RESUMEN DE PUNTOS A TENER EN CUENTA POR EL USUARIO

1. Creación, modificación y supresión de ficheros.
2. Extracción y cesión de datos.
3. Puesto de trabajo y acceso al sistema.
4. Incidencias.
5. Impresoras.
6. Derechos de los titulares de los datos.
7. Deber de secreto.

1. Creación, modificación y supresión de ficheros

En la Intranet de la Universidad no se almacenan ni se utilizan otros datos de carácter personal que los que la Universidad considera necesarios para el cumplimiento de sus fines.

La creación o supresión de un fichero con datos de carácter personal en el sistema informático de la Universidad sólo puede realizarse previa autorización del Rectorado.

Lo mismo sucede con la modificación de la estructura de un fichero ya creado o con la alteración de su finalidad.

No hacen falta especiales requisitos para introducir nuevos registros en un fichero ya creado, ni para actualizarlos, en el normal desarrollo del trabajo.

2. Extracción y cesión de datos

La incorporación de datos personales de un fichero del sistema informático de la Universidad a otro fichero o la comunicación de esos datos a otra persona o entidad en cualquier soporte o formato requiere la conformidad previa por escrito del responsable del fichero. Por ese motivo, al rellenar los impresos en los que se recaban datos personales, los interesados dan su consentimiento para compartir esos datos con las entidades que colaboran institucionalmente con los fines de la Universidad (como la Asociación de Amigos, por ejemplo).

Este es un punto especialmente importante, porque las consecuencias jurídicas de una cesión no autorizada de datos (aunque se produzca sólo por descuido) pueden ser muy graves.

Así, por ejemplo, en un envío múltiple de correo electrónico basado en una lista de direcciones, debe evitarse que el mensaje contenga todas las direcciones de correo electrónico incluidas en la lista.

La publicación, por descuido o buscando otras finalidades, de datos de carácter personal en la página web de la Universidad de Navarra, sin el consentimiento de los interesados (curriculum vitae, por ejemplo), puede ser calificada como cesión de datos.

3. Puesto de trabajo y acceso al sistema

Cada usuario tiene una contraseña para acceder al sistema informático. de acuerdo con el nivel de acceso que tenga asignado su cometido profesional. La contraseña no debe ser conocida por ninguna otra persona.

El usuario puede modificar su contraseña cuando le parezca oportuno y deberá hacerlo cuando sepa o sospeche que otra persona la conoce.

El usuario es responsable de cualquier acceso al sistema que se realice con su contraseña desde cualquier puesto de trabajo. Cuando se ausente de su puesto de trabajo por cualquier motivo, deberá apagar o bloquear el ordenador.

4. Incidencias

Pueden producirse sucesos o situaciones en los que el usuario advierta que hay un fallo en la seguridad, integridad o confidencialidad de los datos personales contenidos en el sistema informático. A título de ejemplo, pueden mencionarse los siguientes casos:

- Cualquier fallo del sistema de seguridad informática que posibilite el acceso a los datos personales de personas no autorizadas.

- El intento no autorizado de sacar de la Universidad un soporte físico con datos personales.

- La destrucción total o parcial del soporte físico en el que se encuentren datos personales.

- El cambio no autorizado de ubicación física de ficheros de datos personales.

- Los intentos de acceso no autorizados o fallidos a ficheros con datos de carácter personal.

- Conocimiento por terceros del identificador de usuario o clave de acceso al sistema.

- Modificación de datos por personal no autorizado o desconocido.

- Pérdida de información.

- Existencia de sistemas de información sin las debidas medidas de seguridad.

El usuario que tenga conocimiento de alguna de estas incidencias (o cualquier otra que, por sentido común, resulte equivalente) deberá advertir de lo sucedido al responsable del fichero de que se trate, cumplimentando el formulario que se encuentra disponible en la Intranet de la Universidad y remitiéndolo a: ***seguridatos@unav.es***

5. Impresoras

Sólo deberán imprimirse datos de carácter personal cuando sea preciso para realizar las funciones que correspondan al usuario en la Universidad.

El usuario deberá recoger con prontitud el papel impreso, evitando dejar trabajos en la bandeja de salida de la impresora.

Una vez cumplida su función, los documentos en soporte papel que contengan datos personales deben destruirse.

6. Derechos de los titulares de los datos

Cuando algún interesado se dirija a un usuario del sistema manifestando alguna pretensión en relación con sus datos de carácter personal incorporados a algún fichero en el sistema informático general de la Universidad (como puede ser, por ejemplo, su voluntad de modificarlos o cancelarlos), el usuario trasladará cuanto antes esa pretensión al responsable del fichero de que se trate, cumplimentando el formulario que se encuentra disponible en la Intranet de la Universidad y remitiéndolo a seguridatos@unav.es con la mayor presteza.

7. Deber de secreto

Los usuarios de las bases de datos de carácter personal están sujetos a un deber de secreto. La revelación de datos personales a terceras personas puede causar prejuicios irreparables a los interesados además de las correspondientes sanciones a los que los revelen. Este deber sigue existiendo incluso una vez extinguida la relación laboral con la Universidad de Navarra.