DECÁLOGO PROTECCIÓN DE DATOS PERSONALES

para el personal de la Universidad de Granada

Proteger los datos es proteger personas. Una responsabilidad compartida en la UGR

1	**Trate los datos personales ajenos como querría que tratasen los suyos**	• Los datos no son de quien los trata, sino de su titular, la persona a la que identifican. Sólo esa persona tiene derecho a decidir y obtener información sobre quién los puede tratar, con qué finalidad y a quién se pueden comunicar o ceder.
2	**Recabe y utilice la información mínima necesaria**	• Existen limitaciones en la recogida y utilización de información con datos personales, que deberán ser siempre exactos, adecuados, pertinentes y ajustados a la finalidad para la que son recogidos. • Recabe y utilice la información mínima necesaria para desempeñar satisfactoriamente su función profesional, docente o investigadora.
3	**No comunique datos personales a terceros no autorizados**	• No debe facilitar datos a personas distintas de su titular, aunque se trate de familiares o personas conocidas. Por este motivo, no proporcione nunca por teléfono datos personales e información confidencial, incluso si el interlocutor dice ser su titular.
4	**Conozca sus obligaciones de confidencialidad**	• Cualquier persona que trate datos personales de terceros está sujeta al deber de confidencialidad, que perdurará incluso una vez finalizada la relación profesional con la Universidad. • No comparta información. Evite comentar con otras personas datos personales o confidenciales que trate en el ejercicio de su actividad, salvo que las personas afectadas hayan consentido o tenga una justificación lícita.
5	**Asegúrese de que el medio de comunicación sea privado**	• Los servicios, aplicaciones y redes sociales suelen tener sólidos mecanismos de seguridad frente a terceros, pero utilizan intensivamente los datos personales que les proporcionamos. Por ello, el tratamiento de información personal y las comunicaciones deben llevarse a cabo, preferentemente, a través de medios propios puestos a disposición por la Universidad de Granada (plataformas educativas, correo electrónico, nubes privadas como "UGRDrive" o "Documenta"…).

6	**Preserve el acceso no autorizado a los datos**	• Bloquee su equipo cuando se ausente, y apáguelo cuando se marche si otra cosa no se le hubiese indicado (por ejemplo, para realizar actualizaciones). • No deje a la vista documentación con datos personales o confidenciales de otras personas sin su supervisión. • Siga una política de mesas limpias y guarde bajo llave, al finalizar la jornada, toda la documentación que maneje en tu trabajo. • Evite llevar documentos, soportes digitales o equipos electrónicos con datos personales fuera de su lugar de trabajo. En su caso, establezca medidas de seguridad dirigidas a evitar el acceso a su contenido, como el cifrado de los soportes o dispositivos.
7	**Destruya los soportes que no necesita**	• No tire a la papelera documentos con datos personales, DVDs, lápices USB, ni otros soportes sin proceder previamente a la destrucción bien de la información que contiene, bien del soporte mismo, de modo que no pueda recuperarse tal información. • Utilice una destructora de documentos/soportes, o un programa de borrado (no basta la opción ordinaria de borrar archivo).
8	**Utilice contraseñas complejas de difícil deducción por terceros, cámbielas con regularidad, y no repita la misma**	• Para aumentar la aleatoriedad es deseable que contengan números, letras mayúsculas y minúsculas, y algún signo de puntuación. Puede protegerlas con una contraseña maestra y generar claves aleatorias seguras con un programa de gestión de contraseñas. Si opta por anotarlas, hágalo en un lugar alejado del entorno en que se usan, y sin que resulte evidente a un tercero de qué servicio es la contraseña.
9	**Cumpla con los procedimientos de seguridad y normas internas de protección de la información personal**	• Conozca la Política de Seguridad de la Información de la Universidad de Granada y sus normas de usos aceptables y buenas prácticas (por ejemplo, normas de uso de sistemas, servicios y comunicaciones, de uso de internet, de correo electrónico, etc.), así como las medidas de protección a aplicar al tratamiento de información con datos personales.
10	**Comunique cualquier incidencia de seguridad**	• Reporte cualquier incidencia que pueda conducir a una comunicación o acceso no autorizado a datos personales, o a su destrucción, pérdida o alteración ilícita, a la Oficina de Protección de Datos (protecciondedatos@ugr.es) o al Área de Seguridad Informática del CSIRC (seguridadinformática@ugr.es).