INSTRUCCIÓNES QUE DEBE CONOCER Y CUMPLIR TODO EL PERSONAL DE 1DOCUMENTACION TIPO, S.L. ,CON ACCESO A DATOS DE CARACTER PERSONAL.

Con el fin de dar cumplimento al Artículo 32.4 del Reglamento General de Protección de Datos UE 2016/679, en adelante RGPD, 1DOCUMENTACION TIPO, S.L., informa mediante este documento a todo el personal de la empresa, de las funciones y obligaciones que deben conocer y cumplir en relación al tratamiento de ficheros que contengan datos personales, y cuyo responsable es 1DOCUMENTACION TIPO, S.L.

1. Funciones y obligaciones con carácter general

Todo el personal interno o externo de la empresa que acceda a los datos de carácter personal, está obligado a conocer y observar las medidas, normas, procedimientos, reglas y estándares que afecten a las funciones que desarrolla.

Constituye una obligación del personal notificar al responsable de los ficheros o actividades de tratamiento o al responsable de seguridad las incidencias de seguridad de las que tengan conocimiento respecto a los recursos protegidos.

Todas las personas deberán guardar el debido secreto y confidencialidad de los datos personales que conozcan en el desarrollo de su trabajo.

El responsable de los ficheros o actividades de tratamiento es 1DOCUMENTACION TIPO, S.L. en la persona de , en calidad de representante legal de la empresa.

2. Funciones y obligaciones que afectan a todo el personal.

2.1 General

Tratar los datos de carácter personal de conformidad con lo establecido por 1DOCUMENTACION TIPO, S.L., accediendo al fichero únicamente cuando sea necesario para el desarrollo de sus funciones.

Mantener el secreto profesional respecto de los datos de carácter personal que se encuentran en el fichero y custodiarlos. Esta obligación perdurará después de finalizar las relaciones con el responsable de los ficheros o actividades de tratamiento.

Conocer la normativa interna en materia de seguridad, y especialmente la referente a protección de datos de carácter personal.

Cumplir lo dispuesto en la normativa interna vigente en cada momento.

Conocer las consecuencias que se pudieran derivar y las responsabilidades en que pudiera incurrir en caso de incumplimiento, que podrían derivar en sanciones.

Comunicar al responsable de los ficheros o actividades de tratamiento, en el mismo día, cualquier solicitud de ejercicio por parte de los afectados de los derechos de acceso, rectificación, supresión, limitación de tratamiento, portabilidad y oposición, así como cualquier incidencia que conozca sobre la confidencialidad e integridad de los datos.

2.1 Puestos de trabajo

El usuario autorizado será el responsable de su puesto de trabajo, garantizando que la información que disponga o muestre su equipo no podrá ser accesible o visible por personas no autorizadas.

Procurará que la disposición de pantallas e impresoras u otros dispositivos de su puesto de trabajo se ubiquen de forma que garanticen la confidencialidad y no sea accesible o visible su contenido por personas no autorizadas.

Al abandonar su puesto de trabajo, aun temporalmente, deberá dejarlo en un estado que impida el acceso o la visualización de los datos protegidos, mediante un protector de pantalla o la salida del sistema y apagado del equipo. La reanudación del trabajo implicará la desactivación de la pantalla protectora o el encendido del equipo con la introducción del nombre de usuario y contraseña correspondiente en cada caso.

No deberá dejar en la impresora documentos impresos en la bandeja de salida que contengan datos protegidos. Si la impresora es compartida con otros usuarios no autorizados para acceder a los datos de Fichero, el responsable de cada puesto de trabajo deberá retirar los documentos conforme vayan siendo impresos.

La configuración de los puestos de trabajo desde los que se tiene acceso al fichero sólo podrá ser cambiada con la autorización del Responsable de los Ficheros o Actividades de Tratamiento, el Responsable de Seguridad o el Administrador del Sistema designado.

2.3 Salvaguarda y protección de las contraseñas personales

Todo usuario es responsable de mantener la confidencialidad de su contraseña. Si la contraseña es conocida por otra persona, el usuario, deberá registrarlo como incidencia y notificarlo al Responsable de los Ficheros o Actividades de Tratamiento o al Responsable de Seguridad, para proceder a su cambio.

2.4 Gestión de incidencias

El usuario que tenga conocimiento de una incidencia deberá de ponerlo en conocimiento del Responsable de los Ficheros o Actividades de Tratamiento o al Responsable de Seguridad y registrarla siguiendo el procedimiento establecido para el registro de incidencias.

El conocimiento y la no notificación de una incidencia por parte de un usuario será considerado como una falta contra la seguridad del Fichero por parte de ese usuario.

Todos los miembros de la organización deben conocer la obligación del responsable de notificar las violaciones de seguridad de los datos a la autoridad de control, por lo que han de ser conocedores de su obligación de comunicar a la mayor brevedad al responsable de cualquier incidencia sobre los datos que llegue a su conocimiento y que pueda poner en peligro los derechos y libertades de los ciudadanos en este ámbito.

2.5 Gestión de soportes para encargados de las copias de seguridad.

Los soportes informáticos que contengan datos del Fichero, han de estar claramente identificados con una etiqueta externa que indique el fichero, tipo de datos y fecha de creación.

Los soportes que sean reutilizables, y que hayan contenido copias de datos del fichero, deberán ser borrados físicamente antes de su reutilización, de forma que los datos que contenían no sean recuperables.

Los soportes que contengan datos del fichero deberán ser almacenados en lugares a los que no tengan acceso personas que no estén autorizadas.

La salida de equipos o soportes fuera de las instalaciones requiere la autorización del Responsable de los Ficheros o Actividades de Tratamiento o del Responsable de Seguridad.

Seguir los procedimientos establecidos de gestión y distribución de soportes y observar las autorizaciones precisas en cada caso.

2.6 Correo electrónico

No utilizar el correo electrónico u otros medios de comunicación interna o con el exterior para transmitir mensajes que contengan o lleven adjuntos datos de carácter personal que por sus características, volumen o destinatarios puedan poner en peligro la confidencialidad o la integridad de los datos.

Atenerse a los procedimientos establecidos y observar las autorizaciones precisas.

2.7 Transferencias de ficheros

No realizar transferencias de ficheros con datos de carácter personal entre sistemas o descargas en equipos salvo en aquellos casos expresamente autorizados, y protegiendo después los contenidos para evitar la difusión o copias no autorizadas.

2.8 Tratamiento fuera de los locales del fichero

Proteger la confidencialidad e integridad de los datos personales de la entidad que excepcionalmente tuvieran que almacenarse o usarse fuera del lugar de trabajo: en casa del cliente, en el propio domicilio o en otras instalaciones alternativas tanto en sistemas fijos como en portátiles.

Siempre que sea posible, se encriptarán los ficheros que contengan datos personales o se protegerán mediante contraseña segura.

3. Funciones y obligaciones del administrador del sistema, personal informático, y responsables de seguridad.

Siempre será posible conocer el personal que intervino con posterioridad a la intervención, dejando constancia de ello, e identificando al personal técnico.

3.1. Entorno del sistema operativo y de comunicaciones

Cuidar de que ningún usuario no autorizado disponga de herramienta o programa que le permita el acceso al fichero.

Guardar en lugar protegido las copias de respaldo y recuperación del fichero, (copias de seguridad), evitando el acceso a las mismas de persona no autorizada.
Asegurarse de que el personal no autorizado no pueda tener acceso a los datos protegidos.

Impedir el acceso remoto de personas no autorizadas al equipo donde esté ubicado el fichero, especialmente si se encuentra integrado en una red de comunicaciones.

3.2 Sistema Informático o aplicaciones de acceso al Fichero

Si la aplicación informática que permite el acceso al Fichero no cuenta con un control de acceso, deberá ser el sistema operativo, donde se ejecuta esa aplicación, el que impida el acceso no autorizado, mediante el control de código de usuario y contraseña.

3.3 Salvaguarda y protección de las contraseñas personales

Las contraseñas se asignarán y se cambiarán mediante el mecanismo y periodicidad que determine 1DOCUMENTACION TIPO, S.L.,. Este mecanismo de asignación y distribución de las contraseñas deberá garantizar la confidencialidad de las mismas, y será responsabilidad del administrador del sistema.

El archivo donde se almacenen las contraseñas deberá estar protegido y bajo la responsabilidad del administrador del sistema.

3.4 Procedimientos de respaldo y recuperación

Obtener periódicamente una copia de seguridad del fichero, que garantice su reconstrucción en el estado en que se encontraba al tiempo de producirse la pérdida o destrucción.

Realizar la copia de respaldo, al menos semanalmente, salvo que en dicho período no se hubiera producido ninguna actualización de los datos.

Comprobar y actualizar el procedimiento, informático o manual, que partiendo de la última copia de respaldo y del registro de las operaciones realizadas desde el momento de la copia, reconstruya los datos del Fichero al estado en que se encontraban en el momento del fallo.

Se entrega copia al abajo firmante, dándose por informado, y obligándose a cumplir todas las funciones y obligaciones dispuestas en este documento. (firmar todas las hojas)

En Almoradí a fecha _____

D/Dña. _____ DNI: _____

Firma: