GUÍA DE BUENAS PRÁCTICAS PARA UN TRATAMIENTO ADECUADO DE LOS DATOS DE CARÁCTER PERSONAL Y SEGURIDAD DE LA INFORMACIÓN

Si en el desempeño de las tareas y funciones de tu puesto de trabajo utilizas recursos o equipos informáticos y tienes acceso o tratas datos de carácter personal debes saber que estás sujeto a la normativa de protección de datos para salvaguardar los derechos de los interesados.

- Reglamento (UE) 2016/679 General de Protección de Datos (RGPD).
- Ley Orgánica 3/2018, de 5 de diciembre, de protección de datos personales y garantía de los derechos digitales (LOPDGDD)

Todos los usuarios de la Universidad deben ser conscientes de la necesidad de garantizar la seguridad e integridad de los sistemas de información que utilicen y la confidencialidad de los datos personales que traten. Por ello, tienen la obligación de conocer y cumplir todas las medidas de seguridad conforme a las instrucciones y procedimientos establecidos por la Universidad.

- Real Decreto 311/2022, de 3 de mayo, Esquema Nacional de Seguridad (ENS)
- Acuerdo 18/CG de 17-06-22 por el que se aprueba la Normativa sobre el equipamiento informático de uso individual gestionado por la Unidad de Tecnologías de la Información
- Acuerdo 5/CG de 14-07-16 por el que se aprueba la Normativa general de uso de recursos TIC y sistemas de información de la Universidad Autónoma de Madrid

A continuación, te ofrecemos una serie de sencillos consejos y recomendaciones que te permitirán actuar correctamente para cumplir la normativa en materia de protección de datos de carácter personal y seguridad de la información:

Obligaciones generales

1. Asegúrate que en todos los formularios (en papel o electrónicos) en que se recaben datos personales está puesta la cláusula de información relativa a la protección de datos según establece el artículo 13 del RGPD y que la actividad está incluida en alguno de los tratamientos recogidos en el Registro de las Actividades de Tratamiento de la Universidad.
2. No solicitar ni recabar de la persona más datos que los estrictamente pertinentes, necesarios e imprescindibles para el uso o finalidad del tratamiento.
3. No tratar ni reutilizar los datos para otros usos o fines diferentes e incompatibles con el inicial para el que se recabaron o solicitaron del interesado.
4. Acceder exclusivamente a aquella información personal o recursos técnicos que se precise y esté autorizado para el desarrollo de las funciones propias de la actividad

profesional y no a otros datos o recursos, aunque estén disponibles y sean accesibles.

5. Guardar secreto profesional y confidencialidad de la información a la que se tiene acceso: nunca divulgues, publiques ni reveles datos de carácter personal a terceras personas.

   a) No ceder o comunicar datos personales a terceros salvo que sea necesario para el tratamiento, por obligación legal o por consentimiento expreso de la persona afectada.

   b) No publicar listados en la página web o tablones de anuncios con nombres y apellidos y NIF/NIE completos sin anonimizar. Puede consultar aquí cómo anonimizar el DNI en excel

   c) No grabar ni difundir imágenes sin el previo y expreso consentimiento de las personas afectadas.

   d) No enviar por emails archivos o ficheros con datos personales fuera del ámbito de la Universidad sin las medidas de seguridad que garanticen que dicha información solo sea accesible por su destinatario (p.ej. contraseña de acceso, cifrado de datos, etc.).

6. Borrar los datos personales, o bloquear su acceso, cuando ya no sea necesario su tratamiento o conservación para la finalidad para la que se recabaron.

7. En el acceso y tratamiento de la información los usuarios están obligados a cumplir todas las medidas de seguridad establecidas por la normativa en protección de datos, y demás requisitos aplicables conforme a las normas y procedimientos establecidos por la Universidad

8. Facilitar el ejercicio de los derechos a los titulares de los datos personales que lo soliciten, informando a la delegada.protecciondedatos@uam.es .

9. Comunicar cualquier incidencia, vulneración o quiebra de seguridad en el tratamiento de los datos personales a la delegada.protecciondedatos@uam.es y a Tecnologías de la Información cert@uam.es

10. Asistir al menos a un curso o sesión formativa sobre protección de datos

Uso y configuración de los equipos informáticos.

1. Los equipos informáticos que la Universidad pone a disposición de sus empleados no deben ser utilizados para fines particulares o privados, tan solo se permite su uso para el desarrollo de tareas académicas, investigadoras o profesionales debiendo observarse en todo momento el deber de diligencia en la utilización del mismo.

2. No se podrán modificar la configuración de los equipos informáticos ni el software instalados a nivel corporativo, ni conectar los puestos de trabajo a redes o sistemas exteriores ajenos a la Universidad, que no estén autorizados por los administradores del sistema.

3. Todos los equipos deberán mantener siempre actualizadas las aplicaciones informáticas y el antivirus correspondiente. No está permitida la desactivación de dichos mecanismos.

4. Activar el bloqueo automático de sesión de nuestros equipos cuando no se utilicen durante un tiempo determinado (p.ej. 5-10 minutos de inactividad)

5. Se prohíbe la instalación de programas o software sin licencia o no corporativos en los ordenadores dado el peligro de que puedan contener programas malignos, como v*irus*, *troyanos o malware.* Si fuera necesaria su instalación, deberá solicitarse al centro de atención a usuarios cau@uam.es para que lo gestione.

6. No deben almacenarse en el disco duro o memoria de los ordenadores documentos que contengan datos de carácter personal utilizando preferentemente las carpetas de las unidades de red o el almacenamiento en la nube a través de OneDrive o Microsoft Teams.

   En caso contrario, los usuarios serán responsables de la custodia y respaldo de toda la información que almacenen en los mismos y deberán realizar periódicamente copias de seguridad, respaldo o backups de los ficheros.

7. Los archivos temporales o las descargas de archivos que contengan datos personales se realizarán en un mismo directorio de forma que no queden dispersos por todo el disco duro del ordenador para proceder periódicamente a su borrado cuando ya no sean necesarios.

8. No se deberán sacar equipos fuera de las instalaciones de la Universidad, excepto que estuviera previamente autorizado para ello y se apliquen las debidas medidas de seguridad para proteger su contenido y archivos.

9. Los usuarios comunicarán cualquier incidencia de funcionamiento o deficiencia de las aplicaciones informáticas que hubieran podido observar al responsable informático del centro, y/o al centro de atención a usuarios cau@uam.es

   Cuando la incidencia y/o deficiencia pudiera suponer una vulneración o quiebra de seguridad en el tratamiento de los datos personales, los usuarios lo podrán en conocimiento del cert@uam.es, y a la delegada.protecciondedatos@uam.es, a fin de que se adopten las medidas oportunas.

Control de cuentas de usuarios y contraseñas

1. Tanto las cuentas de usuario como los certificados digitales son personales e intransferibles y los usuarios deben ser conscientes de que son responsables de las acciones que se realicen con su identidad en los sistemas de información.

   En ningún caso, se deberán facilitar ni revelar a terceros u otros usuarios las claves, password o códigos (PIN, contraseña, etc.) que puedan ser necesarios para su acceso o activación debiendo mantenerlas en todo momento en secreto.

2. Los usuarios deben ser cuidadosos y diligentes en la custodia y salvaguarda de sus claves privadas y contraseñas, debiendo informar a la mayor brevedad al centro de atención a usuarios cau@uam.es cuando haya razones para creer que una contraseña ha sido robada, comprometida o compartida.

3. Nunca reutilizar las contraseñas utilizadas en las distintas aplicaciones de la UAM en servicios proveedores de terceros o para usos privados y personales.

4. Cada usuario es responsable del control, confidencialidad y cambio de la contraseña de acceso a los equipos informáticos. Se recomienda:

   a) Usa una contraseña diferente para cada cuenta o aplicación.

   b) Cambiar la contraseña periódicamente (p.ej cada 15 o 24 meses). Elija una nueva contraseña no relacionada con la anterior.

   c) La contraseña debe ser lo suficientemente larga y compleja para no ser adivinable por terceros. Preferiblemente deberá contener al menos 8 dígitos así como números, letras mayúsculas y minúsculas o algún signo de puntuación.

   d) Activar la autenticación de doble factor o multifactor (MFA) siempre que sea posible.

   e) Use un programa de gestión de contraseñas (p.ej. LastPass, Dashlane) para poder recordarlas y nunca las anote en una libreta o cuaderno.

Internet y cuentas de correo electrónico

1. La utilización de Internet y el correo electrónico corporativo debe responder exclusivamente a fines profesionales, docentes o académicos, debiendo observarse el deber de diligencia en la utilización del mismo.

2. No se accederá a páginas de intercambio y descarga de archivos P2P, redes sociales, correo electrónico personal, páginas web inseguras, así como otros sitios susceptibles de contener virus o favorecer la ejecución de código dañino.

3. No publicar o divulgar en internet, redes sociales, foros, etc. imágenes, videos o listados con nombres y apellidos y NIF/NIE completos sin anonimizar (puede consultar aquí cómo anonimizar el DNI en excel) sin consentimiento expreso de las personas afectadas o lo habilite una ley.

4. No enviar por emails archivos o ficheros con datos personales sin las medidas de seguridad que garanticen que dicha información no sea inteligible ni manipulada por terceros durante la transmisión o que tan solo sea accesible por su destinatario (p.ej. contraseña de acceso, cifrado de datos, etc.).

5. Para evitar el correo masivo no solicitado, también denominado "spam", como regla general, solo se debe dar nuestra dirección de correo electrónico a personas y/o entidades conocidas. Nunca se facilitará nuestra cuenta de correo electrónico en foros, redes sociales o páginas web no institucionales.

6. En el caso de recibir correos electrónicos cuyo remitente y/o contenido sea dudoso, no abrir los archivos adjuntos y ponerse en contacto con el centro de atención de usuarios cau@uam.es para que se analice su posible malignidad.

La seguridad en los dispositivos móviles y smartphones

1. Activa el desbloqueo del teléfono con contraseña o datos biométricos mejor que un patrón.

2. Mantén siempre el dispositivo, aplicaciones y el antivirus actualizados.

3. Desactiva la Wifi y el Bluetooth cuando no sean necesarios. No conectarse a redes Wifi públicas y abiertas

4. Modifica tu configuración de privacidad para limitar el acceso de las diferentes aplicaciones a tus datos. Controla los permisos que habilitas en la descarga de aplicaciones o apps.

5. Evita descargar y guardar en el dispositivo archivos con datos personales o confidenciales. Si es necesario conservarlos, almacénalos en la nube en carpetas de OneDrive o protégelos con una contraseña de acceso.

6. Instalar o activar un servicio de localización para poder recuperar los dispositivos en caso de pérdida, extravío o sustracción.

Impedir la accesibilidad a los datos por personas no autorizadas

1. Custodiar la documentación y garantizar que los datos e información tratada desde su puesto de trabajo no pueda ser visible ni accesible por personas no autorizadas.
    a) La pantalla del ordenador estará orientada para que la información sólo pueda ser visible por el usuario y no por terceras personas.
    b) No deje a la vista documentos con datos personales sobre la mesa, fotocopiadoras o impresoras, etc.
    c) Una vez que haya finalizado el trabajo, los documentos en papel no deben quedarse en la mesa y deberán guardarse bajo llave en su archivador correspondiente o se destruirán.
    d) Cuando los usuarios dejen desatendido el ordenador deberán activar el sistema de bloqueo del que disponga su equipo (salvapantalla protegido por contraseña, bloqueo del terminal, etc.) con el fin de que se no visualicen datos en la pantalla, así como evitar que se acceda al equipo o aplicaciones por terceros no autorizados.
2. Asegurarse que cuando se ausente de su puesto de trabajo, bien temporalmente o bien al finalizar la jornada de trabajo, el despacho queda cerrado con llave, el ordenador queda apagado para evitar que se acceda al equipo y no quedan sobre la mesa documentos que contengan datos de carácter personal.

Trabajo fuera de las oficinas

1. Debe evitarse simultanear la actividad personal o doméstica con la académica y profesional por lo que hay que definir perfiles independientes para desarrollar cada tipo de tarea.

2. Se evitará la conexión de los dispositivos portátiles a la red corporativa desde lugares públicos, así como la conexión a redes WIFI abiertas no seguras, utilizando preferiblemente conexión remota VPN para acceder a la red de la Universidad.

3. Se implementarán las medidas de seguridad preventivas que sean apropiadas para salvaguardar la integridad y confidencialidad de los datos personales cuando se trabaje con el fichero o documentos en papel fuera de la oficina o puesto de trabajo habitual.
    a) No se llevará ni transportará expedientes ni documentación en papel sin las correspondientes medidas de seguridad que garanticen su custodia y

confidencialidad (p.ej. archivadores con llave). Siempre que sea posible y los medios lo permitan, se recomienda escanear la documentación para convertir los documentos en papel a soporte electrónico.

b) No se deberá copiar ni transportar información en ordenadores portátiles, smartphone, tabletas, discos externos, pendrive, etc. sin las correspondientes medidas de seguridad (contraseña de acceso, cifrado de datos, etc.).

c) En la medida de lo posible, evitaremos trabajar con archivos en el disco duro del portátil, utilizando y almacenando la información en las unidades de red y/o en las cuentas de OneDrive o Microsoft Teams que la Universidad pone a disposición de todos los usuarios.

4. Cuando se hable por teléfono, se evitará que se puedan escuchar conversaciones por parte de terceros ajenos utilizando, por ejemplo, auriculares y micrófono o retirándose a un espacio en el que la persona empleada no esté acompañada.

5. En las pausas o concluida la jornada de trabajo debe desconectarse la sesión de acceso remoto y bloquear o apagar el uso del dispositivo para evitar accesos no autorizados por parte de terceros y guardar los documentos que contengan datos de carácter personal.

Destrucción de información y soportes

1. Si habitualmente se genera y trabaja con papel, es importante extremar las precauciones para evitar arrojar hojas enteras o en trozos en papeleras a los que alguien podría acceder y recuperar la información de carácter personal.

2. La destrucción de la información que contenga datos de carácter personal, cualquiera que sea su soporte (ordenadores, CDs, disketes o en papel) deberá ser de tal forma que no pueda ser recuperada ni manipulada por terceras personas utilizando preferentemente las máquinas destructoras.

Sitios de interés

Puedes encontrar más información, guías y recomendaciones con el fin de mejorar el grado de seguridad de los sistemas de información y la confidencialidad de los datos personales en las siguientes webs:

- Agencia Española de Protección de Datos (AEPD)
- Instituto Nacional de Ciberseguridad de España (INCIBE)
- Centro Criptológico Nacional (CCN-CERT)