

DECÁLOGO DE BUENAS PRÁCTICAS EN PROTECCIÓN DE DATOS PERSONALES

1. **CESION DE DATOS:** No des información con datos personales de forma verbal, escrita, por correo, por teléfono, ni fax, sin asegurarte que los destinatarios están autorizados a conocerlos.
2. **CONTRASEÑA:** No la compartas ni la apuntes en sitio visible. Todo lo que hagan con ella, se considera que lo has hecho tú.
3. **CORREO:** No abras correos sospechosos y evita arrastrar correos con datos personales y reenviarlos, sin asegurarte de que todos los destinatarios están autorizados a conocerlos.
4. **TRASLADO DE DATOS:** No traslades información con datos personales sin la protección necesaria, sobres, carpetas, contenedores, tampoco de tu ordenador a ordenadores no corporativos.
5. **DISPOSITIVOS:** No conectes dispositivos USB con contenidos no conocidos o no confiables.
6. **MESAS LIMPIAS:** Cuando te ausentes de tu puesto de trabajo, no dejes sobre la mesa documentos desprotegidos con datos personales y siempre bloquea tu equipo.
7. **DESTRUCCIÓN** de documentos con datos personales, siempre triturado o en contenedores especiales, nunca los tires a una papelera o contenedor de papel general.
8. **PANTALLAZOS:** no imprimas ni guardes en papel pantallazos o fotocopias con datos personales. Eres responsable del uso que se haga de ellos y de su destrucción en forma legal.
9. **INTERNET:** No compartas datos personales del trabajo en Internet. En general las redes, (WhatsApp, Dropbox, Facebook, etc.), no gozan de la necesaria seguridad corporativa. (Todo lo que está en Internet es jaqueable).
10. **DIFUSIÓN** de las buenas prácticas entre tus compañeros de trabajo. Si detectas prácticas mejorables o incidencias de seguridad, ponlo en conocimiento de tus superiores.