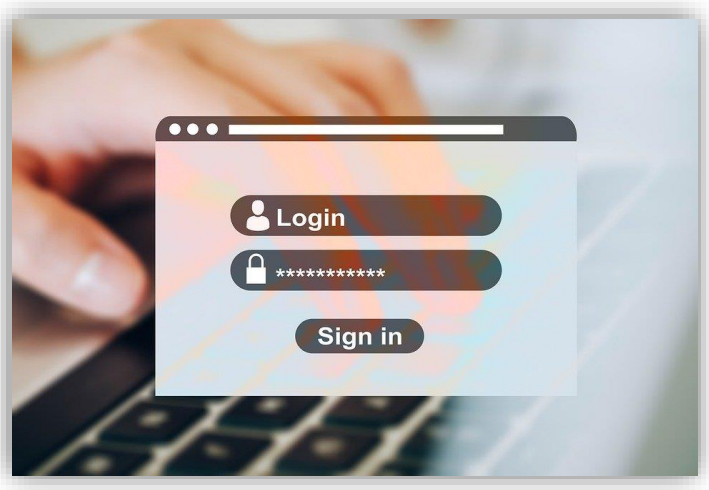
Control de acceso

Las Administraciones Públicas tratan una gran variedad de datos personales de sus ciudadanos.

Así, el acceso a esta información está restringido a aquel personal que, para el desempeño de sus funciones, deba acceder a la información.

La información se puede almacenar y tratar en formato papel, pero en esta breve comunicación, nos queremos enfocar en aspectos a tener en cuenta para proteger la información tratada en soportes digitales.



En la actualidad, la documentación que contiene datos personales de los ciudadanos está accesible a través de sistemas informáticos, a los cuales se debe garantizar un acceso autorizado, para evitar que los datos personales no sean alterados, borrados o utilizados con fines no autorizados.

Es esencial contar con métodos seguros de **identificación y autorización** en los sistemas y equipos de las Administraciones Públicas, así como un **control de acceso**, cuando sea requerido.

Así pues, éstas son algunas de las medidas que el personal deberá tener en cuenta:

- Cuando el personal abandone el puesto de trabajo, temporalmente o al finalizar la jornada laboral, debe dejarlo en estado que impida acceso o visualización al contenido. Lo podrá hacer a través de un salvapantallas y para su reanudación será necesaria contraseña.

- Es necesario que el acceso a la documentación esté protegido y cada empleado debe disponer de una contraseña asignada a un perfil que permita el acceso y en el cual se definan los tratamientos permitidos.

- La contraseña y usuario de acceso de cada trabajador debe ser personal e intransferible, estando prohibida la relevación de esta. La contraseña no se debe almacenar en un lugar visible, que permita su visualización por terceros.

- Las contraseñas deben ser modificadas al menos una vez al año y deben contener una serie de parámetros:

  Longitud mínima de 8 caracteres, entre los que debe figurar al menos una letra mayúscula, minúscula, número y carácter especial.

- Siempre que el personal tenga acceso a la información del sistema, deberá estar identificado de forma única, de modo que se sepa en todo momento quién tiene acceso y quién ha realizado una determinada actividad.

- En los supuestos en los que el personal tenga certeza o sospechas del uso de su identificador o contraseñas por otra persona distinta, deberá comunicarlo al responsable de seguridad.

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