FUNCIONES Y OBLIGACIONES DE LOS USUARIOS QUE TIENEN ACCESO A LOS FICHEROS QUE CONTIENEN DATOS DE CARÁCTER PERSONAL Y A LOS SISTEMAS DE INFORMACIÓN DE ATREVIA.

En cumplimiento de la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales, los usuarios con acceso a los datos de carácter personal incorporados en los ficheros de **ATREVIA** están obligados a cumplir con las funciones y obligaciones relacionadas a continuación, y según las autorizaciones indicadas. El incumplimiento de estas funciones, obligaciones y autorizaciones implicará aquellas responsabilidades que se hayan estipulado por Dirección.

1. Tratar los datos de carácter personal de conformidad con lo establecido en la legislación vigente y en el presente documento.

2. Garantizar la seguridad de los datos de carácter personal.

3. Acceder a los datos de carácter personal y a los sistemas de información únicamente cuando lo precisen para el desarrollo de sus funciones y conforme a las autorizaciones concedidas por **ATREVIA.**

4. Mantener el secreto profesional respecto de los datos de carácter personal a los que accedan, así como su custodia. Esta obligación perdurará tras finalizar sus relaciones con **ATREVIA.**

5. No comunicar los datos personales a los que tienen acceso a terceros. La información obtenida como consecuencia de la relación laboral con **ATREVIA** es estrictamente confidencial.

6. Identificar el tipo de información de cualquier soporte que contenga datos de carácter personal, inventariarlo y almacenarlo de acuerdo con el procediendo establecido al efecto.

7. Disponer de la autorización de **ATREVIA** para la salida de soportes y documentos que contengan datos de carácter personal, incluidos los comprendidos y/o anejos a un correo electrónico, fuera de los locales bajo el control de **ATREVIA** y adoptar las medidas que eviten la sustracción, pérdida o acceso indebido a la información durante su transporte. Los soportes deberán enviarse con sobre cerrado y acuse de recibo para garantizar que el destinatario autorizado lo ha recibido.

8. Comunicar al responsable de seguridad cualquier anomalía o incidencia que se observe durante el tratamiento de datos de carácter personal.

9. Comunicar a **ATREVIA** cualquier solicitud de acceso, rectificación, supresión, oposición y limitación del tratamiento de datos de carácter personal.

10. Evitar que los datos personales a los que tengan acceso sean visibles a través de sus puestos de trabajo por personas no autorizadas; por ello, cuando abandonen este puesto de trabajo, deberán apagar el equipo o bloquearlo. Si se trata de datos personales en soporte documental, se deberán guardar los documentos que contengan datos personales en un lugar que no pueda ser visible para terceros no autorizados.

11. En el uso de impresoras, fax y fotocopiadoras se debe retirar la documentación relativa a los datos personales inmediatamente después de su impresión, envío o copia evitando el acceso por parte de personas no autorizadas.

12. En el caso de desechar un documento que contenga datos de carácter personal se procederá a su destrucción, utilizando la destructora de papel habilitada al efecto. En el caso de desechar un soporte se procederá a su destrucción o borrado, adoptando medidas para evitar el acceso a la información contenida en el mismo o su recuperación o se comunicará al responsable de seguridad para que adopte las precauciones necesarias.

13. En el caso de enviar correos electrónicos a más de un destinatario a la vez, deberá emplearse la opción "copia oculta" (CCO).

14. No modificar la configuración de las aplicaciones ni del sistema operativo, salvo autorización expresa del responsable de seguridad.

15. Mantener la confidencialidad de la contraseña. En el caso de que ésta sea conocida por persona no autorizada, deberá proceder a su cambio y registrarlo como incidencia.

16. Para el uso de dispositivos portátiles en los que se almacenen datos personales o en los tratamientos realizados fuera de los locales de **ATREVIA** debe haber obtenido de éste la autorización correspondiente, y garantizar el nivel de seguridad correspondiente al tipo de fichero tratado. En caso contrario, queda prohibido dicho tratamiento.

17. En la creación de ficheros temporales, para la realización de una tarea concreta, será obligatorio su borrado o destrucción una vez haya finalizado ésta.

18. Cualquier entrada de soportes que contengan datos de carácter personal de nivel medio y alto, deberá ser registrada en el documento habilitado al efecto. El responsable de seguridad tendrá a disposición de los usuarios un modelo de registro de entrada de soportes.

19. Las copias de seguridad de los ficheros únicamente las podrán realizar las personas autorizadas por el responsable de seguridad.

20. Antes de la implantación o modificación de los sistemas de información, no se podrán hacer pruebas con datos reales, salvo que se asegure el nivel de seguridad correspondiente al tratamiento realizado, se verifique la realización previa de una copia de seguridad y se anote su realización en el documento de seguridad.

21. Solamente si está autorizado puede acceder a las dependencias donde se encuentran instalados los equipos físicos que den soporte a los sistemas de información y a los armarios y archivadores que contengan documentos con datos especialmente protegidos.

22. En el caso de distribuir soportes informáticos, por ejemplo CD's, que contengan datos de carácter personal especialmente protegidos (salud, religión, vida sexual, ideología, afiliación sindical o creencias), éstos se tendrán que cifrar, por ejemplo utilizando

programas compresores con contraseña. Para solventar cualquier duda al respecto, el responsable de seguridad facilitará este tipo de programas y explicará su funcionamiento.

23. Se prohíbe la utilización de fax para la transmisión de datos personales especialmente protegidos (salud, religión, vida sexual, ideología, afiliación sindical o creencias).

24. El correo postal que contenga datos de carácter personal especialmente protegidos (salud, religión, vida sexual, ideología, afiliación sindical, creencias), se enviará con sobre cerrado, correo certificado y acuse de recibo.

25. Para transmitir datos personales especialmente protegidos (salud, religión, vida sexual, ideología, afiliación sindical, creencias) a través de Internet, previamente se deberán cifrar utilizando, por ejemplo, programas compresores protegidos con contraseña.

26. Deberá seguir los criterios de archivo de los soportes y documentos establecidos por **ATREVIA** que garantizan la correcta conservación de los mismos, localización y consulta de la información y posibilitan el ejercicio de los derechos de acceso, rectificación, supresión, limitación del tratamiento y oposición.

27. Mientras la documentación con datos de carácter personal no se encuentre archivada en los dispositivos de almacenamiento por estar en proceso de revisión o tramitación, ya sea previo o posterior a su archivo, la persona que se encuentre al cargo de la misma deberá custodiarla e impedir en todo momento que pueda tener acceso a ella personas no autorizadas.

28. Al prestar los servicios a clientes en los locales de éstos, se debe cumplir con las medidas de seguridad que el cliente le traslade y que se incluyan en su documento de seguridad.

29. Cuando al prestar los servicios a los clientes se tenga que acceder a los datos vía remota, se debe cumplir con las medidas de seguridad que el cliente le traslade y que se incluyan en su documento de seguridad.

30. Para recoger datos personales, siempre y cuando **ATREVIA** haya autorizado proceder a dicha recogida de datos personales, se deberá cumplir con lo que se dispone a continuación:

1) Recogida de datos personales:

a) Los datos personales sólo se podrán recoger para su tratamiento cuando éstos sean adecuados, pertinentes y no excesivos en relación con el ámbito y las finalidades determinadas, explícitas y legítimas para las que se hayan obtenido.

b) Los datos personales serán exactos y puestos al día de forma que respondan con veracidad a la situación actual del afectado.

c) Los datos personales serán cancelados cuando hayan dejado de ser necesarios o pertinentes para la finalidad para la cual hubieran sido recabados o registrados. No obstante, podrán conservarse durante el tiempo en que pueda exigirse algún tipo de

responsabilidad derivada de una relación u obligación jurídica o de la ejecución de un contrato o de la aplicación de medidas precontractuales solicitadas por el interesado.

Una vez cumplido el período al que se refieren los párrafos anteriores, los datos sólo podrán ser conservados previa disposición de los mismos, sin perjuicio de la obligación de bloqueo prevista en el Reglamento General de Protección de Datos y en la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales.

2) Derecho de información del afectado.

a) Las personas a las cuales se les soliciten datos personales deberán ser previamente informadas de:

- Del tratamiento de datos de carácter personal, de la finalidad de la recogida de éstos y de los destinatarios de la información.
- Del carácter obligatorio o facultativo de su respuesta a las preguntas planteadas.
- De las consecuencias de la obtención de los datos o de la negativa a suministrarlos.
- De la posibilidad de ejercitar los derechos acceso, rectificación, supresión, limitación del tratamiento y oposición
- De la identidad del Responsable del tratamiento de Datos.

b) Cuando se soliciten cuestionarios u otros impresos para la recogida de datos, figurarán en los mismos, en forma claramente legible, las advertencias a que se refiere el apartado anterior.

3) Consentimiento del afectado.

a) Los datos de carácter personal únicamente podrán ser objeto de tratamiento o cesión si el interesado hubiera prestado previamente su consentimiento.

b) No será preciso el consentimiento del interesado cuando el responsable del tratamiento de datos tenga un interés legítimo, siempre que no se vulneren los derechos y libertades fundamentales del interesado. Tampoco serán necesario el consentimiento del interesado cuando se recabe por el responsable del tratamiento con ocasión de la celebración de un contrato o precontrato o de la existencia de una relación negocial, laboral o administrativa y sea necesario para su mantenimiento o cumplimiento. No obstante, a estas personas se les deberá informar del Derecho de información del afectado.

c) Los datos personales que revelen la ideología, afiliación sindical, religión y creencias, únicamente podrán ser tratados con el consentimiento expreso y por escrito del titular

de los datos. Así mismo, los datos que hagan referencia al origen racial, salud y vida sexual sólo podrán ser recabados, tratados y cedidos cuando, por razones de interés general, así lo disponga una ley o el afectado consienta expresamente.

d) Los datos de carácter personal objeto del tratamiento únicamente podrán ser comunicados a un tercero para el cumplimiento de fines directamente relacionados con las funciones legítimas del cedente y del cesionario con el previo consentimiento por escrito del interesado.

En este caso, se deberán utilizar los documentos de legitimación que se hayan habilitado al efecto.

Autorizaciones:

El usuario no está autorizado para sacar de la empresa soportes y documentos con datos personales automatizados y no automatizados.

El usuario no está autorizado para ejecutar procedimientos de recuperación de datos, almacenar datos automatizados y no automatizados en dispositivos portátiles o tratar datos fuera de los locales de la empresa.

El usuario no está autorizado a acceder a lugares de instalación de equipos físicos que dan soporte a los sistemas de información.

El incumplimiento de estas funciones y obligaciones y los daños y perjuicios ocasionados a **ATREVIA** y a los afectados supondrán una infracción que dará lugar a la imposición de las sanciones disciplinarias correspondientes por parte de **ATREVIA.**

No obstante, la empresa se reserva contra el trabajador las acciones civiles y/o penales que procedan por los daños y perjuicios que se ocasionen.