laboralgroup
CLEVER PARTNER

AYUNTAMIENTO DE CONSUEGRA

FORMACIÓN E INFORMACIÓN A PERSONAS TRABAJADORAS

NORMATIVA DE PROTECCIÓN DE DATOS DE CARÁCTER PERSONAL Y GARANTÍA DE LOS DERECHOS DIGITALES

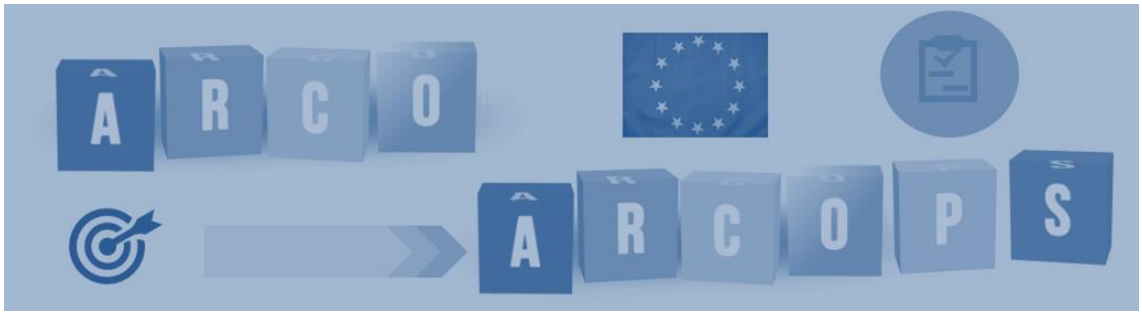
www.laboralgroup.com

Qué HACER si… una persona quiere ejercer sus derechos:

ACTUACIONES EN CASO DE EJERCICIO DE DERECHOS:

- Consultar qué derecho *(ACCESO, RECTIFICACIÓN, CANCELACIÓN (Olvido), OPOSICIÓN, LIMITACIÓN, PORTABILIDAD)* quiere ejercitar.
- Solicitar el **DNI**.
- Facilitarle el documento del ejercicio.
- Informarle del **plazo** de actuación *(Ver en cada documento)*
- Realizar la acción *(Acceder a la base de datos, cambiar o modificar un dato, eliminar el* dato, etc.) y entrega o envío (e-mail) del justificante del derecho ejercido.

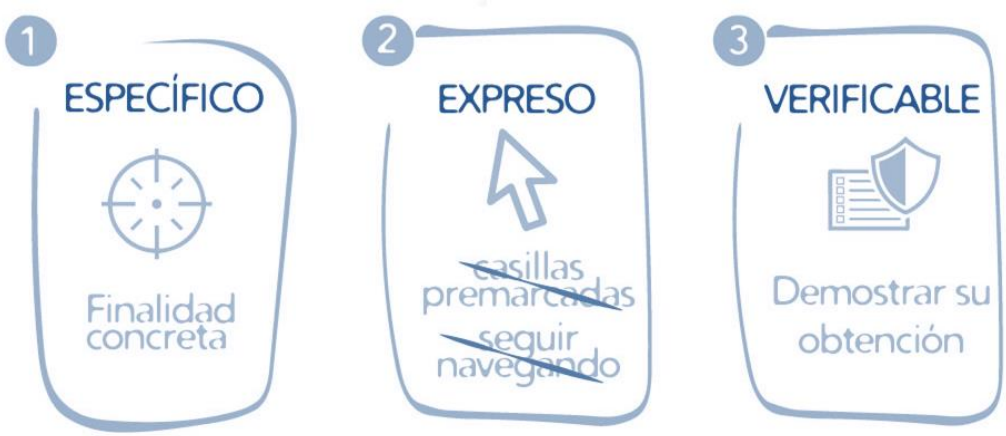
  - Para el **D de acceso** se facilitará a los interesados la lista de los datos personales de que disponga junto con la finalidad para la que han sido recogidos, la identidad de las personas destinatarias de los datos, los plazos de conservación, y la identidad del responsable ante el que pueden solicitar la rectificación supresión y oposición al tratamiento de los datos.
  - Para el **D de rectificación** se procederá a modificar los datos de los interesados que fueran inexactos o incompletos atendiendo a los fines del tratamiento.
  - Para el **D de limitación** estudiaremos que datos quiere suspender y cuales conservar en la actividad de tratamiento.
  - Para el **D de supresión** se suprimirán los datos de los interesados cuando los interesados manifiesten su negativa u oposición al consentimiento para el tratamiento de sus datos y no exista deber legal que lo impida.
  - Para el **D de portabilidad** los interesados deberán comunicar su decisión e informar al responsable, en su caso, sobre la identidad del nuevo responsable al que facilitar sus datos personales.



Qué HACER si… hay que dar de alta a una persona:

ACTUACIONES EN CASO DE CREAR NUEVA FICHA CLIENTE:

- Entregar **documento o ficha** para rellenar con sus datos personales.
- Comprobar que firma el **consentimiento expreso** para la actividad de tratamiento.
- Añadir en **base de datos** de la empresa.



Qué HACER si… tenemos que hacer una copia de seguridad:

ACTUACIONES PARA COPIAS DE SEGURIDAD DE INFORMACIÓN:

- Consultar el **procedimiento** a seguir en la empresa en cuanto a copias de seguridad de la información de los ordenadores. *(Establecido en el PROCEDIMIENTO DE SEGURIDAD elaborado por el RESPONSBALE DE TRATAMIENTO).*
- Disponer de un **PEN, CD, DISCO DURO EXTERNO o claves de acceso a la nube** de datos para poder volcar la información de cada ordenador.
- Cumplir con la **periodicidad** de salida establecida *(Por ejemplo: copias semanales cada viernes).*
- Depositar el medio externo con la copia realizada en el **lugar seguro indicado** *(cajón bajo llave, etc.)*

Qué HACER si… hay una violación de datos:

ACTUACIONES PARA VIOLACIONES DE SEGURIDAD:

- Comunicar al **responsable de tratamiento** (la empresa) la violación de seguridad.
- Enviar a la **autoridad de control** (AEPD) en máximo 72 horas.
- Contenido de la **notificación**:
  - Describir la naturaleza de la violación de la seguridad de los datos personales, inclusive, cuando sea posible, las categorías y el número aproximado de las personas afectadas, y las categorías y el número aproximado de registros de datos personales afectados;
  - Comunicar el nombre y los datos de contacto de la empresa o de otro punto de contacto en el que pueda obtenerse más información;
  - Describir las posibles consecuencias de la violación de la seguridad de los datos personales;
  - Describir las medidas adoptadas o propuestas por el responsable del tratamiento para poner remedio a la violación de la seguridad de los datos personales, incluyendo, si procede, las medidas adoptadas para mitigar los posibles efectos negativos.

Qué HACER si… tengo que cambiar mi contraseña:

- Las contraseñas deben tener al menos **6 caracteres**. *(mayúsculas y minúsculas, no todas iguales, o por cadenas que contengan conjuntamente caracteres alfabéticos y números)*
- No se dejará la contraseña en **blanco**.
- No se usará como contraseña el **código de usuario/a, ni cadenas obtenidas a partir de variaciones** de los caracteres que formen parte del mismo. Ni contraseñas utilizadas con anterioridad.
- No se utilizará como contraseña información sencilla **directamente relacionada con la persona** *(nombres, apellidos, números de teléfono, domicilio, nombres de familiares, etc.)*
- No se guardará la contraseña **por escrito**.
- No se proporcionará la contraseña **a otro usuario**.
- Cada usuario/a deberá cambiar periódicamente su contraseña, sustituyéndola por otra distinta a las utilizadas anteriormente.
- No se podrá mantener la misma contraseña durante más de **seis meses**.

Qué HACER si… conozco una situación de ACOSO LABORAL / MOBBING:

El **centro de trabajo** es un entorno donde puede producirse y reproducirse **acoso** ya sea *sexual, por razón de sexo, por orientación sexual, etc.* Además, debido al uso de las **tecnologías** para trabajar es posible que el acoso se de en **medios digitales (Ciberacoso)**.

En primer lugar, la persona trabajadora conocedora o víctima de esta situación debe **comunicarlo** a la persona encargada o al departamento que gestione el protocolo de prevención de acoso / canal interno de denuncias, etc.

En segundo lugar, debe conocer el **CANAL PRIORITARIO** que la AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS PERSONALES ha creado para dar respuesta este tipo de reclamaciones.

Indica la AEPD que si tienes conocimiento de la existencia de fotografías, vídeos o audios de contenido sexual o violento que circulan por Internet sin el consentimiento de las personas afectadas, solicita su retirada en el Canal prioritario.

En tercer lugar, somos conocedores que un **dato personal** es también una imagen, un vídeo, una grabación de voz, un dato de contacto, de salud, etc. Por ello, el tratamiento debe ser lícito *(Necesitamos el consentimiento expreso de la persona afectada para tu tratamiento y difusión).*

Según Art.4 RGPD: ***toda información sobre una persona física identificada o identificable; se considerará persona física identificable toda persona cuya identidad pueda determinarse, directa o indirectamente, en particular mediante un identificador, como por ejemplo un nombre, un número de identificación, datos de localización, un identificador en línea o uno o varios elementos propios de la identidad física, fisiológica, genética, psíquica, económica, cultural o social de dicha persona"***

Garantía de los Derechos Digitales:

En esta nueva ley se establecen nuevos derechos para los trabajadores entre los que están:

- Desconexión digital del empleado fuera de su horario laboral.
- Derecho al olvido cuando los datos sean:
    - Inadecuados.
    - No pertinentes.
    - Excesivos.
- Protección de la intimidad con protocolos negociados entre empresa y personal para uso de dispositivos digitales.
- Refuerzo de la privacidad de las personas trabajadoras ante sistemas audiovisuales o de geolocalización en el trabajo.
- No podrá ser menoscabada la intimidad de las personas trabajadoras bajo el argumento de la seguridad.

Acceso por la empresa a contenidos del personal

La nueva LOPDGDD permite a la empresa **acceder a los contenidos de los dispositivos digitales facilitados a sus trabajadores/as** solo con el fin de controlar el cumplimiento de las obligaciones laborales. Y, de garantizar la integridad de dichos dispositivos.

Para ello deben cumplirse unos requisitos:

- La empresa elaborará un **protocolo de uso de los dispositivos digitales** y se lo comunicará directamente a cada persona trabajadora.
- Las normas de uso de dispositivos digitales deberán regular con precisión el alcance de la privacidad de la persona.
- Para que la empresa pueda acceder al contenido de dispositivos digitales de sus trabajadores/as es necesario que el **protocolo de uso de esos dispositivos indique de forma precisa los usos admitidos y medidas previstas** para garantizar la intimidad de cada persona.

Confidencialidad y secreto:

- El personal que intervenga en cualquier fase del tratamiento de los datos de carácter personal está obligado al **secreto profesional** respecto de los mismos y al deber de guardarlos, obligaciones que subsistirán aun después de finalizar sus relaciones con la empresa.
- La **seguridad** se ordena a garantizar la **confidencialidad, integridad y disponibilidad** de los datos. La utilización de recursos y aplicaciones informáticas comporta la adopción de ciertas precauciones *(disponer de contraseñas, copias de seguridad, diferentes usuarios, etc.).*

Normativa de referencia aplicable:

- Ley Orgánica de Protección de Datos Personales y Garantía de los Derechos Digitales 3/2018 de 5 de diciembre.
- Reglamento 2016/679 relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos.
- La Ley 34/2002, de 11 de julio de Servicios de la Sociedad de Información y Comercio Electrónico.
- Ley Orgánica 3/2007, de 22 de marzo, para la igualdad efectiva de mujeres y hombres.