## ***Teletrabajo***

Debido a la situación de emergencia motivada por el COVID-19, el teletrabajo se está generalizando, y en ocasiones, implantando de manera urgente para adaptarse a las circunstancias actuales y así poder continuar con la actividad pública del Ayuntamiento.

No obstante, se debe atender a los posibles riesgos asociados a la privacidad y seguridad de los datos personales, de las que el propio Ayuntamiento es responsable.

Es necesario que todos los empleados públicos cumplan con una serie de recomendaciones para la protección de los datos personales en la modalidad de teletrabajo, en especial cuando estos utilicen sus propios dispositivos informáticos:

- Respetar **las políticas de protección de datos**, así como otras instrucciones recibidas en cuanto a la utilización de dispositivos facilitada por el Ayuntamiento.

- Garantizar el cumplimiento del deber de **confidencialidad** en relación con los datos personales a los que tuviera acceso en el desempeño de sus funciones laborales.

- Proteger el dispositivo utilizado, así como el acceso al mismo, a través de la utilización de **contraseñas** de acceso robustas (longitud mínima de 8 caracteres, combinando letras, números y caracteres especiales). Esta contraseña se modificará como mínimo una vez al año, y será diferente a la utilizada para acceder a cuentas personales, redes sociales y otro tipo de aplicaciones utilizadas en su ámbito de su vida personal.

- Mantener **actualizado el sistema operativo**, así como otras aplicaciones instaladas.

- Controlar que el sistema **antivirus** instalado en el equipo esté operativo y actualizado.

- Evitar la conexión a **redes wifi públicas y/o abiertas** o no confiables.

- **Desconectar la sesión** de acceso remoto y apagar o bloquear el acceso al dispositivo cuando no lo esté utilizando o haya finalizado la jornada de trabajo.

- Guardar la **información** en los espacios de red habilitados, evitando el almacenamiento de la información de forma local en el dispositivo utilizado. No se debe utilizar dispositivos de almacenamiento portátiles, tales como USB, discos duros externos, etc.

**En el caso de sospecha de cualquier anomalía que pueda comprometer la seguridad de la información, se debe notificar de forma inmediata al Delegado de Protección de Datos o Responsable de Seguridad.**

- Si es necesario **extraer documentación** en papel, se deberá disponer de la debida autorización y en su caso, registrar cada salida.

- No utilizar bajo ningún concepto **aplicaciones no autorizadas** por el Ayuntamiento para compartir información, como puede ser correos personales o mensajería rápida, entre otros.

- El empleado público **no debe utilizar el correo para enviar datos personales**, u otra información confidencial, si esta comunicación no entrara dentro de sus tareas profesionales.

- **Garantizar la protección de la información** que se está manejando, tanto en lugares públicos como en el entorno doméstico, no dejando documentos visibles o evitando la exposición de la pantalla a la mirada de terceros.

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