



Registre d'incidències

L'usuari o usuària dels sistemes d'informació de la UV que tinga **coneixement d'una incidència** és responsable de la seua comunicació mitjançant la creació d'un tiquet en l'eina de gestió <https://solicitudes.uv.es>.

R.S. art.9

El coneixement i no notificació d'una incidència es considera com una **falta contra la seguretat**.

1

Política de contrasenyes

Les contrasenyes dels comptes d'usuari que proporciona la UV són: **personals i intransferibles** i d'ús exclusiu del seu titular. Cada persona és responsable de la confidencialitat de la seua contrasenya.

U.R.T. art 10.1,10.2,11.R.S.art 4.9,4.10

Cal **canviar la contrasenya** amb la freqüència establida per la política de seguretat de la UV. **No facilitar mai dades** d'usuari i contrasenya a terceres persones.

2

Control de llocs

Accedir a ordinadors i equips vinculats al lloc de treball mitjançant **usuari i contrasenya**. En cas d'absència del lloc de treball en horari d'oficina, **bloquejar l'ordinador** (o que s'active automàticament el bloqueig, passat un màxim de 15 minuts).

R.S. art. 4.5, 4.6 y 4.7

Assegurar que la **pantalla no resulte fàcilment accessible** o llegible per tercers no autoritzats.

3

Taules netes i impressores

No deixar abandonats **documents amb informació protegida** en la impressora, fax o dispositius similars, o desatsos en el lloc de treball. **Limitar la impressió** o fotocòpia de documents a aquells que siguen estrictament necessaris i a doble cara.

R.S. art 5.1, 5.2 y 5.5

Quan s'abandoni el lloc de treball (descansos, pausa per a menjar o fi de jornada laboral), deixar-lo **lliure de documentació**. Netejar adequadament les pissarres de les sales de reunions o despatxos abans d'eixir o permetre que entren persones alienes.

4

Claus, portes i armaris

Mantenir correctament **custodiades les claus d'accés** als despatxos, calaixeres, armaris, així com qualsevol altre element que continga fitxers no automatitzats amb dades de caràcter personal.

R.S. art 4

Tancar amb clau tots els elements d'emmagatzematge, quan la persona s'absente temporalment de la seua ubicació de treball, a fi d'evitar accessos no autoritzats.

5

Atenció al públic

El personal que atenga directament el públic no podrà tenir **cap tipus d'informació sobre un altre al seu abast**.

Obligació

Quan acabem d'atendre una persona, abans de començar amb la següent, **no tenir documentació** que no guarde relació amb la nova a assistir.

6

Emmagatzematge d'informació

Prohibit usar suports d'informació extraïbles (dispositius d'emmagatzematge USB, memòries flaix, etc.) amb dades confidencials o restringides de la UV, sense l'autorització de la persona responsable de la unitat de gestió.
Utilitzar espais de **disc corporatiu** (disco.uv.es o nuvol.uv.es).

Fitxers no automatitzats

Emmagatzemar fitxers no automatitzats en **llocs que permeten el tancament amb clau** o mecanismes que impedisquen la seua obertura.

7

Creació de fitxers, classificació i etiquetatge de la informació

Evitar l'emmagatzematge de còpia de les dades personals dels fitxers en arxius temporals.
Esborrar els fitxers temporals una vegada han deixat de ser necessaris per als fins que van motivar la seua creació.
Classificar i etiquetar la informació.

Fitxers amb dades personals

Si transcorregut un mes, es detecta la necessitat de continuar utilitzant la informació emmagatzemada en el fitxer, cal **comunicar-ho a la persona responsable de seguretat**.

8

Destrucció de dispositius

Destruir qualsevol tipus de suport automatitzat (CD, DVD, disc dur, memòria USB, etc.) o manual (paper, cintes de vídeo, etc.), a través dels procediments establits, de manera que les **dades que contenen no siguen recuperables**.

R.S. art 5.6 y 5.7

No es poden reutilitzar suports informàtics per part de tercers sense que s'haja realitzat un **esborrament complet** de la informació.

9

Accés remot

L'accés remot (des de fora de la xarxa de la UV) als sistemes d'informació s'haurà de realitzar mitjançant una **connexió segura**.
L'usuari o usuària aplicarà al seu equip les normes de seguretat contingudes en el *Reglament de seguretat de la informació en la utilització de mitjans electrònics de la Universitat de València*.

R.S. art 4.13

Quan no es puga garantir una connexió segura (HTTPS o similar) per a accedir als sistemes d'informació, la comunicació s'haurà de realitzar a través de la **connexió VPN** de la UV.

10

Deure de confidencialitat

La informació continguda en els sistemes d'informació de la UV és de la seua exclusiva propietat. Cal 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.

R.S. art 10.1 y 10.2

Tota persona (de la UV o de tercers organitzacions) que, en virtut de la seua activitat professional, tinga accés a dades de caràcter personal, està obligada a **guardar secret** sobre aquestes i 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 UV.

11

Responsabilitat

Tota la comunitat usuària dels sistemes d'informació sota l'abast de l'Esquema Nacional de Seguretat a la UV està obligada a **complir el Reglament de seguretat de la informació en la utilització de mitjans electrònics de la Universitat de València**.

R.S. art 15

El seu incompliment generarà responsabilitat que se substanciarà conforme al procediment establert per a cada cas.

12