

RESUMEN DE LA NORMATIVA DE PROTECCIÓN DE DATOS

Ámbito

La normativa y procedimientos para la protección de los datos de carácter personal se recogen de forma completa en el **Documento de Seguridad de Realía Business**. Este documento constituye un extracto de las normas de actuación que impone a todo el personal, propio y subcontratado, que acceda a los datos manejados por Realía Business

Creación y tratamiento de ficheros con datos de carácter personal

Se ha de tener especial cuidado en el tratamiento de ficheros con datos de carácter personal¹, a lo largo de su ciclo de vida. En caso de duda consultar con el Responsable de Seguridad.

- Creación: no se pueden crear nuevos ficheros con datos de carácter personal sin verificar que se adecuan a los identificados y declarados por Realía Business.
- Tratamiento: no se pueden utilizar los datos para finalidades diferentes sin comprobar si se ajustan a las declaradas.
- Salidas de Datos: las salidas de datos a terceros deben estar o bien consentidas por los interesados en los contratos o impresos de recogida de datos, o bien reguladas por un contrato de prestación de servicios.
- Desechado de soportes: los soportes (informáticos o papel) que contengan datos personales deben ser destruidos al desecharlos o se debe eliminar la información que contienen.

Derechos de acceso, rectificación y cancelación de datos de carácter personal

Las personas sobre las que se manejan datos tienen derecho a:

- Acceso: conocer que datos suyos se manejan.
- Rectificación: pedir su rectificación si son erróneos.
- Cancelación: solicitar su cancelación para todos aquellos casos en que no haya una relación contractual que exija su manejo.

Los plazos para atender estos derechos son estrictos y cortos (acceso: 30 días, rectificación y cancelación: 10 días), por lo que se actuará de la siguiente manera:

Cualquier empleado que reciba por cualquier medio la solicitud de una persona para ejercer sus derechos, o de modo más general para acogerse a la Ley Orgánica de Protección de Datos (LOPD), debe transmitir de modo inmediato dicha solicitud al área responsable del fichero de que se trate o, si no la conoce, al Responsable de Seguridad para su tratamiento.

Normas de acceso a los Sistemas de Información y a los datos

- Los usuarios deben disponer de un único acceso autorizado (identificador de usuario y contraseña) a las aplicaciones y son responsables de toda actividad relacionada con el uso de su acceso autorizado.
- Los usuarios no deben revelar bajo ningún concepto su identificador y/o contraseña a otra persona, ni mantenerla por escrito a la vista o al alcance de terceros.
- Los usuarios no deben utilizar ningún acceso autorizado de otro usuario, aunque dispongan de la autorización del propietario.
- Si un usuario tiene sospechas de que su acceso autorizado (identificador de usuario y contraseña) está siendo utilizado por otra persona, debe proceder al cambio de su contraseña y comunicar la correspondiente incidencia de seguridad.

¹ Dato de carácter personal: dato de cualquier tipo concerniente a una persona física identificada o identificable.

- Los usuarios deben conocer y cumplir las normas definidas en la Política de contraseñas.
- Los usuarios sólo accederán a aquellos datos y recursos que precisen para el desarrollo de sus funciones.

Normas de Seguridad de los Datos de Carácter Personal (DCPs)

- Proteger, los DCPs a los que tienen acceso, contra revelaciones no autorizadas o accidentales, modificación, destrucción o mal uso.
- Utilizar el menor número de informes en formato papel que contengan DCPs y mantener los mismos en lugar seguro y fuera del alcance de terceros.
- Los usuarios autorizados a manejar soportes que contengan DCPs deben guardar los mismos en un lugar seguro cuando éstos no sean usados, especialmente fuera de la jornada laboral.
- Los usuarios autorizados a manejar soportes que contengan DCPs deben inventariar aquellos que tengan guardados y mantener siempre actualizado este inventario.
- Los usuarios sólo podrán crear ficheros temporales que contengan DCPs, especialmente los ficheros ofimáticos, cuando sea necesario para el desempeño de su trabajo. Estos ficheros temporales deberán estar ubicados en directorios debidamente estructurados de los servidores, y nunca en unidades locales de disco de los puestos PC de usuario. Asimismo deberán ser destruidos cuando hayan dejado de ser útiles para la finalidad para la que se crearon.
- En las agendas de contactos de las herramientas ofimáticas (por ejemplo en Outlook) los usuarios únicamente introducirán datos identificativos y direcciones o teléfonos de personas. En ningún caso introducirán datos o valoraciones de personas físicas relativos a ideología, religión, creencias, origen racial, salud o vida sexual. En caso de incumplimiento de esta norma, las posibles responsabilidades recaerán en el usuario que introdujo los datos.

Política de Contraseñas para el acceso a datos

- Los usuarios de un sistema de información dispondrán de una única y personal cuenta de acceso (Id. de usuario y contraseña).
- Las contraseñas tienen una **caducidad** de, como mínimo, **70 días**
- La **longitud** de las contraseñas será igual o superior a **6 caracteres alfanuméricos**.
- Las cuentas de usuarios que estén **inactivas** durante **90 días**, siempre que tecnológicamente sea posible, serán bloqueadas.
- Las contraseñas se almacenarán en modo cifrado.
- Se limita el número de **reintentos** de acceso fallido a **5**.

Registro de incidencias

Toda persona que detecte una incidencia que pueda afectare a la seguridad de los datos debe comunicarlo al Departamento de Informática para su registro, análisis y actuación. A título de ejemplo no exhaustivo se incluyen los siguiente ejemplos:

- Pérdida de la contraseña
- Pérdida de algún soporte con datos.
- Detección de una posible entrada en los sistemas por personas no autorizadas.
- Necesidad de recuperación de datos.