VNIVERSITAT DE VALÈNCIA

-Dodecálogo-
Obligaciones de seguridad

1 Comunicación de incidencias

R.S. art.9

El usuario o usuaria de los sistemas de información de la UV que tenga **conocimiento de una incidencia** es responsable de su comunicación mediante la creación de un tique en la herramienta de gestión ***https://solicitudes.uv.es***.

El conocimiento y la no notificación de una incidencia se considerará como una **falta contra la seguridad**.

2 Política de contraseñas

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

Las contraseñas de las cuentas de usuario que proporciona la UV son: **personales e intransferibles** y de uso exclusivo por su titular. Cada persona es responsable de la confidencialidad de su contraseña.

Cambiar la contraseña con la frecuencia establecida por la política de seguridad de la UV.
No facilitar nunca los datos de usuario y contraseña a terceras personas, aunque se trate de personal propio de la Universitat.

3 Control de puestos

R.S. art. 4.5, 4.6 y 4.7

El **acceso a los ordenadores** y equipos vinculados al puesto de trabajo debe realizarse con **usuario y contraseña**.
En caso de ausencia del lugar de trabajo en horario de oficina, **bloquear el ordenador** (o que se active automáticamente el bloqueo después de un máximo de 15 minutos).

Asegurar que la **pantalla no resulte fácilmente accesible** o legible por terceros no autorizados.

4 Mesas limpias e impresoras

R.S. art 5.1, 5.2 y 5.5

No dejar abandonados **documentos con información protegida** en la impresora, fax o dispositivos similares, o desatendidos en el lugar de trabajo.
Limitar la impresión o fotocopia de documentos a aquellos estrictamente necesarios y a doble cara.

Al abandonar el puesto de trabajo (descansos, pausa para comer o fin de jornada laboral), dejarlo **libre de documentación**.
Limpiar adecuadamente las pizarras de las salas de reuniones o despachos antes de salir o permitir entrar a personas ajenas.

5 Llaves, puertas y armarios

R.S. art 4

Mantener correctamente **custodiadas las llaves de acceso** a los despachos, cajoneras, armarios, así como cualquier elemento que contenga ficheros no automatizados con datos de carácter personal.

Cerrar con llave todos los elementos de almacenamiento, cuando la persona se ausente temporalmente de su ubicación de trabajo, para evitar accesos no autorizados.

6 Atención al público

Obligación

El personal que atienda directamente al público no podrá tener ningún tipo de **información acerca de otro a su alcance**.

Cuando se termine de atender a una persona, antes de comenzar con la siguiente, **no tener documentación** que no guarde relación con la nueva a asistir.

Almacenamiento de información

Prohibido usar soportes de información extraíbles (dispositivos de almacenamiento USB, memorias *flash*, etc.) con datos confidenciales o restringidos de la UV, sin la autorización de la persona responsable de la unidad de gestión.
Utilizar espacios de **disco corporativo** (disco.uv.es o nuvol.uv.es).

7

R.S. art 6.1

Almacenar ficheros no automatizados **en lugares que permitan ser cerrados con llave** o con mecanismos que impidan su apertura.

Creación de ficheros, clasificación y etiquetado de la información

Evitar el **almacenamiento de copia de los datos personales** de ficheros en archivos temporales.
Borrar los ficheros temporales cuando dejen de ser necesarios para los fines que motivaron su creación.
Clasificar y etiquetar la información.

8

Ficheros con datos personales

Si transcurrido un mes, se detecta la necesidad de continuar utilizando la información almacenada en el fichero, debe ser **comunicarlo a la persona responsable de seguridad**.

Destrucción de dispositivos

Destruir cualquier tipo de soporte automatizado (CD, DVD, disco duro, memoria USB, etc.) o manual (papel, cintas de vídeo, etc.), a través de los procedimientos establecidos, de forma que los datos que contenían **no sean recuperables.**

9

R.S. art 5.6 y 5.7

No pueden reutilizarse soportes informáticos por parte de terceros sin que se haya realizado un **borrado completo** de la información.

Acceso remoto

El acceso remoto (desde fuera de la red de la Universitat) a los sistemas de información debe realizarse mediante una **conexión segura**.
El usuario o usuaria aplicará a su equipo las normas de seguridad contenidas en el *Reglamento de seguridad de la información en la utilización de medios electrónicos de la Universitat de València*.

10

R.S. art 4.13

Cuando no se pueda garantizar una conexión segura (HTTPS o similar) para acceder a los sistemas de información, la comunicación debe realizarse a través de la **conexión VPN** de la UV.

Deber de confidencialidad

La información contenida en los sistemas de información de la UV es de su exclusiva propiedad.
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.

11

R.S. art 10.1 y 10.2

Toda persona (de la UV o de terceras organizaciones) que, en virtud de su actividad profesional, tenga acceso a datos de carácter personal, está obligada a **guardar secreto** sobre estos y a aplicar las medidas previstas en el documento de seguridad.
Este deber se mantendrá **de forma indefinida**, incluso más allá de la relación laboral o profesional con la UV.

Responsabilidad

Toda la comunidad usuaria de los sistemas de información, bajo el alcance del Esquema Nacional de Seguridad en la UV, está obligada a **cumplir el *Reglamento de seguridad*** *de la información en la utilización de medios electrónicos de la Universitat de València*.

12

R.S. art 15

Su incumplimiento generará responsabilidad que se substanciará conforme al procedimiento establecido para cada caso.

UV-> Universitat de València.
R.S.-> Reglamento de seguridad de la información en la utilización de medios electrónicos de la Universitat de València.
U.R.T.->Reglamento de uso de los recursos relacionados con las tecnologías de la información y las comunicaciones de la Universitat de València.