Gestión de Contraseñas para la seguridad y confidencialidad de los datos personales.

Las contraseñas son, junto al código o identificador de usuario, el medio de acceso a los datos personales y a los equipos utilizados para su tratamiento. De tal modo, para garantizar una seguridad y confidencialidad adecuadas de los datos personales, es necesario que las contraseñas que se utilicen como mecanismo de autenticación para el acceso a los mismos sean **«robustas»**, esto es, difícilmente vulnerables.

El artículo 5, apartado 2, del Reglamento (UE) 2016/679, establece expresamente el principio de «responsabilidad proactiva», según el cual el responsable del tratamiento será responsable del cumplimiento (y capaz de demostrarlo), entre otros, de los principios de «integridad y confidencialidad», según el cual:

"Los datos personales serán tratados de tal manera que se garantice una seguridad adecuada de los datos personales, incluida la protección contra el tratamiento no autorizado o ilícito y contra su pérdida, destrucción o daño accidental, mediante la aplicación de medidas técnicas u organizativas apropiadas («integridad y confidencialidad»)".

Las contraseñas deben ser fáciles de recordar y de introducir por el usuario, y asimismo difíciles de adivinar y de descubrir. Decimos por esto, que las contraseñas deben ser robustas.

«Directrices generales para la creación de contraseñas robustas»:

- Deberán tener una longitud mínima de 8 caracteres.
- Deberán combinar caracteres de distinto tipo: letras mayúsculas y minúsculas, números y signos de puntuación.
- No deberán coincidir con el código o identificador de usuario.
- No deberán estar basadas en cadenas de caracteres que sean fácilmente asociables al usuario: nombre, apellidos, ciudad o fecha de nacimiento, número de DNI, nombres de familiares, matrícula del coche, etc., o combinaciones de las mismas (por ejemplo, nombre + año de nacimiento).
- No deberán estar basadas en el uso de caracteres repetitivos (por ejemplo, «aaaaaaaa») o secuenciales (por ejemplo, «1234abcd».
- No deberán coincidir con palabras sencillas en cualquier idioma que puedan figurar en un diccionario.
- No deberán estar basadas en palabras formadas por caracteres próximos en el teclado (por ejemplo, «qwertyui»).
- La contraseña no deberá ser igual a ninguna de las últimas contraseñas usadas (no reutilización).

«Directrices generales de uso de contraseñas»

- El usuario deberá salvaguardar en todo momento el carácter confidencial, personal e intransferible de la contraseña. No deberá entregarla ni comunicarla a nadie. En caso de haber tenido necesidad de hacerlo por motivos de trabajo o mantenimiento, el usuario deberá proceder a cambiarla de forma inmediata.
- El usuario no deberá apuntar su contraseña en un papel, pósit, o en cualquier otro lugar no seguro.
- El usuario no deberá escribir su contraseña en correos electrónicos ni en formularios web cuyo origen no sea confiable.
- El usuario no deberá utilizar la misma contraseña para el acceso a distintos servicios o recursos.
- El usuario no deberá utilizar la misma contraseña para el acceso a distintos dispositivos.
- El usuario no deberá utilizar la misma contraseña para uso profesional y para uso personal o doméstico.
- El usuario no deberá hacer uso de funcionalidades de recordatorio de contraseñas, ya que pueden facilitar el acceso a personas no autorizadas.
- El usuario deberá proceder a cambiar la contraseña de forma inmediata si tiene indicios de que la confidencialidad de la misma ha podido verse comprometida.
- Ningún usuario está autorizado a acceder al sistema de información utilizando el código o identificador de usuario y la contraseña de otros usuarios.

Ante cualquier duda, por favor contacte con el Responsable de Seguridad: informatica@huesca.es o el Delegado de Protección de Datos Personales: dpd@huesca.es