniment i destrucció de dispositius o suports que continguen informació protegida.
  - Eixides i entrades de dades.
  - Correu electrònic i xarxa corporativa.
  - Recursos informàtics.
  - Incidències de seguretat.
  - Informació institucional i dades personals.
  - Publicació en web.

# 1. Introducció al Reglament de seguretat de la informació en la utilització de mitjans electrònics de la Universitat de València

L' **Esquema Nacional de Seguretat** (Reial Decret 311/2022, de 3 de maig) estableix que les Administracions públiques disposaran d'un reglament de seguretat de la informació.

La Universitat de València es va adaptar en 2014 als requisits de l'Esquema Nacional de Seguretat (ENS) i va aprovar el seu reglament que va ser actualitzat en 2021 i 2023.

- **Reglament de seguretat de la informació en la utilització de mitjans electrònics** (ACGUV 245/2023).

- **Garantir** als usuaris i usuàries **l'accés a la informació** amb la quantitat i qualitat que es requereix per a l'acompliment de les seues funcions.
- **Evitar pèrdues d'informació** i accessos no autoritzats a aquesta.



El Reglament és un instrument **al servei de la Universitat i de totes les persones usuàries** capaç de:

- proporcionar **confiança** en els sistemes;
- preservar **l'exercici de les funcions** i responsabilitats pròpies de cada usuari i usuària;
- garantir la **qualitat i veracitat** de la informació objecte de tractament.

- **Personal públic** de la Universitat de València.
- **Membres de comissions** o òrgans relacionats amb la Universitat de València.
- **Prestadors de serveis**, entitats col·laboradores o qualsevol un altre amb algun tipus de vinculació amb la Universitat de València.



- Es defineix un conjunt de **39 normes sobre 8 aspectes** (situacions) diferents.
- Les normes pretenen establir unes **bones pràctiques** en el nostre treball diari, que es poden estendre a altres sistemes d'informació encara que no siguin els inclosos en l'Esquema Nacional de Seguretat (ENS).





# **Reglament de seguretat de la informació en la utilització de mitjans electrònics de la Universitat de València (ACGUV 245/2023)**

**[DESCARREGAR](#)**

## 2. Normes de seguretat

## **Aspectes** que abasten les normes de seguretat.

- Controls d'accés físic i lògic.
- Ús, manteniment i destrucció de dispositius o suports que continguen informació protegida.
- Eixides i entrades de dades.
- Correu electrònic i xarxa corporativa.
- Recursos informàtics.
- Incidències de seguretat.
- Informació institucional i dades personals.
- Publicació en web.

## Resum

**No s'ha de permetre l'accés de personal extern** (no autoritzat) a les zones que continguen infraestructures TIC o documentació amb informació protegida.

## Comentari

Es tracta d'evitar la manipulació dels equips i descàrregues d'informació mitjançant:

- instal·lació de *software* maliciós en els sistemes;
- manipulació dels sistemes de comunicació;
- ús de dispositius d'emmagatzematge portàtil;
- fotografies de documents.

## Resum

Es requereix **identificació personal** en l'accés als sistemes informàtics de la UV.

### Comentari

La identificació proporciona confiança al personal de la UV i a la ciutadania.

- El personal solament és responsable de la seua activitat.
- El ciutadà i ciutadana ha de saber qui i quan va accedir a la seua informació.

## Resum

Cal prendre mesures en el treball quotidià per a **dificultar l'accés a la informació** a terceres persones.

## Comentari

Es tracta d'evitar que terceres persones puguen:

- accedir al nostre ordinador de treball fent ús del nostre usuari personal;
- visualitzar o registrar informació sobre altres usuaris i usuàries (ciutadans i ciutadanes) mostrada en l'ordinador de treball.

## Resum

S'han de **protegir les credencials d'identitat** (usuari i contrasenya) que permeten accedir als recursos TIC de la UV.

## Comentari

Les credencials personals ens identifiquen en els sistemes i, per tant, ens fan responsables de les accions realitzades amb aquestes.

- És molt important protegir-les, especialment la contrasenya, i no cedir-les a terceres persones.
- La protecció de la contrasenya és responsabilitat de la usuària i usuari. Si sospites que algú poguera conèixer-la, canvia-la al més prompte possible.

## Sobre les contrasenyes en la UV

- Les contrasenyes personals s'emmagatzemen encriptades en els sistemes informàtics de la UV.
- Ningú en la Universitat coneix la nostra contrasenya.
- El personal tècnic de la Universitat no demanarà mai que li proporcionem la nostra contrasenya personal.

### Precaució

- Si reps algun missatge (correu electrònic) demanant la teua contrasenya o que accedisques a una pàgina web externa per a introduir-la, és un engany .
- No respongues mai a aquests avisos i informa al Servei d'Informàtica.



## Resum

Els accessos a les aplicacions des d'ordinadors externs a la UV s'han de fer mitjançant **mecanismes segurs**.

- De la seguretat en la comunicació s'encarrega el Servei d'Informàtica de la Universitat de València, habilitant mecanismes de connexió que assegurin l'encriptació en la transmissió de les dades (VPN, https).

## Comentari

Si emmagatzemem informació de la Universitat en ordinadors externs a la UV, per exemple d'altres institucions, hem d'assegurar-nos que aquests **ordinadors complisquen també les mesures de seguretat** establides en el Reglament de seguretat.

## Resum

S'ha d'**evitar que l'emmagatzematge de documents en paper amb dades protegides** siga accessible a persones alienes a la UV.

## Comentari

- Destruir els documents impresos una vegada que han deixat de ser útils.
- Imprimir o fotocopiar només aquells documents estrictament necessaris i a doble cara. No reutilitzar fotocòpies errònies quan continguen dades personals.
- Si cal emmagatzemar documents impresos, cal fer-ho en un lloc no accessible per tercers.

## Resum

Mesures que s'han de prendre per a la **destrucció d'informació generada** en el nostre treball diari que no estiga en paper.

## Comentari

- La informació o documents deixats a les sales de reunions compartides poden contenir dades personals. Per això, s'han d'esborrar o retirar en acabar la reunió.
- Els suports informàtics (DVD, memòria USB, etc.) han de ser esborrats o destruïts adequadament.

## Resum

Mesures que s'han de prendre per a **evitar l'emmagatzematge d'informació en mitjans no segurs.**

### Comentari

- Afegir components d'emmagatzematge o de comunicació en els ordinadors del lloc de treball introdueix inseguretats sobre l'accés a les dades emmagatzemades o transmesos a través d'ells.
- Els serveis d'emmagatzematge en el núvol externs a la UV són còmodes però insegurs, ja que en general els proveïdors tenen lliure accés a la informació que contenen.
- La UV disposa de serveis d'emmagatzematge similars que permeten l'emmagatzematge segur de la informació ([disco.uv.es](https://disco.uv.es)).

## Resum

Es requereix **autorització per a l'entrada i eixida d'informació** de la qual és dipositària la UV.

### Comentari

- Es prohibeix expressament l'ús de suports d'informació extraïbles (dispositius d'emmagatzematge USB, memòries flaix, etc.) amb dades confidencials o restringides de la Universitat de València sense autorització de la persona responsable de la Unitat de Gestió.
- Per a la portabilitat d'informació, el mitjà més segur és sempre el sistema d'emmagatzematge virtual de la UV, que manté la informació en servidors de la UV.

## Resum

Les comunicacions efectuades per usuaris i usuàries de la UV amb motiu del seu treball s'han de fer **mitjançant els comptes de correu oficials** i la xarxa de comunicacions de la UV.

## Comentari

- Incloure en els missatges de correu sortints 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.
- Correu UV = Confiança pel ciutadà i ciutadana i protecció de la informació.

## Resum

Es requereix **autorització per a l'enviament** per mitjans telemàtics a terceres persones d'informació de la qual és dipositària la UV.

## Comentari

- Haurà d'estar autoritzada per la persona 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 l'enviament mitjançant un procediment que impedisca accessos no autoritzats.

## Resum

Evitar comportaments en l'ús del correu electrònic i d'Internet que pogueren **comprometre la seguretat de la informació**.

## Comentari

Determinats correus electrònics o pàgines web poden descarregar *software* maliciós en els nostres ordinadors i generar:

- descàrregues d'informació;
- mal funcionament del nostre sistema;
- atacs a altres ordinadors des del nostre.



## Resum

Assegurar la **confiança en l'ordinador del lloc de treball** amb què es processa la informació de la Universitat.

### Comentari

- Mantenir actualitzada la seguretat dels sistemes operatius, antivirus i tallafocs (*firewalls*) del equip de treball mitjançant actualitzacions automàtiques o amb l'assistència del Centre d'Atenció a l'Usuari del Servei d'Informàtica.
- La persona usuària únicament podrà instal·lar els programes per als quals la Universitat de València tinga llicència d'ús en el catàleg de *software*  
<https://software.uv.es>.

## Resum

**Notificar al Servei d'Informàtica** qualsevol possible incidència sobre la seguretat de la informació de la qual es poguera tenir coneixement.

## Comentari

La informació permetrà resoldre el problema i controlar els riscos.

## Resum

La Universitat de València és responsable de la informació dipositada pels ciutadans i ciutadanes. Tota persona que tinga accés a aquesta en virtut del seu treball té el deure de **guardar-ne confidencialitat.**

## Comentari

- Els usuaris i usuàries 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.
- El deure de guardar el secret es mantindrà de manera indefinida, fins i tot més enllà de la relació laboral o professional amb la Universitat de València.

## Resum

En les pàgines web de la UV solament s'ha de **publicar informació** que siga:

- de caràcter públic (“No classificada”);
- autèntica i íntegra;
- vigent.

## Comentari

Cal tenir especial precaució amb les dades personals que es publiquen en les pàgines web.

No s'ha de causar confusió a la ciutadania i cal cuidar la fiabilitat i la vigència de la informació publicada. És molt important retirar la informació quan haja perdut vigència, especialment quan incloga dades personals amb dret a l'oblit.

Si tens algun dubte sobre seguretat o tractament de dades, envia un correu electrònic a [enseg@uv.es](mailto:enseg@uv.es) o [lopd@uv.es](mailto:lopd@uv.es), respectivament.



VNIVERSITAT  
DE VALÈNCIA