



Buenas prácticas en Seguridad de la Información

Estimado/a usuario/a: este **documento forma parte del actual plan de concienciación en seguridad** que la Universidad Complutense de Madrid ha puesto en marcha. Por esto, y como miembro de nuestra comunidad universitaria, te pedimos que dediques unos minutos a leer **este resumen de buenas prácticas en seguridad e información** sobre diferentes cuestiones.

En la web <https://www.ucm.es/seguridad-y-proteccion> puedes ver la política de seguridad de la Universidad, la normativa sobre protección de datos, consejos, noticias y enlaces interesantes sobre seguridad y protección de la información.

También ponemos a tu disposición unas recomendaciones para mantener la seguridad de tu información: <https://www.ucm.es/seguridad-y-proteccion/recomendaciones>.

Seguridad básica

Utiliza contraseñas robustas y cámbialas al menos un par de veces al año o cuando sospeches que tu sistema ha podido ser comprometido. No reveles nunca tus contraseñas a nadie. (Recuerda que **tu identificador es único y personal**). Usa un gestor de contraseñas.

Plantéate utilizar el **segundo factor de autenticación** que tienes a tu disposición en el gestor de identidad de la UCM.

Si detectas cualquier incidente de seguridad **ponte inmediatamente en contacto con los Servicios Informáticos** (SSII) abriendo una incidencia a la mayor brevedad, para mitigar los posibles efectos.

Realiza periódicamente copias de seguridad de tu información, es la única garantía ante las potenciales amenazas (como por ejemplo el famoso **ransomware**).

No dejes documentos con información delicada a la vista.

Recoge los documentos de impresoras compartidas rápidamente y **evita imprimir en impresoras que no tengas controladas visualmente.**



Los datos de carácter personal



Si manejas **datos de carácter personal**, hazlo correctamente. Contacta con la **Oficina del Delegado de Protección de Datos** o con la **Unidad de Seguridad y Protección de la Información** de la universidad si necesitas más información sobre cómo hacerlo.

La Agencia Española de Protección de Datos define los datos de carácter personal como “cualquier información numérica, alfabética, gráfica, fotográfica, acústica o de cualquier otro tipo concerniente a personas físicas identificadas o identificables”.



Sobre las aplicaciones

La instalación de software puede afectar al rendimiento y la seguridad de su equipo. Hazlo sabiendo lo que haces.

El uso legal del software ofrece garantía y soporte, sin contar las implicaciones legales de utilizar software de forma no legítima. **Consulta el [software que la Universidad pone a tu disposición](#).**

Instala las actualizaciones de seguridad en el sistema operativo y en las aplicaciones, con especial atención en aquellas de carácter crítico.

No ejecutes nunca programas de origen dudoso o desconocido y, en la medida de lo posible, no uses las macros de los paquetes ofimáticos de manera automática.

Instala el **[software antivirus corporativo](#)** (pide ayuda a los SSII si la necesitas).

Trabaja habitualmente en el sistema **como usuario sin privilegios**, no como Administrador.



El correo electrónico

No pulses en ningún enlace ni descargues ningún archivo adjunto de un mensaje de correo electrónico que presente cualquier indicio o patrón fuera de lo habitual.

No confíes únicamente en el nombre del remitente. Comprueba que el propio dominio del correo recibido es de confianza. **Si un correo procedente de un contacto conocido solicita información inusual, contacta con ese contacto por teléfono u otra vía de comunicación para corroborar la legitimidad del mismo.**

Antes de abrir cualquier archivo descargado desde el correo, comprueba la extensión y no te fíes del icono asociado al mismo.

No pulses en ningún enlace que solicite datos personales o bancarios.

Evita pulsar directamente en cualquier enlace desde el propio cliente de correo. Si el enlace es desconocido, es recomendable buscar información del mismo en motores de búsqueda como Google o Bing.

Cifra los mensajes de correo que contengan información sensible. Es la mejor opción.