RECOMENDACIONES DE SEGURIDAD

1

UTILIZAR SIEMPRE ANTIVIRUS

- **Instalar el antivirus corporativo.** Funciona en comunicación con un servidor que proporciona la configuración adecuada, actualiza los ficheros de patrones de virus y puede ejecutar acciones de emergencia para proteger en caso de epidemia.
- **Mantener actualizado el antivirus permanentemente** para la detección y eliminación de virus.
- **La instalación del antivirus corporativo se hace a través de red.** El requisito fundamental es no tener otro antivirus instalado.

2

MANTENER EL EQUIPO ACTUALIZADO

- Mantener **actualizadas aplicaciones y sistema operativo.**
- Los **sistemas operativos y aplicaciones obsoletos** no disponen de soporte. Consecuencias:
  - en caso de incidencia, no podrá ser solucionada;
  - no existen actualizaciones para mejorar errores y seguridad;
  - presencia de vulnerabilidades que permiten el acceso de agentes no autorizados y dañinos a la información de nuestro equipo.

3

VERIFICAR CADA CORREO ELECTRÓNICO ANTES DE ABRIRLO

- **No abrir ningún enlace** ni descargar ningún fichero adjunto procedente de un correo electrónico que presente cualquier indicio o patrón fuera de lo habitual.
- **Verificar el remitente.** No confiar en el nombre del remitente, comprobar que el dominio del correo es de confianza.

VNIVERSITAT DE VALÈNCIA

RECOMENDACIONES DE SEGURIDAD

4

NO DARSE DE ALTA CON EL USUARIO DE LA UV EN TERCERAS ENTIDADES

- **No darse de alta en servicios ofrecidos por terceras empresas u organismos** (ejemplo: plataformas de *streaming* tipo Netflix o HBO, *marketplaces* como Amazon…) **con el usuario de la Universitat de València.**
- Si por algún motivo, fuera necesario e inevitable darse de alta con el usuario de la UV en alguna entidad externa, **no utilizar la misma contraseña** que en los servicios de la Universitat.

5

NO DESCARGAR PROGRAMAS EN SITIOS NO SEGUROS DE LA RED

La instalación de programas no seguros puede afectar al rendimiento y comprometer la seguridad de dispositivos y equipos.

- Descargar únicamente **programas disponibles en** https://software.uv.es. Emplear *software* legal y vigente ofrece garantía y soporte.
- Instalar y mantener **parches y actualizaciones de seguridad**.

6

REALIZAR COPIAS DE SEGURIDAD PERIÓDICAMENTE

- Si hay información que deseas mantener, la Universitat de València pone a nuestra disposición dos servicios que realizan copias de seguridad periódicas: disco.uv.es o nuvol.uv.es. Garantizan la seguridad con un **sistema de copias centralizadas.**
- Si tienes alguna incidencia o duda con estos servicios, puedes contactar con el **Centro de Atención al Usuario** (CAU).

VNIVERSITAT DE VALÈNCIA

RECOMENDACIONES DE SEGURIDAD

7

UTILIZAR USUARIO SIN PRIVILEGIOS PARA TAREAS GENÉRICAS

Trabajar en el sistema como **usuario sin privilegios**. Evitar trabajar como "Administrador". Razones:

- **l**a mayoría de las **tareas comunes** no necesitan un usuario con privilegios;
- si algún **virus** u otro programa malicioso quiere entrar en nuestro equipo, se verá muy **limitado** en su capacidad para causar daño.

8

LIMPIEZA DE DOCUMENTOS

- **Inspeccionar y borrar los metadatos** y otros datos ocultos existentes en los documentos.
- Los metadatos son **incorporados de forma automática** por los programas de generación y tratamiento de documentos, o por los propios usuarios o usuarias de la organización.

9

DOBLE FACTOR DE AUTENTICACIÓN

Hablamos de **doble factor en la autenticación** (2FA) cuando le decimos a nuestros sistemas que:

- usaremos nuestro **usuario y contraseña** (o un certificado digital);
- y un segundo dato que permita **comprobar nuestra identidad**.

Objetivo: evitar los casos en los que alguna persona malintencionada quiera hacer un **uso fraudulento de tu identidad de usuario de la UV**.

- Actualmente, algunos servicios o aplicaciones de la Universitat de València requieren la doble autenticación para acceder.

VNIVERSITAT DE VALÈNCIA