Gestión segura de contraseñas

Todos/as los/as trabajadores/as que realizan un tratamiento de datos están obligados/as a adoptar medidas técnicas y organizativas que garanticen la protección de datos personales. El conocimiento de los siguientes aspectos sobre **la gestión segura de contraseñas** es de especial interés para el total de los/as trabajadores/as, y contribuye a reducir los riesgos inherentes de tales situaciones para los derechos y libertades de los interesados/as.

1. Es muy recomendable **no utilizar las contraseñas por defecto**. Debemos cambiar las claves por defecto, las que traen los equipos y sistemas al adquirirlos, por otras a nuestra elección.

2. Se aconseja implantar un **sistema de autenticación doble** en el acceso a servicios que contengan información especialmente sensible o crítica.

3. **No compartir** las contraseñas con nadie, ya que dejarán de ser secretas y por tanto perderán su utilidad. Debemos asegurarnos de lo siguiente:

   - No compartirlas con nadie;
   - No apuntarlas en papeles o post-it;
   - No escribirlas en correos electrónicos o formularios de webs no confiables.

4. Las contraseñas **deben de ser robustas**:
   - Deben contener al menos ocho caracteres;
   - Deben combinar caracteres de distinto tipo (mayúsculas, minúsculas, números y símbolos);
   - No deben contener los siguientes tipos de palabras:
     - palabras sencillas en cualquier idioma;

- nombres propios, fechas, lugares o datos de carácter personal;
- palabras que estén formadas por caracteres próximos en el teclado;
- palabras excesivamente cortas.

➢ Tampoco se deben utilizar claves formadas únicamente por elementos o palabras que puedan ser públicas o fácilmente adivinables (ej. nombre + fecha de nacimiento);

5. No utilizar la misma contraseña para servicios diferentes. **Nunca debemos utilizar la misma contraseña para diferentes servicios**, ni tampoco utilizaremos las mismas contraseñas para uso profesional y doméstico.

6. Cambiar las contraseñas periódicamente. Para garantizar la confidencialidad de nuestras **contraseñas deben ser cambiadas periódicamente**. No deben utilizarse contraseñas que hayan sido usadas con anterioridad. Pueden utilizarse sistemas que fuercen al cambio de contraseña en el plazo seleccionado.

7. **No hacer uso del recordatorio de contraseñas**. No es recomendable utilizar las funcionalidades de recordatorio de contraseñas, ya que pueden facilitar el acceso a personal no autorizado. Esto es especialmente frecuente en el uso de navegadores web.

8. Utilizar gestores de contraseñas. Debemos considerar **el uso de gestores de contraseñas en aquellos casos en los que tengamos que recordar un gran número de ellas** para acceder a muchos servicios. En estos casos es muy recomendable elegir un gestor cuyo control quede bajo nuestra supervisión, que cifre las credenciales e implantar doble factor de autenticación para acceder al mismo.

Ante cualquier duda, contacte con el Responsable informatica@huesca.es o el Delegado de Protección de Datos Personales dpdhuesca@unive.es