MEMORIA DE CUMPLIMIENTO DE PROTECCIÓN DE DATOS SEGÚN LA LEY ORGÁNICA DE PROTECCIÓN DE DATOS DE CARÁCTER PERSONAL 15/1999 DE 13 DE DICIEMBRE

DATO DE CARATER PERSONAL:

"Cualquier información numérica, alfabética, gráfica, fotográfica, acústica o de cualquier otro tipo concerniente a personas físicas identificadas o identificables".
(art. 3 a L.O.P.D)
Como se desprende de esta definición, cuando la ley habla de datos de carácter personal no sólo hace referencia al nombre y apellido de la persona, sino que, de manera muy amplia, incluye cualquier tipo de información, (DNI, fotografías, vídeos, voz, huellas…. Siempre que haga referencia a una persona física identificada (se sabe a quién pertenece el dato) o identificable. (No se sabe a quién pertenece el dato pero se podría averiguar fácilmente)

FICHERO:

Físicamente un fichero es un soporte en el que se encuentran almacenados o registrados los datos de carácter personal, pero jurídicamente el término fichero está definido de una manera mucho más amplia y abstracta incluyendo a "Todo conjunto organizado de datos de carácter personal, que permita el acceso a los datos con arreglos a criterios determinados, cualquiera que fuera la forma o modalidad de su creación, almacenamiento, organización y acceso". (art. 3 b L.O.P.D)
En el caso de Candelita, todos los ficheros están automatizados y dados de alta en la **Agencia Española de Protección de datos.**

COPIA DE SEGURIDAD:

Una copia de seguridad, en tecnologías de la información e informática es una copia de los datos originales que se realiza con el fin de disponer de un medio para recuperarlos en caso de su pérdida. Las copias de seguridad son útiles ante distintos eventos y usos: recuperar los sistemas informáticos y los datos de una catástrofe informática, natural o ataque; restaurar una pequeña cantidad de archivos que pueden haberse eliminado accidentalmente, corrompido, infectado por un virus informático u otras causas; guardar información histórica de forma más económica que los discos duros y además permitiendo el traslado a ubicaciones distintas de la de los datos originales; etc…

El proceso de copia de seguridad se complementa con otro conocido como restauración de los datos que es la acción de leer y grabar en la ubicación original u otra alternativa los datos requeridos.

DERECHO DE ACCESO, RECTIFICACIÓN, CANCELACIÓN, OPOSICIÓN Y MODIFICACIÓN DE LOS DATOS. (ARCO):

Los denominados derechos ARCO son el conjunto de acciones a través de las cuales una persona física puede ejercer el control sobre sus datos personales. Estos derechos se regulan en el Título III de la Ley Orgánica de Protección de Datos (LOPD) y en el Título III de su Reglamento de Desarrollo, y son cuatro: Acceso, Rectificación, Cancelación y Oposición.

Se trata de derechos cuyo ejercicio es personalísimo, es decir, que sólo pueden ser ejercidos por el titular de los datos, por su representante legal o por un representante acreditado, de forma que el responsable del fichero puede denegar estos derechos cuando la solicitud sea formulada por persona distinta del afectado y no se acredite que actúa en su representación.

El ejercicio de estos derechos se debe llevar a cabo mediante medios sencillos y gratuitos puestos a disposición por el responsable del fichero y que están sujetos a plazo, por lo que resulta necesario establecer procedimientos para su satisfacción. Si la persona reclamante cree que sus derechos no han sido atendidos en forma y plazo según la LOPD y su reglamento, puede acudir a la tutela de la Agencia Española de Protección de Datos (AEPD).

Derecho de Acceso

El derecho de acceso es el derecho del afectado a obtener información sobre si sus propios datos de carácter personal están siendo objeto de tratamiento, la finalidad del tratamiento que, en su caso, se esté realizando, así como la información disponible sobre el origen de dichos datos y las comunicaciones realizadas o previstas de los mismos.

Derecho de Rectificación

Derecho del afectado a que se modifiquen los datos que resulten ser inexactos o incompletos.

Derecho de Cancelación

Derecho del afectado a que se supriman los datos que resulten ser inadecuados o excesivos

Derecho de Oposición

Derecho del afectado a que no se lleve a cabo el tratamiento de sus datos de carácter personal o se cese en el mismo en los supuestos en que no sea necesario su consentimiento para el tratamiento, que se tratase de ficheros de prospección comercial o que tengan la finalidad de adoptar decisiones referidas al interesado y basadas únicamente en el tratamiento automatizado de sus datos.

Candelita, de acuerdo con lo establecido en la **L**ey **O**rgánica de **P**rotección de **D**atos de Carácter Personal 15/1999 de 13 de Diciembre, tiene puestas en marcha las siguientes acciones relacionadas con el personal y los usuarios/as:

OBLIGACIONES QUE AFECTAN A TODO EL PERSONAL

1. Puestos de trabajo

- ✓ Los puestos de trabajo estarán bajo la responsabilidad de algún usuario autorizado que garantizará que la información que muestran no pueda ser visible por personas no autorizadas.
- ✓ Esto implica que tanto las pantallas como las impresoras u otro tipo de dispositivos conectados al puesto de trabajo deberán estar físicamente ubicados en lugares que garanticen esa confidencialidad.
- ✓ Cuando el responsable de un puesto de trabajo lo abandone, bien temporalmente o bien al finalizar su turno de trabajo, deberá dejarlo en un estado que impida la visualización de los datos protegidos. Esto podrá realizarse a través de un protector de pantalla que impida la visualización de los datos. La reanudación del trabajo implicará la desactivación de la pantalla protectora con la introducción de la contraseña correspondiente.
- ✓ En el caso de las impresoras deberá asegurarse de que no quedan documentos impresos en la bandeja de salida que contengan datos protegidos. Si las impresoras son compartidas con otros usuarios no autorizados para acceder a los datos de Fichero, los responsables de cada puesto deberán retirar los documentos conforme vayan siendo impresos.
- ✓ Queda expresamente prohibida la conexión a redes o sistemas exteriores de los puestos de trabajo desde los que se realiza el acceso al fichero. La revocación de esta prohibición será autorizada por el responsable del fichero, quedando constancia de esta modificación en el Libro de incidencias.
- ✓ Los puestos de trabajo desde los que se tiene acceso al fichero tendrán una configuración fija en sus aplicaciones, sistemas operativos que solo podrá ser cambiada bajo al autorización del responsable de seguridad o por administrador

2. Salvaguarda y protección de las contraseñas personales

- ✓ Cada usuario será responsable de la confidencialidad de su contraseña y, en caso de que la misma sea conocida fortuita o fraudulentamente por personas no autorizadas, deberá registrarlo como incidencia y proceder a su cambio.

3. Gestión de incidencias

- ✓ Cualquier usuario que tenga conocimiento de una incidencia es responsable de la comunicación de la misma al administrador del sistema, o en su caso del registro de la misma en el sistema de registro de incidencias del Fichero.
- ✓ 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.

4. Gestión de soportes

- ✓ Los soportes que contengan datos del Fichero, bien como consecuencia de operaciones intermedias propias de la aplicación que los trata, o bien como consecuencia de procesos periódicos de respaldo o cualquier otra operación esporádica, deberán estar claramente identificados con una etiqueta externa que indique de qué fichero se trata, que tipo de datos contiene, proceso que los ha originado y fecha de creación.
- ✓ Aquellos medios 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 lo que no tengan acceso personas no autorizadas para el uso del Fichero
- ✓ Cuando la salida de datos del Fichero se realice por medio de correo electrónico, los envíos se realizarán, siempre y únicamente, desde una dirección de correo controlada por el administrador de seguridad, dejando constancia de estos envíos en el directorio histórico de esa dirección de correo o en algún otro sistema de registro de salidas que permita conocer en

cualquier momento los envíos realizados, a quien iban dirigidos y la información enviada.

- ✓ Cuando los datos del Fichero deban ser enviados fuera del recinto físicamente protegido donde se encuentra ubicado el Fichero, bien sea mediante un soporte físico de grabación de datos o bien sea mediante correo electrónico, deberán ser encriptados de forma que solo puedan ser leídos e interpretados por el destinatario.
- ✓ Se deberán registrar mediante correo electrónico o transferencia de datos por red, de forma que se pueda siempre identificar su origen, tipo de datos, formato, fecha y hora del envío y destinatario de los mismos.

OBLIGACIONES DEL RESPONSABLE DEL FICHERO

Implantar las medidas de seguridad establecidas en este documento.

El responsable del Fichero deberá garantizar la difusión de este Documento entre todo el personal que vaya a utilizar.

Deberá mantenerlo actualizado siempre que se produzcan cambios relevantes en el sistema de información o en la organización del mismo, según los artículos 8 y 9 de la Normativa de Seguridad.

Deberá adecuar en todo momento el contenido del mismo a las disposiciones vigentes en materia de seguridad de datos.

Deberá designar uno o varios responsables de seguridad.

Entorno de Sistema Operativo y de Comunicaciones

+ El responsable del Fichero aprobará o designará al administrador que se responsabilizará del sistema operativo

+ En el caso más simple, como es que el Fichero se encuentre ubicado en un ordenador personal y accedido mediante una aplicación local monopuesto, el administrador del sistema operativo podrá ser el mismo usuario que accede usualmente al Fichero.

Sistema Informático o aplicaciones de acceso al Fichero

+ El responsable del fichero se encargará de que los sistemas informáticos de acceso al Fichero tengan su acceso restringido mediante un código de usuario y una contraseña.

+ Asimismo cuidará que todos los usuarios autorizados para acceder al Fichero, tengan un código de usuario que será único, y que estará asociado a la contraseña correspondiente, que sólo será conocida por el propio usuario.

Salvaguarda y protección de las contraseñas personales

+ Sólo las personas autorizadas, podrán tener acceso a los datos del Fichero.

Gestión de soportes

+ La salida de soportes informáticos que contengan datos del Fichero fuera de los locales donde está ubicado el Fichero deberá ser expresamente autorizada por el responsable del Fichero.

Entrada y salida de datos por red

+ Todas las entradas y salidas de datos del Fichero que se efectúen mediante correo electrónico se realizarán desde una única cuenta o dirección de correo controlada por un usuario especialmente autorizado por el responsable del Fichero. Igualmente si se realiza la entrada o salida de datos mediante sistemas de transferencia de ficheros por red, únicamente un usuario o administrador estará autorizado para realizar esas operaciones.

Procedimientos de respaldo y recuperación

+ El responsable del Fichero se encargará de verificar la definición y correcta aplicación de las copias de respaldo y recuperación de los datos.
+ Será necesaria la autorización por escrito del responsable del fichero para la ejecución de los procedimientos de recuperación de los datos, y deberá dejarse constancia en el registro de incidencias de las manipulaciones que hayan debido realizarse para dichas recuperaciones, incluyendo la persona que realizó el proceso, los datos restaurados y los datos que hayan debido ser grabados manualmente en el proceso de recuperación.

Controles periódicos de verificación del cumplimiento

+ El responsable del fichero junto con el responsable de seguridad, analizarán con periodicidad al menos trimestral las incidencias registradas en el libro correspondiente, para independientemente de las medidas particulares que se hayan adoptado en el momento que se produjeron, poner las medidas correctoras que limiten esas incidencias en el futuro.
+ Al menos cada dos años, se realizará una auditoría, externa o interna que dictamine el correcto cumplimiento y la adecuación de las medidas del presente documento de seguridad o las exigencias del Reglamento de seguridad, identificando las deficiencias y proponiendo las medidas correctoras necesarias. Los informes de auditoría serán analizados por el responsable de seguridad, quien propondrá al responsable del Fichero las medidas correctoras correspondientes.

ATENCIÓN A LOS USUARIOS/AS,

Todas aquellas personas que facilitan sus datos a nuestro personal, es informado de sus derechos de acceso, rectificación, cancelación y oposición de sus datos. Todas aquellas personas inscritas en algún proyecto, programa o servicio, firman su consentimiento.

A continuación, adjuntamos modelo de registro de datos.

ESTIMADO/A USUARIO/A:

De acuerdo con lo establecido en la **L**ey **O**rgánica de **P**rotección de **D**atos de Carácter Personal 15/1999 de 13 de Diciembre, le informamos de la incorporación de sus datos personales a varios ficheros automatizados y en soporte papel, los cuales son titularidad de "CANDELITA" autorizando al tratamiento de los mismos para la prestación de los servicios ----------.

Estos ficheros se encuentran debidamente inscritos en la Agencia de Protección de Datos, y sus datos son tratados con el grado de protección requerido según el Real Decreto 1720/2007, de 21 de diciembre de 2007.

El/la usuario/a podrá ejercer en cualquier momento su derecho de acceso, rectificación, cancelación y oposición de sus datos, y revocar la autorización concedida, notificándolo al responsable del fichero, "CANDELITA", bien en este establecimiento, o mediante carta dirigida a: Calle Montera, 9,1º dcha. 28013 – Madrid.

Nombre de Usuario/a:

Número de DNI/ Pasaporte:

Fecha:

Firma: