PROTOCOLO DE SEGURIDAD – TRATAMIENTO DE DATOS PERSONALES

NECESIDAD DE ANALIZAR LOS RIESGOS

El Reglamento (UE) 2016/679, General de Protección de Datos (RGPD) exige la adopción de **medidas técnicas y organizativas apropiadas** con el fin de garantizar la protección de los derechos y libertades de las personas físicas con respecto al tratamiento de datos personales.

A fin de poder demostrar el cumplimiento del RGPD, el responsable del tratamiento debe adoptar **políticas internas** y aplicar medidas de seguridad que cumplan los principios de protección de datos desde el diseño y por defecto.

Además, se deben **evaluar los riesgos inherentes al tratamiento y aplicar medidas para mitigarlos**. Estas medidas deben garantizar un nivel de seguridad adecuado, incluida la confidencialidad, teniendo en cuenta el estado de la técnica y el coste de su aplicación con respecto a los riesgos y la naturaleza de los datos personales que deban protegerse.

Al evaluar el riesgo en relación con la seguridad de los datos, se deben tener en cuenta los riesgos que se derivan del tratamiento de los datos personales, como la destrucción, pérdida o alteración accidental o ilícita de datos personales transmitidos, conservados o tratados de otra forma, o la comunicación o acceso no autorizados a dichos datos, susceptibles en particular de ocasionar daños y perjuicios físicos, materiales o inmateriales.

Así, el presente documento contiene los **principios** que STOCKCROWD FANRAISING, S.L. debe aplicar a los tratamientos realizados, desde su recogida (ya sea del propio interesado o de un tercero), hasta su eliminación, cuando ya no son necesarios para los fines para los que fueron recogidos.

De la misma manera, se recogen las **medidas técnicas y organizativas mínimas** que STOCKCROWD FANRAISING, S.L. deberá aplicar al tratamiento de los datos que, de acuerdo al previo análisis de riesgos, son necesarias para garantizar la seguridad de los datos personales tratados.

MEDIDAS DE SEGURIDAD APLICADAS EN EL TRATAMIENTO AUTOMATIZADO

Funciones y obligaciones del personal

Las funciones y obligaciones de cada uno de los usuarios o perfiles de usuarios con acceso a los datos de carácter personal y a los sistemas de información estarán claramente definidas y documentadas.

STOCKCROWD FANRAISING, S.L. adoptará las medidas necesarias para que el personal conozca de una forma comprensible las normas de seguridad que afecten al desarrollo de sus funciones así como las consecuencias en que pudiera incurrir en caso de incumplimiento.

- **Control de acceso**

Los usuarios deberán tener acceso únicamente a aquellos recursos que precisen para el desarrollo de sus funciones. STOCKCROWD FANRAISING, S.L. se encargará de que exista una relación actualizada de usuarios y perfiles de usuarios, y los accesos autorizados para cada uno de ellos. Esto, podrá conseguirse teniendo actualizada la información en la plataforma de MICROLAB, en relación a los perfiles del personal.

STOCKCROWD FANRAISING, S.L. establecerá, además, mecanismos para evitar que un usuario pueda acceder a recursos con derechos distintos de los autorizados. Exclusivamente el personal autorizado para ello podrá conceder, alterar o anular el acceso autorizado sobre los recursos.
En caso de que exista personal ajeno a la organización de STOCKCROWD FANRAISING, S.L., que tenga acceso a los recursos, deberá estar sometido a las mismas condiciones y obligaciones de seguridad que el personal propio.

- **Gestión de soportes y documentos**

Los soportes y documentos que contengan datos de carácter personal deberán permitir identificar el tipo de información que contienen, ser inventariados y solo deberán ser accesibles por el personal autorizado para ello, aunque se exceptúan estas obligaciones cuando las características físicas del soporte imposibiliten su cumplimiento.

La salida de soportes y documentos que contengan datos de carácter personal fuera de los locales bajo el control de STOCKCROWD FANRAISING, S.L., deberá ser autorizada por este. En el traslado de la documentación se adoptarán las medidas dirigidas a evitar la sustracción, pérdida o acceso indebido a la información durante su transporte.

Por su parte, siempre que vaya a desecharse cualquier documento o soporte que contenga datos de carácter personal deberá procederse a su destrucción o borrado, mediante la adopción de medidas dirigidas a evitar el acceso a la información contenida en el mismo o su recuperación posterior.

La identificación de los soportes que contengan datos de carácter personal que la organización considerase especialmente sensibles se podrá realizar utilizando sistemas de etiquetado comprensibles y con significado que permitan a los usuarios con acceso autorizado a los citados soportes y documentos identificar su contenido, y que dificulten la identificación para el resto de personas, por ejemplo, a través de códigos.

- **Identificación y autenticación (CONTRASEÑAS)**

STOCKCROWD FANRAISING, S.L. deberá adoptar las medidas que garanticen la correcta identificación y autenticación de los usuarios, estableciendo un mecanismo que permita la identificación de forma inequívoca y personalizada de todo aquel usuario que intente acceder al sistema de información y la verificación de que está autorizado.

Cuando el mecanismo de autenticación se base en la existencia de contraseñas existirá un procedimiento de asignación, distribución y almacenamiento que garantice su confidencialidad e integridad. La periodicidad con la que tienen que ser cambiadas las contraseñas en ningún caso será superior a un año y, mientras estén vigentes, se almacenarán de forma ininteligible.

Para acceder a los sistemas informáticos se debe requerir nombre de usuario y contraseña.

Se deben evitar tipos de contraseña que contenga nombre de personas, o nombre de usuario, fecha de nacimiento, DNI, etc., se recomienda configurar las Directivas del Sistema en Windows para especificar el nivel de complejidad de las contraseñas.

Para que una contraseña sea segura debe contener al menos ocho caracteres y estar compuesta por letras números y símbolos.

- **Copias de respaldo y recuperación**

Deberán establecerse procedimientos de actuación para la realización como mínimo semanal de copias de respaldo, salvo que en dicho período no se hubiera producido ninguna actualización de los datos.

Asimismo, se establecerán procedimientos para la recuperación de los datos que garanticen en todo momento su reconstrucción en el estado en que se encontraban al tiempo de producirse la pérdida o destrucción.

STOCKCROWD FANRAISING, S.L. se encargará de verificar cada seis meses la correcta definición, funcionamiento y aplicación de los procedimientos de realización de copias de respaldo y de recuperación de los datos.

Deberá conservarse, además, una copia de respaldo de los datos y de los procedimientos de recuperación de los mismos en un lugar diferente de aquel en que se encuentren los equipos informáticos que los tratan, que deberá cumplir en todo caso las medidas de seguridad exigidas en este documento, o utilizando elementos que garanticen la integridad y recuperación de la información, de forma que sea posible su recuperación.

Las pruebas anteriores a la implantación o modificación de los sistemas de información que traten ficheros con datos de carácter personal no se realizarán con datos reales, salvo que se asegure el nivel de seguridad correspondiente al tratamiento realizado. Si está previsto realizar pruebas con datos reales, previamente deberá haberse realizado una copia de seguridad.

- **Bloqueo de la pantalla**

Se debe activar el bloqueo de pantalla cuando no hay actividad. En la configuración de Windows / Panel de control debe activarse el bloqueo de pantalla con intervalo de tiempo para salvaguardar la posible información de datos personales y evitar que sea visualizada por personas no autorizadas.

La desactivación del bloqueo de pantalla debe requerir contraseña.

- **Control de protección frente a las amenazas externas**

Se debe disponer de un antivirus actualizado correctamente. En la medida de lo posible se deben evitar las nuevas variantes de virus y amenazas que van apareciendo a diario.

Además, se deben realizar revisiones periódicas de los sistemas de seguridad. Es conveniente comprobar que todos los parámetros estén actuando correctamente, revisar los registros de seguridad, antivirus, cortafuegos, etc.

- **Control del software instalado**

Todas las licencias de software de gestión instaladas en los equipos deben ser originales y existir un inventario.

Se deben instalar licencias originales para poder mantener los sistemas operativos actualizados a fin de beneficiarse de las nuevas versiones que en muchos casos incorporan utilidades y parches de seguridad y, en su caso, poder activar las actualizaciones de seguridad que Windows.

Además, es altamente recomendable realizar actualizaciones de seguridad (en el caso de Windows, a través de Windows Update), para descargar las últimas actualizaciones de seguridad de forma totalmente automática.

- **Medidas de seguridad a aplicar en tablets y smartphones**

Debido a la practicidad de estos dispositivos, se han popularizado tanto en el ámbito profesional como en el doméstico, siendo utilizadas para todo tipo de operaciones de tratamiento. Por esta razón, las medidas de seguridad a aplicar en estos dispositivos deberán ser igual de estrictas que las aplicadas en el sistema informático de la organización:
- Instalación de aplicaciones de seguridad: existen en el mercado gran variedad de este tipo de aplicaciones, destinadas a proteger el dispositivo de virus y otros ataques. Además, muchas de ellas permiten el bloqueo y borrado remoto en caso de robo o pérdida.
- Bloqueo firme: se deberá proteger el dispositivo con un patrón o contraseña (es más segura la segunda opción) que sea única y robusta. Es necesario, además, cambiarla con la misma periocidad que la contraseña de los equipos informáticos.
- Uso de aplicaciones: se debe evitar la instalación de aplicaciones que innecesarias para la labor profesional. Además, únicamnente se deberán instalar aplicaciones oficiales y legítimas, utilizando únicamente tiendas seguras, como Google Play y App Store.
- Evitar el WiFi público: se debe evitar por todas las vías la conexión a redes WiFi públicas, pues este tipo de redes comprometen gravemente la integridad de la información contenida en el dispositivo, pudiendo ser accesible a terceros con conocimientos informáticos.

- **Violaciones de la seguridad**

El RGPD define la violación de la seguridad de los datos personales como “toda violación de la seguridad que ocasione la destrucción, pérdida o alteración accidental o ilícita de datos personales transmitidos, conservados o tratados de otra

forma, o la comunicación o acceso no autorizados a dichos datos".

STOCKCROWD FANRAISING, S.L. documentará cualquier violación de la seguridad de los datos personales, incluidos los hechos relacionados con ella, sus efectos y las medidas correctivas adoptadas.

Tan pronto como STOCKCROWD FANRAISING, S.L. tenga conocimiento de que se ha producido una violación de la seguridad de los datos personales de su responsabilidad, debe, sin dilación indebida y, de ser posible, a más tardar 72 horas después de que haya tenido constancia de ella, notificar la violación de la seguridad de los datos personales a la Agencia Española de Protección de Datos, a menos que pueda demostrar la improbabilidad de que la violación de la seguridad de los datos personales entrañe un RIESGO para los derechos y las libertades de las personas físicas. Es decir, se deberá notificar la violación de seguridad a la Agencia Española de Protección de Datos cuando constituya un RIESGO para los derechos y las libertades de los interesados.

Esta notificación deberá contener, como mínimo:

1. Una descripción de la naturaleza de la violación de la seguridad de los datos personales, inclusive, cuando sea posible, las categorías y el número aproximado de interesados afectados, y las categorías y el número aproximado de registros de datos personales afectados.
2. Comunicar el nombre y los datos de contacto del delegado de protección de datos o de otro punto de contacto en el que pueda obtenerse más información.
3. Describir las posibles consecuencias de la violación de la seguridad de los datos personales.
4. Describir las medidas adoptadas o propuestas para poner remedio a la violación de la seguridad de los datos personales, incluyendo las medidas adoptadas para mitigar los posibles efectos negativos.

Si dicha notificación no es posible en el plazo de 72 horas, debe acompañarse de una indicación de los motivos de la dilación, pudiendo facilitarse información por fases sin más dilación indebida.

Cuando sea probable que la violación de la seguridad de los datos personales entrañe un ALTO RIESGO para los derechos y libertades de las personas físicas, STOCKCROWD FANRAISING, S.L. la comunicará al interesado sin dilación indebida. La comunicación al interesado describirá en un lenguaje claro y sencillo la naturaleza de la violación de la seguridad de los datos personales, el nombre y los datos de contacto del delegado de protección de datos o el punto de contacto, describir las consecuencias de la violación, así como las medidas adoptadas para poner remedio a esta o mitigar sus efectos.

Sin embargo, esta comunicación al interesado no será necesaria si:
a. STOCKCROWD FANRAISING, S.L. ha adoptado medidas de protección técnicas y organizativas apropiadas, en particular aquellas que hagan ininteligibles los datos personales para cualquier persona que no esté autorizada a acceder a ellos, como el cifrado.
b. STOCKCROWD FANRAISING, S.L. ha tomado medidas ulteriores que garanticen que ya no exista la probabilidad de que se concretice el alto riesgo para los derechos y libertades del interesado.
c. Supone un esfuerzo desproporcionado. En este caso, se optará en su lugar por una comunicación pública o una medida semejante por la que se informe de manera igualmente efectiva a los interesados.

- **Proceso de verificación, evaluación y valoración de la seguridad**

STOCKCROWD FANRAISING, S.L. deberá implantar un proceso de verificación, evaluación y valoración regulares de la eficacia de las medidas técnicas y organizativas para garantizar la seguridad del tratamiento.

Con carácter extraordinario deberá realizarse dicha verificación siempre que se realicen modificaciones sustanciales en el sistema de información que puedan repercutir en el cumplimiento de las medidas de seguridad implantadas con el objeto de verificar la adaptación, adecuación y eficacia de las mismas.

MEDIDAS DE SEGURIDAD APLICADAS EN EL TRATAMIENTO NO AUTOMATIZADO (PAPEL)

Además de aplicar las medidas anteriormente descritas, que lógicamente puedan trasladarse al tratamiento de datos en

soporte no automatizado o en papel, se deberán aplicar las siguientes medidas, a fin de garantizar la seguridad de este tipo de tratamientos.

- **Criterios de archivo**

El archivo de los soportes o documentos se realizará de acuerdo con los criterios previstos en su respectiva legislación. Estos criterios deberán garantizar la correcta conservación de los documentos, la localización y consulta de la información y posibilitar el ejercicio de los derechos de oposición al tratamiento, acceso, rectificación y cancelación:

En aquellos casos en los que no exista norma aplicable, STOCKCROWD FANRAISING, S.L. deberá establecer los criterios y procedimientos de actuación que deban seguirse para el archivo.

- **Dispositivos de almacenamiento**

Los dispositivos de almacenamiento de los documentos que contengan datos de carácter personal deberán disponer de mecanismos que obstaculicen su apertura. Cuando las características físicas de aquéllos no permitan adoptar esta medida, STOCKCROWD FANRAISING, S.L. adoptará medidas que impidan el acceso de personas no autorizadas.

- **Custodia de los soportes**

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 ser accedida por persona no autorizada.

- **Destrucción de la información**

Cuando sea necesario deshacerse de la documentación que contenga datos personales, esta deberá ser destruida de tal manera que se impida la posible recuperación de la información. Para ello, es muy recomendable recurrir a una máquina destructora de papel.