REGISTRO DE ACTIVIDADES DE TRATAMIENTO

MARTINEZ CENTRO DE GESTIÓN, S.L.

Documento actualizado el 06 de octubre de 2019

ÍNDICE

1. ÁMBITO DE APLICACIÓN

Para poder realizar la adaptación se ha aplicado la nueva Ley Orgánica de Protección de Datos y garantía de los derechos digitales de fecha 3/2018, de 5 de Diciembre y el nuevo Reglamento General de Protección de Datos (RGPD) que entró en vigor en mayo de 2016 y es de aplicación a partir de mayo de 2018.

El nuevo Reglamento General de Protección de Datos (RGPD) entró en vigor en mayo de 2016 y es de aplicación a partir de mayo de 2018. El RGPD es una norma directamente aplicable, que no requiere de normas internas de trasposición ni tampoco, en la mayoría de los casos, de normas de desarrollo o aplicación. Por ello, los responsables deben ante todo asumir que la norma de referencia es el RGPD y no las normas nacionales, como venía sucediendo hasta ahora con la Directiva 95/46. No obstante, la ley que sustituirá a la actual Ley Orgánica de Protección de Datos (LOPD) sí podrá incluir algunas precisiones o desarrollos en materias en las que el RGPD lo permite.

El RGPD contiene muchos conceptos, principios y mecanismos similares a los establecidos por la Directiva 95/46 y por las normas nacionales que la aplican. Por ello, las organizaciones que en la actualidad cumplen adecuadamente con la LOPD española tienen una buena base de partida para evolucionar hacia una correcta aplicación del nuevo Reglamento.

Sin embargo, el RGPD modifica algunos aspectos del régimen actual y contiene nuevas obligaciones que deben ser analizadas y aplicadas por cada organización teniendo en cuenta sus propias circunstancias.

Dos elementos de carácter general constituyen la mayor innovación del RGPD para los responsables y se proyectan sobre todas las obligaciones de las organizaciones:

El principio de responsabilidad proactiva

El RGPD describe este principio como la necesidad de que el responsable del tratamiento aplique medidas técnicas y organizativas apropiadas a fin de garantizar y poder demostrar que el tratamiento es conforme con el Reglamento.

En términos prácticos, este principio requiere que las organizaciones analicen qué datos tratan, con qué finalidades lo hacen y qué tipo de operaciones de tratamiento llevan a cabo. A partir de este conocimiento deben determinar de forma explícita la forma en que aplicarán las medidas que el RGPD prevé, asegurándose de que esas medidas son las adecuadas para cumplir con el mismo y de que pueden demostrarlo ante los interesados y ante las autoridades de supervisión.

En síntesis, este principio exige una actitud consciente, diligente y proactiva por parte de las organizaciones frente a todos los tratamientos de datos personales que lleven a cabo.

El enfoque de riesgo

El RGPD señala que las medidas dirigidas a garantizar su cumplimiento deben tener en cuenta la naturaleza, el ámbito, el contexto y los fines del tratamiento así como el riesgo para los derechos y libertades de las personas.

De acuerdo con este enfoque, algunas de las medidas que el RGPD establece se aplicarán sólo cuando exista un alto riesgo para los derechos y libertades, mientras que otras deberán modularse en función del nivel y tipo de riesgo que los tratamientos presenten.

La aplicación de las medidas previstas por el RGPD debe adaptarse, por tanto, a las características de las organizaciones.

El RGPD mantiene el principio recogido en la Directiva 95/46 de que todo tratamiento de datos necesita apoyarse en una base que lo legitime. También recoge las mismas bases jurídicas que contenía la Directiva y que reproduce la LOPD:

- Consentimiento.
- Relación contractual.
- Intereses vitales del interesado o de otras personas.
- Obligación legal para el responsable.
- Interés público o ejercicio de poderes públicos.
- Intereses legítimos

2. BASES DE LEGITIMACIÓN PARA EL TRATAMIENTO DE DATOS

El consentimiento debe ser "inequívoco". El consentimiento inequívoco es aquel que se ha prestado mediante una manifestación del interesado o mediante una clara acción afirmativa.

A diferencia del Reglamento de Desarrollo de la LOPD, no se admiten formas de consentimiento tácito o por omisión, ya que se basan en la inacción.

- Se contemplan situaciones en las que el consentimiento, además de inequívoco, ha de ser explícito:

• Tratamiento de datos sensibles.

• Adopción de decisiones automatizadas.

• Transferencias internacionales.

- El consentimiento puede ser inequívoco y otorgarse de forma implícita cuando se deduzca de una acción del interesado.

- Los tratamientos iniciados con anterioridad al inicio de la aplicación del RGPD sobre la base del consentimiento seguirán siendo legítimos siempre que ese consentimiento se hubiera prestado del modo en que prevé el propio RGPD, es decir, mediante una manifestación o acción afirmativa.

- No seguir obteniendo consentimientos por omisión y revisar esos tratamientos.

La adaptación puede llevarse a cabo:

• Obteniendo un consentimiento de los interesados acorde con las disposiciones del RGPD.

• Valorando si los tratamientos afectados pueden apoyarse en otra base legal. Como puede ser, entre otras, el interés legítimo del responsable o del cesionario de los datos que prevalezca sobre los derechos del interesado (los interesados deben ser informados y podrán ejercitar los derechos que, como el de oposición, sean específicamente aplicables a la nueva base legal elegida).

El presente documento será de aplicación a los ficheros que contienen datos de carácter personal que se hallan bajo la responsabilidad de MARTINEZ CENTRO DE GESTIÓN, S.L., incluyendo los sistemas de información, soportes y equipos empleados para el tratamiento de datos de carácter personal, que deban ser protegidos de acuerdo a lo dispuesto en normativa vigente, las personas que intervienen en el tratamiento y los locales en los que se ubican.

Su objeto es la salvaguarda de la autodeterminación informativa de las personas físicas ante el uso ilegítimo de sus datos de carácter personal.

Ofrece a su titular las facultades necesarias para ejercer un verdadero control sobre la información personal, un poder de disposición sobre los datos personales.

El Tribunal Europeo de Derechos Humanos ha tutelado el derecho fundamental a la protección de datos con fundamento en la protección de la vida privada del artículo 8 del Convenio europeo de Derechos Humanos y del Convenio 108 de 1981.

El documento contempla las obligaciones asumidas por parte del responsable de tratamiento.

En concreto, los ficheros sujetos a las medidas de seguridad establecidas en este documento, con indicación del nivel de seguridad correspondiente, son los siguientes:

- Fichero de Clientes y Proveedores
- Fichero de Usuarios web
- Fichero de Fiscal-Contable
- Fichero de Nóminas, Personal y Recursos Humanos

LEGITIMACIÓN DE LOS TRATAMIENTOS

MARTINEZ CENTRO DE GESTIÓN, S.L., realiza los siguientes tratamientos:

- tratamiento de datos personales de empleados, no recabando el consentimiento expreso o explícito de los interesados dado que el tratamiento está autorizado por ley.
- tratamiento de datos personales de interesados cuyos datos son objeto de gestión de recursos humanos, recabando el consentimiento expreso o explícito de los interesados para todos los tratamientos que se realizan.
- tratamiento de datos personales de usuarios web, para lo cual se recaba el consentimiento libre, específico, inequívoco, explícito e informado de los interesados.
- tratamiento de datos personales de proveedores, no recabando el consentimiento expreso o explícito de los interesados dado que el tratamiento responde a una relación negocial, entre las partes, o bien está autorizado por ley.
- tratamiento de datos personales de Clientes, recabando el consentimiento expreso o explícito de los interesados.

En el Anexo 3 se describen detalladamente cada uno de los ficheros o tratamientos, junto con los aspectos que les afecten de manera particular.

3. MEDIDAS, NORMAS Y REGLAS DESTINADAS A GARANTIZAR LOS NIVELES DE SEGURIDAD EXIGIDOS EN ESTE DOCUMENTO.

Las medidas de seguridad definidas en el presente documento son de aplicación a todas las áreas, divisiones, departamentos, servicios y dependencias de MARTINEZ CENTRO DE GESTIÓN, S.L., y tanto a sus directivos como a otros empleados y también a los profesionales y empresas con las que haya sido suscrito un contrato de prestación de servicios que conlleve el tratamiento de datos de carácter personal. Además, las medidas de seguridad van encaminadas a proteger de manera general el sistema de información en sentido amplio, los ficheros, aplicaciones y herramientas de actualización y consulta, recursos del sistema operativo, redes de telecomunicaciones, soportes y equipos informáticos gestionados.

Respecto a las Medidas de seguridad aplicables a los **tratamientos no automatizados**, hay que explicar que los locales donde se ubican los ficheros no automatizados están protegidos de forma que se garantiza la disponibilidad y confidencialidad de los datos. Los locales cuentan con los medios de seguridad que evitan accesos no autorizados que puedan comprometer la confidencialidad de los datos. Existe una habitación cerrada bajo llave, en la cual encontramos los ficheros en armarios cerrados bajo llave.

Cuando se extraiga documentación de los archivos físicos, la persona autorizada para ello será responsable de garantizar su confidencialidad y de retornarla una vez cumplida las finalidades administrativas o asistenciales que motivaron la salida de la documentación del archivo.

Se delimitarán las zonas de acceso al público en general y las zonas de acceso restringido al personal autorizado al acceso a los datos de carácter personal, dentro de estas zonas estarán ubicados físicamente los ficheros no automatizados.

El equipo directivo informará a todos los empleados y al personal, que intervenga en la prestación de servicios, de la obligatoriedad de guardar el máximo secreto y confidencialidad sobre toda la información de carácter personal que contengan los ficheros no automatizados y que afecte a la esfera íntima de los usuarios. Además, informarán sobre las medidas de seguridad que se deben adoptar con el objeto de proteger los ficheros no automatizados.

Por último, se aplicarán a los ficheros no automatizados, todas aquellas medidas de seguridad recogidas en el Reglamento de Medidas de Seguridad de ficheros automatizados que puedan ser aplicadas de forma análoga.

Respecto a las Medidas de seguridad aplicables a los **tratamientos automatizados**, se utilizará para los equipos informáticos:

- Software antivirus y de seguridad específicos, así como la configuración del software del navegador con las opciones de seguridad más restrictivas. Se actualizarán periódicamente todos ellos, a ser posible con comprobaciones diarias, con objeto de disponer de las últimas versiones.

- Se utilizarán solo sistemas operativos modernos, que cuenten actualmente con actualizaciones de seguridad del fabricante. Se actualizará periódicamente el sistema operativo, a ser posible de manera automatizada.

- El intercambio y la entrega de datos de carácter personal en sitios web, deberán efectuarse exclusivamente en los sitios web que dispongan de protocolos seguros y de política de privacidad.

- El intercambio y la entrega de datos de carácter personal o el almacenamiento de copias de seguridad, por ejemplo unidades de disco externas, DVD o memorias USB, deberá efectuarse exclusivamente en medios que cuenten con medidas de seguridad como la encriptación de su contenido.

- Los equipos estarán protegidos mediante contraseña, impidiendo con ello los inicios de sesión y accesos no autorizados.

- Deberá asegurarse la confianza o acreditación de los sitios web antes de proceder a la descarga de archivos de los mismos.

Para el correo electrónico: Para acceder a la cuenta de correo electrónico, además del código de usuario se utilizará una contraseña. Contraseña que no sea una palabra de los idiomas más utilizados ni una secuencia de números; se recomienda una combinación aleatoria de letras mayúsculas y minúsculas, números y símbolos, a ser posible totalmente aleatorios, y se cambiará de forma periódica. La contraseña contará con un mínimo de ocho caracteres y deberá cambiarse al menos cada tres meses.

- ✓ No se utilizará la opción de “Guardar contraseña” que, en ocasiones, se ofrece para evitar reintroducirla en cada conexión.

- ✓ En los envíos de correo a una lista de distribución se incluirán los destinatarios del mensaje en el campo “Con copia Oculta (CCO)” de tal forma que ninguno de los receptores podrá acceder a la dirección de correo electrónico del resto de los destinatarios.

- ✓ Se configurará el programa de correo en el nivel de seguridad máximo.

- ✓ No se abrirán los mensajes que ofrezcan dudas en cuanto a su origen o posible contenido sin asegurarse, al menos, que han sido analizados por su software antivirus.

- ✓ Los filtros de correo no deseado estarán activados.
- ✓ No se utilizará para uso personal la dirección de correo electrónico proporcionada en el marco de la relación laboral.
- ✓ En el caso de envío por Internet de documentos privados, es necesario utilizar sistemas que permitan el cifrado de su contenido.
- ✓ Se delimitarán las zonas de acceso al público en general y las zonas de acceso restringido al personal autorizado al acceso a los datos de carácter personal, dentro de estas zonas estarán ubicados físicamente los ficheros no automatizados.

El equipo directivo informará a todos los empleados y al personal, que intervenga en la prestación de servicios, de la obligatoriedad de guardar el máximo secreto y confidencialidad sobre toda la información de carácter personal que contengan los ficheros no automatizados y que afecte a la esfera íntima. Además, informarán sobre las medidas de seguridad que se deben adoptar con el objeto de proteger los ficheros no automatizados.

Por último, se aplicarán a los ficheros no automatizados, todas aquellas medidas de seguridad aplicables a los ficheros automatizados que puedan ser aplicadas de forma análoga.

3.1. Medidas de Seguridad

El artículo 5.1.f del Reglamento General de Protección de Datos (RGPD) determina la necesidad de establecer garantías de seguridad adecuadas contra el tratamiento no autorizado o ilícito, contra la pérdida de los datos personales, la destrucción o el daño accidental. Esto implica el establecimiento de medidas técnicas y organizativas encaminadas a asegurar la integridad y confidencialidad de los datos personales y la posibilidad (artículo 5.2) de demostrar que estas medidas se han llevado a la práctica (responsabilidad proactiva).

A tenor del tipo de tratamiento que ha puesto de manifiesto cuando ha cumplimentado el respectivo formulario, las medidas mínimas de seguridad que debería tener en cuenta son las siguientes:

INFORMACIÓN QUE DEBERÁ SER CONOCIDA POR TODO EL PERSONAL CON ACCESO A DATOS PERSONALES:

Todo el personal con acceso a los datos personales deberá tener conocimiento de sus obligaciones con relación a los tratamientos de datos personales y serán informados acerca de dichas obligaciones. La información mínima que será conocida por todo el personal será la siguiente:

- DEBER DE CONFIDENCIALIDAD Y SECRETO

  - Se deberá evitar el acceso de personas no autorizadas a los datos personales, a tal fin se evitará: dejar los datos personales expuestos a terceros (pantallas electrónicas desatendidas, documentos en papel en zonas de acceso público, soportes con datos personales, etc.), esta consideración incluye las pantallas que se utilicen para la visualización de imágenes del sistema de videovigilancia. Cuando se ausente del puesto de trabajo, se procederá al bloqueo de la pantalla o al cierre de la sesión.

  - Los documentos en papel y soportes electrónicos se almacenarán en lugar seguro (armarios o estancias de acceso restringido) durante las 24 horas del día.

  - No se desecharán documentos o soportes electrónicos (CD, DVD, pen drives, discos duros, etc.) con datos personales sin garantizar su destrucción.

  - No se comunicarán datos personales o cualquier información personal a terceros, se prestará atención especial en no divulgar datos personales protegidos durante las consultas telefónicas, correos electrónicos, etc.

  - El deber de secreto y confidencialidad persiste incluso cuando finalice la relación laboral del trabajador con la empresa.

DERECHOS DE LOS TITULARES DE LOS DATOS

Se informará a todos los trabajadores acerca del procedimiento para atender los derechos de los interesados, definiendo de forma clara los mecanismos por los que pueden ejercerse los derechos (medios electrónicos, dirección postal, etc.) teniendo en cuenta lo siguiente:

- Previa presentación de su documento nacional de identidad o pasaporte, los titulares de los datos personales (interesados) podrán ejercer sus derechos de acceso, rectificación, supresión, oposición y portabilidad. El responsable del tratamiento deberá dar respuesta a los interesados sin dilación indebida.

- Para el derecho 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 los destinatarios 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 derecho de rectificación se procederá a modificar los datos de los interesados que fueran inexactos o incompletos atendiendo a los fines del tratamiento.

- Para el derecho 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 derecho 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.

El responsable del tratamiento deberá informar a todas las personas con acceso a los datos personales acerca de los términos de cumplimiento para atender los derechos de los interesados, la forma y el procedimiento en que se atenderán dichos derechos.

VIOLACIONES DE SEGURIDAD DE DATOS DE CARÁCTER PERSONAL

- Cuando se produzcan violaciones de seguridad DE DATOS DE CARÁCTER PERSONAL, como por ejemplo, el robo o acceso indebido a los datos personales se notificará a la Agencia Española de Protección de Datos en término de 72 horas acerca de dichas violaciones de seguridad, incluyendo toda la información necesaria para el esclarecimiento de los hechos que hubieran dado lugar al acceso indebido a los datos personales. La notificación se realizará por medios electrónicos a través de la sede electrónica de la Agencia Española de Protección de Datos en la dirección: https://sedeagpd.gob.es

MEDIDAS TÉCNICAS

- Cuando el mismo ordenador o dispositivo se utilice para el tratamiento de datos personales y fines de uso personal se recomienda disponer de varios perfiles o usuarios distintos para cada una de las finalidades. Deben mantenerse separados los usos profesional y personal del ordenador.

- Se recomienda disponer de perfiles con derechos de administración para la instalación y configuración del sistema y usuarios sin privilegios o derechos de administración para el acceso a los datos personales. Esta medida evitará que en caso de ataque de ciberseguridad puedan obtenerse privilegios de acceso o modificar el sistema operativo.

- Se garantizará la existencia de contraseñas para el acceso a los datos personales almacenados en sistemas electrónicos. La contraseña tendrá al menos 8 caracteres, mezcla de números y letras.

- Cuando a los datos personales accedan distintas personas, para cada persona con acceso a los datos personales, se dispondrá de un usuario y contraseña específicos (identificación inequívoca).

- Se debe garantizar la confidencialidad de las contraseñas, evitando que queden expuestas a terceros. Para la gestión de las contraseñas puede consultar la guía de privacidad y seguridad en internet de la Agencia Española de Protección de Datos y el Instituto Nacional de Ciberseguridad. En ningún caso se compartirán las contraseñas ni se dejarán anotadas en lugar común y el acceso de personas distintas del usuario.

DEBER DE SALVAGUARDA

A continuación se exponen las medidas técnicas mínimas para garantizar la salvaguarda de los datos personales:

- ACTUALIZACIÓN DE ORDENADORES Y DISPOSITIVOS: Los dispositivos y ordenadores utilizados para el almacenamiento y el tratamiento de los datos personales deberán mantenerse actualizados en la media posible.

- MALWARE: En los ordenadores y dispositivos donde se realice el tratamiento automatizado de los datos personales se dispondrá de un sistema de antivirus que garantice en la medida posible el robo y destrucción de la información y datos personales. El sistema de antivirus deberá ser actualizado de forma periódica.

- CORTAFUEGOS O FIREWALL: Para evitar accesos remotos indebidos a los datos personales se velará para garantizar la existencia de un firewall activado en aquellos ordenadores y dispositivos en los que se realice el almacenamiento y/o tratamiento de datos personales.

- CIFRADO DE DATOS: Cuando se precise realizar la extracción de datos personales fuera del recinto donde se realiza su tratamiento, ya sea por medios físicos o por medios electrónicos, se deberá valorar la posibilidad de utilizar un método de encriptación para garantizar la confidencialidad de los datos personales en caso de acceso indebido a la información.

- COPIA DE SEGURIDAD: Periódicamente se realizará una copia de seguridad en un segundo soporte distinto del que se utiliza para el trabajo diario. La copia se almacenará en lugar seguro, distinto de aquél en que esté ubicado el ordenador con los ficheros originales, con el fin de permitir la recuperación de los datos personales en caso de pérdida de la información.

Las medidas de seguridad serán revisadas de forma periódica, la revisión podrá realizarse por mecanismos automáticos (software o programas informáticos) o de forma manual. Considere que cualquier incidente de seguridad informática que le haya ocurrido a cualquier conocido le puede ocurrir a usted, y prevéngase contra el mismo.

3.2. Control de acceso

El personal sólo accederá a aquellos datos y recursos que precise para el desarrollo de sus funciones. Cada perfil tiene asociados determinados privilegios de acceso y/u operación sobre los datos del fichero. El Responsable de Tratamiento define los diferentes perfiles de acceso a los datos del fichero, así como los mecanismos para obtener la relación actualizada de usuarios con acceso a los sistemas. Para facilitar las labores de gestión de la explotación del sistema, el original de esta información puede encontrarse almacenado en formato electrónico en el propio sistema de ficheros.

Los accesos a los recursos estarán protegidos, además de por controles físicos, por controles preventivos y de detección de tipo lógico, es decir, no tangibles, acordes con lo que se deba proteger, y según el estado de la tecnología.

Los usuarios tendrán acceso únicamente a aquellos recursos que precisen para el desarrollo de sus funciones.

El Responsable del Fichero se encargará de que exista una relación actualizada de usuarios y perfiles de usuarios y los perfiles autorizados para cada uno de ellos. El Responsable del Fichero establecerá mecanismos para evitar que un usuario pueda acceder a recursos con derechos distinto de los autorizados.

En el caso que exista personal ajeno al responsable del fichero que tenga acceso a los recursos estará sometido a las mismas condiciones y obligaciones de seguridad que el personal propio.

Los usuarios serán responsables de todas las actividades y accesos que se realicen con su código de usuario, por lo que está expresamente prohibido ceder o comunicar la contraseña o mecanismo de autenticación a otros y deben custodiarse debidamente, y la clave no teclearse bajo la mirada de otros.

En el caso de necesitar compartir datos o correo se usarán otros mecanismos como carpetas o directorios públicos o sistemas de trabajo en grupo.

Los administradores de seguridad y de redes deberán establecer sistemas suficientemente flexibles y eficaces como para poder otorgar acceso a cualquier usuario autorizado en un tiempo razonable, para evitar tener que utilizar un código de usuario ajeno en caso de ausencia o sustitución.

Cuando un usuario varía de función, o bien deja de ser trabajador, su usuario será eliminado o al menos bloqueado mientras tanto, y se deberá asignar a alguien la custodia y revisión de los ficheros, programas y documentación que hubiera usado hasta entonces, al menos de forma provisional.

Cualquier incidencia relacionada con los accesos debe ser comunicada al Responsable de Tratamiento.

Exclusivamente MARTINEZ CENTRO DE GESTIÓN, S.L., está autorizado para conceder, alterar o anular el acceso autorizado sobre los datos y los recursos, conforme a los criterios establecidos por el responsable del fichero

En el Anexo 1.4, se incluye la relación de usuarios actualizada con acceso autorizado a cada sistema de la información.

Controles de acceso Físico y Lógico

Los usuarios tendrán acceso únicamente a aquellos recursos que precisen para el desarrollo de sus funciones.

El responsable del fichero se encargará de que exista una relación actualizada de usuarios y perfiles de usuarios, y los accesos autorizados para cada uno de ellos.

El responsable del fichero establecerá mecanismos para evitar que un usuario pueda acceder a recursos con derechos distintos de los autorizados.

Exclusivamente el personal autorizado para ello en este documento podrá conceder, alterar o anular el acceso autorizado sobre los recursos, conforme a los criterios establecidos por el responsable del fichero.

En caso de que exista personal ajeno al responsable del fichero que tenga acceso a los recursos deberá estar sometido a las mismas condiciones y obligaciones de seguridad que el personal propio.

3.3. Medidas y normas relativas a la identificación y autenticación del personal autorizado a acceder a los datos personales.

Gestión de soportes

Soportes informáticos son todos aquellos medios de grabación y recuperación de datos que se utilizan para realizar copias o pasos intermedios en los procesos de la aplicación que gestiona el fichero.

Los soportes que contengan datos de carácter personal deberán permitir identificar el tipo de información que contiene, ser inventariados y almacenarse en un lugar con acceso restringido al personal autorizado para ello en el documento de seguridad.

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 del responsable del fichero o tratamiento deberá ser autorizada por el responsable del fichero o encontrarse debidamente autorizada en este documento.

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.

Deberá establecerse un sistema de registro de entrada de soportes informáticos que permita directa o indirectamente, conocer el tipo de soporte, la fecha y hora, el emisor, el número de soportes, el tipo de información que contienen, la forma de envío y la persona responsable de la recepción que deberá estar debidamente autorizada.

Cuando un soporte vaya a ser desechado o reutilizado se adoptarán las medidas necesarias para impedir cualquier recuperación posterior de la información almacenada en él, previamente a que se proceda a su baja en el inventario.

La distribución de los soportes que contengan datos de carácter personal se realizará cifrando dichos datos o bien utilizando otro mecanismo que garantice que dicha información no sea inteligible ni manipulada durante su transporte.

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.

En el Anexo 4.1 podemos observar un modelo de gestión de soportes.

3.4. Copias de seguridad

La seguridad de los datos personales del Fichero no sólo supone la confidencialidad de los mismos sino que también conlleva la integridad y la disponibilidad de esos datos.

Para garantizar estos dos aspectos fundamentales de la seguridad es necesario que existan unos procesos de respaldo y de recuperación que, en caso de fallo del sistema informático, permitan recuperar y en su caso reconstruir los datos del Fichero. 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.

Únicamente, en el caso de que la pérdida o destrucción afectase a ficheros o tratamientos parcialmente automatizados, y siempre que la existencia de documentación permita alcanzar el objetivo al que se refiere el párrafo anterior, se deberá proceder a grabar manualmente los datos quedando constancia motivada de este hecho en este documento.

El responsable del fichero 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.

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 y se anote su realización en el documento de seguridad.

Si está previsto realizar pruebas con datos reales, previamente deberá haberse realizado una copia de seguridad.

En el Anexo 3.A.3 y 3.B.3 se detallan los procedimientos de copia y recuperación de respaldo para cada fichero.

3.5. Acceso a datos a través de redes de telecomunicaciones.

Con objeto de dar cumplimiento al RGPD, se implantarán las medidas tendentes a garantizar la confidencialidad e integridad de los contenidos y minimizar los ataques activos o pasivos, en definitiva, garantizar un nivel de seguridad equivalente al correspondiente a los accesos en modo local. Toda conexión al sistema de información, mediante accesos a través de redes de comunicaciones sean o no públicas requerirá siempre el mismo nivel de seguridad exigido para el acceso a modo local o red de área local, medidas como:

- Sistemas de autenticación fiables en los terminales: mediante contraseña u otros.
- Protecciones físicas de acceso a terminales, servidores, cableado y equipos de comunicaciones.
- Bloqueo de terminales inactivos pasado un tiempo, según posibilidades de acceso y ubicación de los mismos.
- Selección de equipos y elementos de red fiables.

Se podrán realizar evaluaciones de riesgos periódicas, sin descartar el análisis de puntos débiles con herramientas.

3.6. Régimen de trabajo fuera de los locales de la ubicación del fichero.

La ejecución de tratamiento de datos de carácter personal fuera de los locales de la ubicación del fichero deberá ser autorizada expresamente por el responsable del fichero y, en todo caso, deberá garantizarse el nivel de seguridad correspondiente al tipo de fichero tratado.

3.7. Ficheros temporales.

Aquellos ficheros temporales o copias de documentos que se hubiesen creado exclusivamente para la realización de trabajos temporales o auxiliares deberán cumplir el nivel de seguridad que les corresponda conforme a los criterios establecidos en el RGPD.

Todo fichero temporal o copia de trabajo así creado será borrado o destruido una vez que haya dejado de ser necesario para los fines que motivaron su creación.

Se deberán cumplir las siguientes normas:

- Los usuarios sólo crearán los ficheros temporales o copias de trabajos de documentos que sean estrictamente necesarios, y que estén autorizados, al menos de forma genérica por el Responsable de tratamiento.

- El sistema de información donde se almacenen los nuevos ficheros temporales o copias de documentos deberán cumplir con las mismas medidas de seguridad que las establecidas en el presente documento.

- La persona que cree el fichero temporal o copia de trabajo de documentos, será responsable de la adecuada custodia de la contraseña que asigne en su caso, y que deberá preservar de forma confidencial.

- El fichero temporal o copia de trabajo de documentos será eliminado una vez haya dejado de ser necesario para la finalidad para la cual se creó.

- En los casos en que sea posible, se incluirá el borrado automático de ficheros temporales al final de cada proceso o cadena de trabajos, o bien cuando el usuario se desconecta de la red o sale de la aplicación.

Se borrarán periódicamente los correos electrónicos y los ficheros, documentos anexos, así como el resultado de comprimir o descomprimir ficheros, o de clasificarlos, en todos los casos cuando tengan datos personales.

4. FUNCIONES Y OBLIGACIONES DEL PERSONAL.

Todo el personal 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 a **MARTINEZ CENTRO DE GESTIÓN, S.L.,** las incidencias de seguridad de las que tengan conocimiento respecto a los recursos protegidos, según los procedimientos establecidos en este Documento, y en concreto en su Anexo 1.

El personal que realice trabajos que no impliquen el tratamiento de datos personales tendrán limitado el acceso a estos datos, a los soportes que los contengan, o a los recursos del sistema de información.

Cuando se trate de personal ajeno, el contrato de prestación de servicios recogerá expresamente la prohibición de acceder a los datos personales y la obligación de secreto respecto de aquellos datos que hubiera podido conocer durante la prestación del servicio.

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

El Reglamento de Protección de Datos Europeo, identifican las figuras del Responsable del fichero o Tratamiento y el Encargado del Tratamiento al que le atribuyen responsabilidad:

a) El Responsable del fichero o Tratamiento. Éste puede ser la persona física o jurídica, de naturaleza pública o privada, u órgano administrativo, que decida sobre la finalidad, contenido y uso del tratamiento. Sus principales funciones son:

- Decidir sobre las medidas de seguridad aplicables.
- Responder jurídicamente de la seguridad del fichero y de las medidas establecidas en el presente documento,
- Implantar las medidas de seguridad establecidas en el presente documento y adoptar las medidas necesarias para que el personal afectado por este documento conozca las normas que afecten al desarrollo de sus funciones.
- Mantener actualizado el Registro de Actividades del Tratamiento, siempre que se produzcan cambios relevantes en el sistema de información, en la organización del mismo o en las disposiciones vigentes en materia de seguridad de datos.
- Autorizar expresamente la salida de soportes informáticos que contengan datos del Fichero fuera de los locales donde está ubicado el Fichero.

- Verificar la definición y correcta aplicación de las copias de respaldo y recuperación de los datos.

b) Encargado del tratamiento.

El encargado del tratamiento es la persona física o jurídica, autoridad pública, servicio u otro organismo que presta un servicio al responsable que conlleva el tratamiento de datos personales por cuenta de éste.

Los tipos de encargado del tratamiento y las formas en que se regulará su relación pueden ser tan variados como los tipos de servicios que puedan suponer acceso a datos personales.

Así, podemos encontrar servicios cuyo objeto principal es el tratamiento de datos personales y otros que tratan datos personales sólo como consecuencia de la actividad que presta por cuenta del responsable del tratamiento.

Pese a que la definición puede parecer clara, en la práctica se dan multitud de situaciones donde puede ser difícil deslindar cuándo estamos frente a un encargado o a un responsable del tratamiento. Para facilitar esta distinción, debemos tener en cuenta que corresponde al responsable decidir sobre la finalidad y los usos de la información, mientras que el encargado del tratamiento debe cumplir con las instrucciones de quien le encomienda un determinado servicio, respecto al correcto tratamiento de los datos personales a los que pueda tener acceso como consecuencia de la prestación de este servicio.

El encargado puede realizar todos los tratamientos, automatizados o no, que el responsable del tratamiento le haya encomendado formalmente. La definición de tratamiento nos permite concretarlos atendiendo al ciclo de vida de la información: recogida, registro, organización, estructuración, conservación, adaptación o modificación, extracción, consulta, utilización, comunicación por transmisión, difusión o cualquier otra forma de habilitación de acceso, cotejo o interconexión, limitación, supresión o destrucción. En todo caso, deben quedar claramente delimitados en el acuerdo que se adopte.

El encargado del tratamiento puede adoptar todas las decisiones organizativas y operacionales necesarias para la prestación del servicio que tenga contratado. En ningún caso puede variar las finalidades y los usos de los datos ni los puede utilizar para sus propias finalidades.

La regulación de la relación entre el responsable y el encargado del tratamiento debe establecerse a través de un contrato o de un acto jurídico similar que los vincule. El contrato o acto jurídico debe constar por escrito, inclusive en formato electrónico.

La posibilidad de regular esta relación a través de un acto jurídico unilateral del responsable del tratamiento es una de las novedades previstas en el RGPD. En cualquier caso debe tratarse de un acto jurídico que establezca y defina la posición del encargado del tratamiento, siempre y cuando ese acto vincule jurídicamente al encargado del tratamiento.

En cualquier caso, ya se trate de un acuerdo o de otro acto jurídico, su contenido debe reunir los requisitos establecidos en el RGPD, a los que más adelante se hace referencia.

El contenido del acto o acuerdo puede basarse en cláusulas tipo establecidas por la Comisión Europea o por la autoridad de control, inclusive cuando formen parte de una certificación otorgada al responsable o al encargado del tratamiento.

Artículo 28 del Reglamento de Protección de Datos establece:

1. Cuando se vaya a realizar un tratamiento por cuenta de un responsable del tratamiento, este elegirá únicamente un encargado que ofrezca garantías suficientes para aplicar medidas técnicas y organizativas apropiados, de manera que el tratamiento sea conforme con los requisitos del presente Reglamento y garantice la protección de los derechos del interesado.

2. El encargado del tratamiento no recurrirá a otro encargado sin la autorización previa por escrito, específica o general, del responsable. En este último caso, el encargado informará al responsable de cualquier cambio previsto en la incorporación o sustitución de otros encargados, dando así al responsable la oportunidad de oponerse a dichos cambios.

3. El tratamiento por el encargado se regirá por un contrato u otro acto jurídico con arreglo al Derecho de la Unión o de los Estados miembros, que vincule al encargado respecto del responsable y establezca el objeto, la duración, la naturaleza y la finalidad del tratamiento, el tipo de datos personales y categorías de interesados, y las obligaciones y derechos del responsable. Dicho contrato o acto jurídico estipulará, en particular, que el encargado:

a) tratará los datos personales únicamente siguiendo instrucciones documentadas del responsable, inclusive con respecto a las transferencias de datos personales a un tercer país o una organización internacional, salvo que esté obligado a ello en virtud del Derecho de la Unión o de los Estados miembros que se aplique al encargado; en tal caso, el encargado informará al responsable de esa exigencia legal previa al tratamiento, salvo que tal Derecho lo prohíba por razones importantes de interés público;

b) garantizará que las personas autorizadas para tratar datos personales se hayan comprometido a respetar la confidencialidad o estén sujetas a una obligación de confidencialidad de naturaleza estatutaria;

c) tomará todas las medidas necesarias de conformidad con el artículo 32;

d) respetará las condiciones indicadas en los apartados 2 y 4 para recurrir a otro encargado del tratamiento;

e) asistirá al responsable, teniendo cuenta la naturaleza del tratamiento, a través de medidas técnicas y organizativas apropiadas, siempre que sea posible, para que este pueda cumplir con su obligación de responder a las solicitudes que tengan por objeto el ejercicio de los derechos de los interesados establecidos en el capítulo III;

f) ayudará al responsable a garantizar el cumplimiento de las obligaciones establecidas en los artículos 32 a 36, teniendo en cuenta la naturaleza del tratamiento y la información a disposición del encargado;

g) a elección del responsable, suprimirá o devolverá todos los datos personales una vez finalice la prestación de los servicios de tratamiento, y suprimirá las copias existentes a menos que se requiera la conservación de los datos personales en virtud del Derecho de la Unión o de los Estados miembros;

h) pondrá a disposición del responsable toda la información necesaria para demostrar el cumplimiento de las obligaciones establecidas en el presente artículo, así como para permitir y contribuir a la realización de auditorías, incluidas inspecciones, por parte del responsable o de otro auditor autorizado por dicho responsable.

En relación con lo dispuesto en la letra h) del párrafo primero, el encargado informará inmediatamente al responsable si, en su opinión, una instrucción infringe el presente Reglamento u otras disposiciones en materia de protección de datos de la Unión o de los Estados miembros.

4. Cuando un encargado del tratamiento recurra a otro encargado para llevar a cabo determinadas actividades de tratamiento por cuenta del responsable, se impondrán a este otro encargado, mediante contrato u otro acto jurídico establecido con arreglo al Derecho de la Unión o de los Estados miembros, las mismas obligaciones de protección de datos que las estipuladas en el contrato u otro acto jurídico entre el responsable y el encargado a que se refiere el apartado 3, en particular la prestación de garantías suficientes de aplicación de medidas técnicas y organizativas apropiadas de manera que el tratamiento sea conforme con las disposiciones del presente Reglamento. Si ese otro encargado incumple sus obligaciones de protección de datos, el encargado inicial seguirá siendo plenamente responsable ante el responsable del tratamiento por lo que respecta al cumplimiento de las obligaciones del otro encargado.

5. La adhesión del encargado del tratamiento a un código de conducta aprobado a tenor del artículo 40 o a un mecanismo de certificación aprobado a tenor del artículo 42 podrá utilizarse como elemento para demostrar la existencia de las garantías suficientes a que se refieren los apartados 1 y 4 del presente artículo.

6. Sin perjuicio de que el responsable y el encargado del tratamiento celebren un contrato individual, el contrato u otro acto jurídico a que se refieren los apartados 3 y 4 del presente artículo podrá basarse, total o parcialmente, en las cláusulas contractuales tipo a que se refieren los apartados 7 y 8 del presente artículo, inclusive cuando formen parte de una certificación concedida al responsable o encargado de conformidad con los artículos 42 y 43.

7. La Comisión podrá fijar cláusulas contractuales tipo para los asuntos a que se refieren los apartados 3 y 4 del presente artículo, de acuerdo con el procedimiento de examen a que se refiere el artículo 93, apartado 2.

8. Una autoridad de control podrá adoptar cláusulas contractuales tipo para los asuntos a que se refieren los apartados 3 y 4 del presente artículo, de acuerdo con el mecanismo de coherencia a que se refiere el artículo 63.

9. El contrato u otro acto jurídico a que se refieren los apartados 3 y 4 constará por escrito, inclusive en formato electrónico.

10. Sin perjuicio de lo dispuesto en los artículos 82, 83 y 84, si un encargado del tratamiento infringe el presente Reglamento al determinar los fines y medios del tratamiento, será considerado responsable del tratamiento con respecto a dicho tratamiento.

Los datos identificativos del Responsable del Tratamiento se contienen en el Anexo 1.1.

Las obligaciones que con carácter general tienen que conocer los empleados de MARTINEZ CENTRO DE GESTIÓN, S.L., en el desarrollo de sus funciones son las siguientes:

- El personal es responsable individualmente del entendimiento y el respeto de las reglas establecidas con respecto a la seguridad de los sistemas informáticos y la información que en ellos se trata.

- Quienes intervengan en cualquier fase del tratamiento de datos de carácter personal están obligados al secreto profesional respecto de los mismos y al deber de guardarlos, subsistiendo estas obligaciones aún después de haber cambiado de función.

- Usar los datos exclusivamente para el fin que han sido facilitados y de acuerdo con la función que le ha sido encomendada.

- Utilizar software homologado por los órganos pertinentes.

- Utilizar las facilidades de control de acceso a todos los niveles en ordenadores que almacenan datos de carácter personal.

- Proteger y mantener en secreto las contraseñas utilizadas para su gestión y cambiarlas con la periodicidad que establezca el documento de seguridad.

- Apagar de forma ordenada la estación de trabajo, al finalizar la jornada de trabajo.

- Comunicar cualquier anomalía por mal funcionamiento (hardware, software, virus informáticos), así como cualquier incidencia de seguridad (intentos de acceso no autorizados, manejo inadecuado de datos, etc.) al Responsable de tratamiento de los datos.

- Habilitar los medios necesarios para proteger los soportes que contengan datos de carácter personal.

- Utilizar los medios necesarios para destruir los soportes antes de desecharlos o reutilizarlos cuando la información contenida en estos así lo requiera.

- Guardar los soportes que contengan datos de carácter personal en armarios o escritorios protegidos con llave al finalizar la jornada de trabajo.

- Utilizar los equipos informáticos exclusivamente para la finalidad para la que han sido facilitados y nunca para trabajos particulares.

5. PROCEDIMIENTO DE NOTIFICACIÓN, GESTIÓN Y RESPUESTA ANTE LAS INCIDENCIAS.

Se considerarán como "incidencias de seguridad", entre otras cualquier incumplimiento de la normativa desarrollada en este documento, así como cualquier anomalía que afecte o pueda afectar a la seguridad de los datos de carácter personal de MARTINEZ CENTRO DE GESTIÓN, S.L.

Se recogerá cuantas incidencias de seguridad se produzcan sobre los datos de carácter personal que trata. Con tal objeto, se recoge en el procedimiento de notificación, gestión y respuesta una lista de incidencias a modo enunciativo y no limitativo que serán registradas a criterio del Responsable del Fichero, es decir, se recogerá cualquier anomalía que afecte o pudiera afectar a la seguridad de los datos de carácter personal. Algunos ejemplos de Incidencias son:

- Incidencias que afecten a los Derechos de Acceso a los Datos.
- Incidencias que afecten a los procedimientos de Copias de Respaldo o Recuperación.
- Incidencias que afecten a la identificación y autenticación de los usuarios.
- Incidencias que afecten a la gestión de soporte informáticos.
- Cualquier otra de las observadas como consecuencia de la ejecución de los controles definidos para garantizar el cumplimiento de lo dispuesto en el Documento de Seguridad.

Existe un procedimiento de notificación y gestión de incidencias que se describe en el Anexo 2.1.

6. PROCEDIMIENTOS DE REVISIÓN.

El documento deberá mantenerse en todo momento actualizado y deberá ser revisado siempre que se produzcan cambios relevantes en el sistema de información, en el contenido de la información incluida en los ficheros o como consecuencia de los controles periódicos realizados. En todo caso se entenderá como cambio relevante cuando pueda repercutir en el cumplimiento de las medidas de seguridad implantadas. Asimismo, deberá adecuarse, en todo momento, a las disposiciones vigentes en materia de seguridad de los datos de carácter personal.

Al menos cada dos años, se realizará una auditoria, externa o interna que dictamine el correcto cumplimiento y la adecuación de las medidas del presente documento, identificando las deficiencias y proponiendo las medidas correctoras necesarias.

7. EJERCICIO DE DERECHOS

Con carácter general, los responsables deben facilitar a los interesados el ejercicio de sus derechos, y los procedimientos y las formas para ello deben ser visibles, accesibles y sencillos.

Se requiere que los responsables posibiliten la presentación de solicitudes por medios electrónicos, especialmente cuando el tratamiento se realiza por estos medios.

El ejercicio de los derechos será gratuito para el interesado, excepto:

En los casos en que se formulen solicitudes manifiestamente infundadas o excesivas, especialmente por repetitivas, el responsable podrá cobrar un canon que compense los costes administrativos de atender a la petición o negarse a actuar (el canon no podrá implicar un ingreso adicional para el responsable, sino que deberá corresponderse efectivamente con el verdadero coste de la tramitación de la solicitud).

Obligaciones

- Articular procedimientos que permitan fácilmente que los interesados puedan acreditar que han ejercido sus derechos por medios electrónicos (actualmente, en muchas ocasiones, no es viable).

- El responsable debe demostrar el carácter infundado o excesivo de las solicitudes que tengan un coste para el interesado.

- El responsable deberá informar al interesado sobre las actuaciones derivadas de su petición en el plazo de un mes (podrá extenderse dos meses más cuando se trate de solicitudes especialmente complejas y deberá notificar esta ampliación dentro del primer mes).

- Si el responsable decide no atender una solicitud, deberá informar de ello, motivando su negativa, dentro del plazo de un mes desde su presentación.

- El titular de los datos personales podrá escoger entre las posibilidades de acceso a la información como por ejemplo la visualización en pantalla, telecopia, fotocopia, escritura o cualquier otro procedimiento adecuado a la configuración y la implantación material del fichero. En el Anexo 4.9 tenemos una serie de modelos de solicitud de ejercicio de derechos.

7.1. Derecho de Acceso

El interesado tendrá derecho a obtener del responsable del tratamiento confirmación de si se están tratando o no datos personales que le conciernen y, en tal caso, derecho de acceso a los datos personales y a la siguiente información:

a) los fines del tratamiento;

b) las categorías de datos personales de que se trate;

c) los destinatarios o las categorías de destinatarios a los que se comunicaron o serán comunicados los datos personales, en particular destinatarios en terceros u organizaciones internacionales;

d) de ser posible, el plazo previsto de conservación de los datos personales o, de no ser posible, los criterios utilizados para determinar este plazo;

e) la existencia del derecho a solicitar del responsable la rectificación o supresión de datos personales o la limitación del tratamiento de datos personales relativos al interesado, o a oponerse a dicho tratamiento;

f) el derecho a presentar una reclamación ante una autoridad de control;

g) cuando los datos personales no se hayan obtenido del interesado, cualquier información disponible sobre su origen;

h) la existencia de decisiones automatizadas, incluida la elaboración de perfiles, a que se refiere el artículo 22, apartados 1 y 4, y, al menos en tales casos, información significativa sobre la lógica aplicada, así como la importancia y las consecuencias previstas de dicho tratamiento para el interesado.

2. Cuando se transfieran datos personales a un tercer país o a una organización internacional, el interesado tendrá derecho a ser informado de las garantías adecuadas en virtud del artículo 46 relativas a la transferencia.

3. El responsable del tratamiento facilitará una copia de los datos personales objeto de tratamiento. El responsable podrá percibir por cualquier otra copia solicitada por el interesado un canon razonable basado en los costes administrativos. Cuando el interesado presente la solicitud por medios electrónicos, y a menos que este solicite que se facilite de otro modo, la información se facilitará en un formato electrónico de uso común.

4. El derecho a obtener copia mencionado en el apartado 3 no afectará negativamente a los derechos y libertades de otros.

7.2. Derecho de Supresión

1. El interesado tendrá derecho a obtener sin dilación indebida del responsable del tratamiento la supresión de los datos personales que le conciernan, el cual estará obligado a suprimir sin dilación indebida los datos personales cuando concurra alguna de las circunstancias siguientes:

a) los datos personales ya no sean necesarios en relación con los fines para los que fueron recogidos o tratados de otro modo;

b) el interesado retire el consentimiento en que se basa el tratamiento de conformidad con el artículo 6, apartado 1, letra a), o el artículo 9, apartado 2, letra a), y este no se base en otro fundamento jurídico;

c) el interesado se oponga al tratamiento con arreglo al artículo 21, apartado 1, y no prevalezcan otros motivos legítimos para el tratamiento, o el interesado se oponga al tratamiento con arreglo al artículo 21, apartado 2;

d) los datos personales hayan sido tratados ilícitamente;

e) los datos personales deban suprimirse para el cumplimiento de una obligación legal establecida en el Derecho de la Unión o de los Estados miembros que se aplique al responsable del tratamiento;

f) los datos personales se hayan obtenido en relación con la oferta de servicios de la sociedad de la información mencionados en el artículo 8, apartado 1.

2. Cuando haya hecho públicos los datos personales y esté obligado, en virtud de lo dispuesto en el apartado 1, a suprimir dichos datos, el responsable del tratamiento, teniendo en cuenta la tecnología disponible y el coste de su aplicación, adoptará medidas razonables, incluidas medidas técnicas, con miras a informar a los responsables que estén tratando los datos personales de la solicitud del interesado de supresión de cualquier enlace a esos datos personales, o cualquier copia o réplica de los mismos.

3. Los apartados 1 y 2 no se aplicarán cuando el tratamiento sea necesario:

a) para ejercer el derecho a la libertad de expresión e información;

b) para el cumplimiento de una obligación legal que requiera el tratamiento de datos impuesta por el Derecho de la Unión o de los Estados miembros que se aplique al responsable del tratamiento, o para el cumplimiento de una misión realizada en interés público o en el ejercicio de poderes públicos conferidos al responsable.

c) por razones de interés público en el ámbito de la salud pública de conformidad con el artículo 9, apartado 2, letras h) e i), y apartado 3;

d) con fines de archivo en interés público, fines de investigación científica o histórica o fines estadísticos, de conformidad con el artículo 89, apartado 1, en la medida en que el derecho indicado en el apartado 1 pudiera hacer imposible u obstaculizar gravemente el logro de los objetivos de dicho tratamiento, o

e) para la formulación, el ejercicio o la defensa de reclamaciones.

7.3. Derecho de Oposición

El interesado tendrá derecho a oponerse en cualquier momento, por motivos relacionados con su situación particular, a que datos personales que le conciernan sean objeto de un tratamiento basado en lo dispuesto en el artículo 6, apartado 1, letras e) o f), incluida la elaboración de perfiles sobre la base de dichas disposiciones. El responsable del tratamiento dejará de tratar los datos personales, salvo que acredite motivos legítimos imperiosos para el tratamiento que prevalezcan sobre los intereses, los derechos y las libertades del interesado, o para la formulación, el ejercicio o la defensa de reclamaciones.

Cuando el tratamiento de datos personales tenga por objeto la mercadotecnia directa, el interesado tendrá derecho a oponerse en todo momento al tratamiento de los datos personales que le conciernan, incluida la elaboración de perfiles en la medida en que esté relacionada con la citada mercadotecnia.

Cuando el interesado se oponga al tratamiento con fines de mercadotecnia directa, los datos personales dejarán de ser tratados para dichos fines.

A más tardar en el momento de la primera comunicación con el interesado, el derecho indicado en los apartados 1 y 2 será mencionado explícitamente al interesado y será presentado claramente y al margen de cualquier otra información.

En el contexto de la utilización de servicios de la sociedad de la información, y no obstante lo dispuesto en la Directiva 2002/58/CE, el interesado podrá ejercer su derecho a oponerse por medios automatizados que apliquen especificaciones técnicas.

Cuando los datos personales se traten con fines de investigación científica o histórica o fines estadísticos de conformidad con el artículo 89, apartado 1, el interesado tendrá derecho, por motivos relacionados con su situación particular, a oponerse al tratamiento de datos personales que le conciernan, salvo que sea necesario para el cumplimiento de una misión realizada por razones de interés público.

7.4. Derecho de Rectificación.

El interesado tendrá derecho a obtener sin dilación indebida del responsable del tratamiento la rectificación de los datos personales inexactos que le conciernan. Teniendo en cuenta los fines del tratamiento, el interesado tendrá derecho a que se completen los datos personales que sean incompletos, inclusive mediante una declaración adicional.

7.5. Derecho a la Limitación del tratamiento.

El interesado tendrá derecho a obtener del responsable del tratamiento la limitación del tratamiento de los datos cuando se cumpla alguna de las condiciones siguientes:

a) el interesado impugne la exactitud de los datos personales, durante un plazo que permita al responsable verificar la exactitud de los mismos;

b) el tratamiento sea ilícito y el interesado se oponga a la supresión de los datos personales y solicite en su lugar la limitación de su uso;

c) el responsable ya no necesite los datos personales para los fines del tratamiento, pero el interesado los necesite para la formulación, el ejercicio o la defensa de reclamaciones;

d) el interesado se haya opuesto al tratamiento en virtud del artículo 21, apartado 1, mientras se verifica si los motivos legítimos del responsable prevalecen sobre los del interesado.

2. Cuando el tratamiento de datos personales se haya limitado en virtud del apartado 1, dichos datos solo podrán ser objeto de tratamiento, con excepción de su conservación, con el consentimiento del interesado o para la formulación, el ejercicio o la defensa de reclamaciones, o con miras a la protección de los derechos de otra persona física o jurídica o por razones de interés público importante de la Unión o de un determinado Estado miembro.

3. Todo interesado que haya obtenido la limitación del tratamiento con arreglo al apartado 1 será informado por el responsable antes del levantamiento de dicha limitación.

7.6. Derecho a la limitación del tratamiento.

El interesado tendrá derecho a recibir los datos personales que le incumban, que haya facilitado a un responsable del tratamiento, en un formato estructurado, de uso común y lectura mecánica, y a transmitirlos a otro responsable del tratamiento sin que lo impida el responsable al que se los hubiera facilitado, cuando:

a) el tratamiento esté basado en el consentimiento con arreglo al artículo 6, apartado 1, letra a), o el artículo 9, apartado 2, letra a), o en un contrato con arreglo al artículo 6, apartado 1, letra b), y

b) el tratamiento se efectúe por medios automatizados.

2. Al ejercer su derecho a la portabilidad de los datos de acuerdo con el apartado 1, el interesado tendrá derecho a que los datos personales se transmitan directamente de responsable a responsable cuando sea técnicamente posible.

3. El ejercicio del derecho mencionado en el apartado 1 del presente artículo se entenderá sin perjuicio del artículo 17. Tal derecho no se aplicará al tratamiento que sea necesario para el cumplimiento de una misión realizada en interés público o en el ejercicio de poderes públicos conferidos al responsable del tratamiento.

4. El derecho mencionado en el apartado 1 no afectará negativamente a los derechos y libertades de otros.

Existe un modelo de solicitud de ejercicio de derechos en el Anexo 4.6.

8. ACCESO A LOS DATOS POR CUENTA DE TERCEROS

El acceso a los datos por cuenta de terceros es el acceso permitido a terceros que no tienen la condición de responsable del fichero, usuario o interesado, sin que por ello se produzca una cesión o comunicación de datos.

Se trata de la posibilidad de que los datos personales puedan ser tratados por personas distintas de los usuarios de la propia organización del responsable del fichero, por encargo de éste. Esta tercera persona se convierte en este caso en encargado de tratamiento, y presta servicios al responsable del fichero, siempre que dichos servicios tengan como objeto una finalidad lícita y legítima. El servicio prestado por el encargado podrá tener o no carácter remunerado y ser temporal o indefinido.

La LOPD regula la relación entre el responsable del fichero y el encargado del tratamiento, estableciendo una serie de obligaciones encaminadas a garantizar la seguridad del tratamiento de los datos personales.

Esta relación debe regularse en un contrato escrito o en alguna otra forma que permita acreditar su celebración en el que conste:

— Que el encargado únicamente tratará los datos conforme a las instrucciones del responsable del tratamiento.

— Las medidas de seguridad que el encargado del tratamiento está obligado a implementar.

— Que el encargado del tratamiento no utilizará los datos con fines distintos a los que figuren en el contrato.

— Que el encargado del tratamiento no cederá los datos a otras personas, ni siquiera para su conservación.

— Que una vez cumplida la prestación, los datos serán destruidos o devueltos al responsable, al igual que cualquier soporte o documentos en que consten datos objeto del tratamiento.

Por otra parte, el encargado del tratamiento responderá de las infracciones en las que hubiera incurrido personalmente, equiparándose en tal caso su figura, en materia de responsabilidad, a la del responsable del tratamiento, con independencia de las posibles y concretas obligaciones propias del responsable del tratamiento.

No obstante, el encargado del tratamiento no incurrirá en responsabilidad cuando, previa indicación expresa del responsable, comunique los datos a un tercero designado por aquél, al que hubiera encomendado la prestación de un servicio.

Para que esta subcontratación tenga lugar será necesario que el encargado del tratamiento haya obtenido la autorización del responsable del fichero. Esta subcontratación se efectuará siempre en nombre y por cuenta del responsable del fichero.

Sin embargo, será posible la subcontratación sin necesidad de autorización del responsable del fichero siempre y cuando se cumplan los siguientes requisitos:

a) Que se especifiquen en el contrato los servicios que puedan ser objeto de subcontratación y la empresa con la que se vaya a subcontratar.

b) Que el tratamiento de datos de carácter personal por parte del subcontratista se ajuste a las instrucciones del responsable del fichero.

c) Que el encargado del tratamiento y la empresa subcontratista formalicen el contrato, en los términos previstos para el contrato entre el responsable del fichero y el encargado del tratamiento.

En este caso, el subcontratista será considerado encargado del tratamiento.

En el supuesto que durante la prestación del servicio resultase necesario subcontratar una parte del mismo y dicha circunstancia no hubiera sido prevista en el contrato, deberán someterse al responsable del fichero los extremos señalados anteriormente.

Los modelos de contrato se encuentran en el Anexo 4.8.

ANEXOS

ANEXO 1: ASPECTOS RELATIVOS A LOS FICHEROS

1.1) Datos del Responsable del Tratamiento

Nombre de la Organización	MARTINEZ CENTRO DE GESTIÓN, S.L.
NIF	B46953170
Domicilio del Centro	C/ ALBACETE, Nº 10 (VALENCIA)
Sedes	BENETUSSER: CALLE CERVANTES 45 (46910) BENAGUASIL: PLAZA MAYOR DE LA VILA Nº 17 (46180)
Teléfono	96.317.22.54
Actividad	GESTIÓN TRIBUTARIA Y DE MULTAS, CONSERVACIÓN, CONSULTA, REGISTRO, INTERCONEXIÓN Y COMUNICACIÓN.
Representante del Responsable Del Fichero	ANTONIO MARTÍNEZ FERRERO
Delegado de Protección de datos	CARLOS FOSSATI MEDEL

1.2) Tratamientos

Fichero Inscrito	VIDEOVIGILANCIA
Carácter	Privado
Sistema de Tratamiento	Automatizado

Fichero Inscrito	CLIENTES Y PROVEEDORES
Carácter	Privado
Sistema de Tratamiento	Mixto

Fichero Inscrito	USUARIOS WEB
Carácter	Privado
Sistema de Tratamiento	Automatizado

Fichero Inscrito	NOMINAS, PERSONAL Y RECURSOS HUMANOS
Carácter	Privado
Sistema de Tratamiento	Mixto

Fichero Inscrito	FISCAL CONTABLE
Carácter	Privado
Sistema de Tratamiento	Mixto

1.3) Obligaciones del Responsable del Fichero

- ⇒ Emprender las operaciones determinadas reglamentariamente para proceder a la notificación, inscripción y modificación de ficheros.
- ⇒ Informar a lo afectados de la existencia, finalidad y tratamiento de los ficheros, así como de posibles cesiones de datos.
- ⇒ Obtener consentimiento de los afectados, en los casos en que éste sea obligatorio, para el tratamiento y cesión de los datos personales contenidos en los ficheros.
- ⇒ Cumplir con el secreto profesional respecto de los datos de carácter personal y con el deber de guardarlos. Estas obligaciones subsistirán aun después de finalizar las relaciones con el titular de los datos.
- ⇒ Hacer efectivo el derecho de rectificación o cancelación de los interesados.
- ⇒ Implantar las medidas de seguridad establecidas en este Documento.
- ⇒ Garantizar la difusión de este Documento entre todo el personal usuario de los Ficheros.
- ⇒ Mantener actualizado el Documento siempre que se produzcan cambios relevantes en el sistema de información o en la organización del mismo.
- ⇒ Adecuar en todo momento el contenido del Documento a las disposiciones vigentes en materia de seguridad de datos.
- ⇒ Autorizar, en su caso, la ejecución de tratamiento de datos de carácter personal fuera de los locales de la ubicación del fichero.
- ⇒ Encargarse de que exista una relación actualizada de usuarios que tengan acceso autorizado al sistema de información y de establecer procedimientos de identificación y autenticación para dicho acceso.
- ⇒ Establecer los criterios para la autorización de acceso a ficheros, modificación de accesos y anulación de accesos.
- ⇒ Se encargará de la autorización de la salida de soportes fuera de los locales en los que esté ubicado el fichero, así como de la entrada de soportes.
- ⇒ Verificar la correcta aplicación de los procedimientos de respaldo y recuperación de datos.

1.4) Personal con acceso físico a los datos personales.

Exclusivamente el personal que se indica a continuación, podrá tener acceso a los locales donde se encuentren ubicados los sistemas de información:

NOMBRE Y APELLIDOS	CARGO	FIRMA	BAJA

NOMBRE Y APELLIDOS	CARGO	FIRMA	BAJA

ANEXO 2: MEDIDAS ADOPTADAS PARA LOS FICHEROS.

2.1) Notificación y gestión de incidencias.

Se ha redactado un formulario de registro de incidencias a disposición de todos los usuarios con acceso a los ficheros con el fin de que quede debidamente registrada cualquier incidencia que al producirse haya puesto en peligro o haya dañado los ficheros de datos.

El Usuario que tenga en conocimiento la incidencia se responsabiliza directa y personalmente de registrarla en el citado impreso, entregándolo a continuación al Responsable del departamento para su comprobación el cual lo remitirá al Responsable de tratamiento.

Si se hubiesen visto afectados los ficheros de datos de especial protección y sea necesario llevar a cabo algún procedimiento de recuperación de datos, será necesario que el Responsable del fichero autorice la ejecución de dicho procedimiento, mediante su firma en el impreso de registro de incidencias.

No registrar las incidencias, o no entregar el impreso cuando sea necesario será considerado como una falta contra la que se impondrán las sanciones previstas especificadas en la normativa laboral aplicable a la organización.

Localización de las incidencias: Despacho Central del Responsable del fichero, donde a través del formato Word se gestionarán dichas incidencias.

2.2) Procedimiento de bajas de usuario del fichero.

El responsable del departamento debe notificar al responsable de tratamiento las bajas de usuarios utilizando para ello el impreso disponible al efecto. Esta comunicación deberá producirse cuando el cese de la relación laboral o un cambio de departamento hagan innecesario su acceso a los datos. En el impreso de notificación se indicará los datos básicos del usuario y los ficheros a los que se les deben cancelar el acceso.

El impreso, debidamente firmado por el responsable del departamento, se remitirá al responsable de seguridad que procederá a formalizar la baja en la relación de usuarios de este documento. Una vez firmado, se remitirá al responsable de tratamiento junto con la solicitud de baja. Éste una vez desactivado el usuario lo excluirá en la relación de usuarios de este documento.

2.3) Procedimiento de Altas de Usuario.

El responsable del departamento debe notificar al responsable de tratamiento las altas de usuarios utilizando para ello el impreso disponible al efecto. En el mismo indicará los datos básicos del usuario y los ficheros físicos a los que se debe permitir el acceso.

Se le informará al usuario de sus obligaciones contenidas en este documento.

El impreso en el que se notifiquen las obligaciones, debidamente firmado, se remitirá al responsable de seguridad junto con la solicitud de alta. Una vez activado el nuevo usuario lo incluirá en la relación de usuarios de este documento.

2.4) Entorno de Red.

Existen aprox.95 ordenadores con sistemas operativos Windows 10 con conexión a Internet. Se utilizan antivirus (KASPERSKY).

2.5) Procedimiento de desechado y reutilización de soportes.

El desechado de los discos externos USB y las unidades de memoria flash USB está expuesto a un riesgo de seguridad, dado que existen herramientas de software capaces de leer el contenido de éstos incluso después de haber sido formateados (incluso tras un formateo completo). Para evitar este riesgo se utilizará software de borrado seguro de datos, según se detalla a continuación.

La reutilización de los soportes: Los discos externos USB y las unidades de memoria flash USB se borrarán utilizando las herramientas disponibles en el sistema operativo del ordenador (eliminación de ficheros).

Desechado del soporte: En los discos externos USB es necesario realizar un borrado seguro de los datos antes de ser desechados. Nunca se utilizará en estos casos el formateo rápido ni el formateo habitual. Se utilizará para ello un software de borrado seguro de datos, como por ejemplo Clean Disk Security, Eraser o Prevent Restore. En caso de que el disco externo USB estuviera averiado, defectuoso o no se pudiera formatear, se realizará una destrucción física del disco.

Desechado del soporte: En las unidades de memoria flash USB es necesario realizar un formateo completo antes de ser desechados. Nunca se utilizará en estos casos el formateo rápido. Para mayor seguridad se podrá utilizar para ello un software de borrado seguro de datos, como por ejemplo Prevent Restore. En caso de que la memoria flash USB estuviera averiada, defectuosa o no se pudiera formatear, se realizará una destrucción física de la misma.

ANEXO 3: DATOS DE LOS FICHEROS

3.A) Datos del Fichero Clientes y Proveedores.

Nombre	**CLIENTES Y PROVEEDORES**
Finalidad	Permite la gestión administrativa de los clientes y Proveedores que acceden a la empresa.
Descripción	Contiene los datos identificativos de nivel básico.
Campos del fichero	Datos de carácter identificativo: D.N.I. / N.I.F., Nombre y apellidos, Dirección (postal, electrónica), Teléfono.
Sistema de Tratamiento	Automatizado
Lugar físico de almacenamiento	Despacho Central
Domicilio	VALENCIA: C/ ALBACETE, Nº 10 BENETUSSER: CALLE CERVANTES 45 46910 BENAGUASIL: PLAZA MAYOR DE LA VILA Nº 17 46180
Descripción	El despacho se encuentra cerrado bajo llave.
Unidad/es con acceso al fichero o tratamiento	Profesional autorizado.

3.B) Datos del Fichero Nominas, Personal y Recursos Humanos.

Nombre	**NÓMINAS, PERSONAL Y RECURSOS HUMANOS**
Finalidad	Permite la gestión administrativa y contable de los empleados.
Descripción	Contiene los datos identificativos de las personas y entidades necesarias.
Campos del fichero	Datos de carácter identificativo: D.N.I. /N.I.F., Nombre y apellidos, Dirección (postal, electrónica), Teléfono. Datos de características personales: Datos de estado civil, Fecha de nacimiento, Lugar de nacimiento, Edad.
Sistema de Tratamiento	Mixto
Lugar físico de almacenamiento	Despacho Central
Domicilio del Despacho Central	C/ ALBACETE, Nº 10 (VALENCIA)
Descripción	El despacho se encuentra cerrado bajo llave.
Unidad/es con acceso al fichero o tratamiento	Profesional autorizado.

3.C) Datos del Fichero Fiscal-Contable.

Nombre	**FISCAL-CONTABLE**
Finalidad	Permite la gestión fiscal y contable de la empresa
Descripción	Contiene los datos identificativos de las personas y entidades necesarias.
Campos del fichero	Datos de carácter identificativo: D.N.I. /N.I.F., Nombre y apellidos, Dirección (postal, electrónica), Teléfono. Datos de características personales: Datos de estado civil, Fecha de nacimiento, Lugar de nacimiento, Edad.
Sistema de Tratamiento	Mixto
Lugar físico de almacenamiento	Despacho Central
Domicilio	C/ ALBACETE, Nº 10 (VALENCIA)
Encargado del Tratamiento	LEOPOLDO GARCÍA ASESORES, S.L. CIF: B98030968 C/ NICOLAZ ESTEVANEZ, Nº3 VALENCIA
Descripción	El despacho se encuentra cerrado bajo llave.
Unidad/es con acceso al fichero o tratamiento	Profesional autorizado.

3. D) Datos del Fichero Usuarios Web.

Nombre	**USUARIOS WEB**
Finalidad	Permite la gestión administrativa de los usuarios registrados en la página web.
Descripción	Contiene los datos de categorías especiales
Campos del fichero	Datos de carácter identificativo: D.N.I. / N.I.F., Nombre y apellidos, Dirección (postal, electrónica), Teléfono. Datos de características personales: Datos de estado civil, Datos de familia, Fecha de nacimiento, Lugar de nacimiento, Edad, Sexo, Nacionalidad.
Sistema de Tratamiento	Mixto
Lugar físico de almacenamiento	Despacho Central
Domicilio	C/ ALBACETE, Nº 10 (VALENCIA)
Descripción	El despacho se encuentra cerrado bajo llave.
Unidad/es con acceso al fichero o tratamiento	Profesional autorizado.

3.E) Datos del Fichero Videovigilancia.

Nombre	**VIDEOVIGILANCIA**
Finalidad	Permite la gestión y captación de imágenes.
Descripción	Contiene los datos identificativos de nivel básico.
Campos del fichero	Datos de carácter identificativo: D.N.I. / N.I.F., Nombre y apellidos, Dirección (postal, electrónica), Teléfono.
Sistema de Tratamiento	Automatizado
Lugar físico de almacenamiento	Despacho Central
Domicilio	C/ ALBACETE, Nº 10 (VALENCIA)
Descripción	El despacho se encuentra cerrado bajo llave.
Unidad/es con acceso al fichero o tratamiento	Profesional autorizado.
Empresa prestadora del servicio	GUIREX

REALIZACIÓN DE COPIAS DE SEGURIDAD Y RESTAURACIÓN

- SERVIDORES VIRTUALES

Existe instalado en los servidores virtuales de HyperV-1 (Citrix1, Citrix2, VMAdministracion, VMAntivirus, VMCentralita) e HyperV-2 (VinAccess, Vintegris, Vm-Pobles, Vm-Pobles-BBDD y VmServicios) el programa Shadow Protect, que hace copias incrementales cada hora del día desde las 8 a las 19 horas. Existe un Manager instalado en VM-Pobles que controla las ubicaciones y copias de seguridad. Así mismo, hemos instalado un servidor ShadowControl, en Ubuntu, que tiene una consola que permite controlar los Shadow Protect de cada uno de los servidores. Este servidor tiene la IP 0.254.0.140.

Las copias de seguridad de las máquinas virtuales se alojan en **\\valencia-bbdd\copiamv** Desde aquí se subirá a Azure con la herramienta de copia de archivos.

Un archivo de imagen de backup de ShadowProtect es una representación de un momento dado del volumen de un equipo. No es una copia estándar del archivo del volumen, sino un duplicado sector a sector del volumen. Debido a esto, puede montar un archivo de imagen de backup (usando la utilidad Montaje de ShadowProtect) y ver sus contenidos como si fuera un volumen regular. Se usa un archivo de clave de contraseña para cifrar un archivo de imagen de backup.

- BASES DE DATOS

Las copias de seguridad de bases de datos se realizan con la utilidad de backup del propio SQLServer. Se hace tanto en el servidor de Valencia como en VM-Pobles-BBDD. Una vez generados los ficheros de copia, se sacan a un disco duro externo conectado al equipo de Enrique Pérez con la utilidad EaseUs Backup. Se dispone de dos discos duros en los cuales almacenamos copias de seguridad de hasta 2 semanas. La copia de realiza a partir de las 00:00 en tres trabajos de copia distintos.

- ARCHIVOS Y CARPETAS

Los archivos correspondientes a los datos del Ajuntament de Valencia se encuentran alojados en el LeftHand. De ellos el responsable de seguridad hace una copia de seguridad semanal en dos discos duros externos conectados a Valencia-BBDD.

Los datos de los restantes clientes de la empresa se encuentran alojados en discos duros en Hyperv-2. Se hace una copia en Azure incremental diaria desatendida con un agente instalado en el servidor Hyperv-2.

Los archivos y carpetas de los usuarios se configuran para utilizarlos desde OneDrive, de forma que se tiene una copia instantánea de la información que hay en las carpetas.

Todo ello se anota en el registro de copias de seguridad de la empresa.

- CORREOS ELECTRÓNICOS

Los correos electrónicos se copian en un disco duro externo conectado al equipo de Adrián, en una carpeta compartida llamada "Correo Electrónico", que tiene una estructura de carpetas por departamentos. Se realiza copia de seguridad mediante la utilidad de copia de Windows 10 de los correos los jueves por la noche mediante tareas programadas en cada uno de los ordenadores de los que se hace copia, excepto Pascual que la tiene programada diaria a mediodía con el software de copia WD Backup en disco duro conectado a su PC.

RESTAURACIÓN

Todas las restauraciones que se hayan de realizar de datos reales han de ser autorizadas por la Comisión de Seguridad de la Información siguiendo el modelo R03 de LOPD.

Se ha planificado una restauración de cada uno de los módulos en Julio de cada año, con el fin de comprobar la fiabilidad de los sistemas de copia.

- SERVIDORES VIRTUALES

Desde la utilidad de copia ShadowProtect, se siguen las instrucciones de restauración, montando una unidad de disco desde el fichero de copia de seguridad y seleccionando los archivos a restaurar.

- BASES DE DATOS

Desde la utilidad de copia EaseUs Backup se seleciona el archivo de copia de seguridad, copiando el archivo bak de la base de datos a restaurar en una unidad local al servidor donde se va a hacer la restauración. A partir de este momento, desde el SQL Server Management se restaura la base de datos en el servidor.

- ARCHIVOS Y CARPETAS

Los datos del Ajuntament de Valéncia, se accede a los discos duros externos y se copia la información que se necesite.

En el caso de los pueblos, desde la interfaz de Azure se buscan los archivos correspondientes, se seleccionan y se restauran en la ubicación elegida.

Los usuarios disponen de la copia de OneDrive para gestionar las copias de sus archivos.

- CORREOS ELECTRÓNICOS

Para restaurar la copia se utiliza la misma utilidad de Windows 10, que restaura todo el sistema de carpetas del cual se ha hecho copia de seguridad.

Procesador	Ram	Disco Duro	Monitor	TAMAÑO	S.O.	OFIMATICA	ANTIVIRUS
					WINDOWS 10	OFFICE 365	KASPERSKY
INTEL CORE I5-6500 3,20 GHz	8 GB	500 GB	HP Compaq LA2306X (x2)	23''	WINDOWS 10	OFFICE 365	KASPERSKY
INTEL CORE 2 6400 2,13 GHz	4 GB	222 GB	HP 1940T	19''	WINDOWS 10	OFFICE 365	KASPERSKY
INTEL CORE 2 6400 2,13 GHz	4 GB	240 GB	HP L1940T	19''	WINDOWS 10	OFFICE 365	KASPERSKY
INTEL CORE I5 5200 2,2 GHz	4 GB	500 GB	HP LE2201W	22''	WINDOWS 10	OFFICE 365	KASPERSKY
INTEL CORE 2 6400 2,13 GHz	4 GB	224 GB	HP V212A	21''	WINDOWS 10	OFFICE 365	KASPERSKY
INTEL CORE 2 DUO E8300 2,83 GHz	2 GB	150 GB	HP 1908WI	19''	WINDOWS 10	OFFICE 365	KASPERSKY
					WINDOWS 10	OFFICE 365	KASPERSKY
INTEL CORE 2 6400 2,13 GHz	2 GB	222 GB	HP LA2205WG	22''	WINDOWS 10	OFFICE 365	KASPERSKY
					WINDOWS 10	OFFICE 365	KASPERSKY
INTEL CORE 2 6400 2,13 GHz	4 GB	232 GB	HP PRO DISPLAY P221	22''	WINDOWS 10	OFFICE 365	KASPERSKY
INTEL CORE 2 6400 2,13GHz	4 GB	240 GB	HP 1901WI	19''	WINDOWS 10	OFFICE 365	KASPERSKY
INTEL CORE I7 7660U 2,50 GHz	16 GB	474 GB	HP E223	22''	WINDOWS 10	OFFICE 365	KASPERSKY
INTEL CORE 2 6400 2,13 GHz	4 GB	222 GB	HP L1908W	19''	WINDOWS 10	OFFICE 365	KASPERSKY
INTEL CORE 2 6400 2,13 GHz	4 GB	232 GB	HP L1940T	19''	WINDOWS 10	OFFICE 365	KASPERSKY
INTEL CORE 2 6400 2,13 GHz	4 GB	222 GB	HP L1940T	19''	WINDOWS 10	OFFICE 365	KASPERSKY
INTEL CORE I5 3470 3,20 GHz	4 GB	80 GB	HP 1940T	19''	WINDOWS 10	OFFICE 365	KASPERSKY
INTEL CORE 2 DUO E8400 3,0GHz	3 GB	232 GB	HP 1908WI	19''	WINDOWS 10	OFFICE 365	KASPERSKY
INTEL CORE 2 6400 2,13 GHz	4 GB	222 GB	HP 1720	17''	WINDOWS 10	OFFICE 365	KASPERSKY
INTEL CORE I3 4130	4 GB	500 GB			WINDOWS 10	OFFICE 365	KASPERSKY
Intel Core i5-6470 3,20 GHz	8 GB	500Gb	Hp EliteDisplay E231 + HP Pavilion 23xi	23''	WINDOWS 10	OFFICE 365	KASPERSKY
					WINDOWS 10	OFFICE 365	KASPERSKY
INTEL CORE 2 6400 2,13 GHz	3 GB	240 GB	HP LE1901WI	19''	WINDOWS 10	OFFICE 365	KASPERSKY
					WINDOWS 10	OFFICE 365	KASPERSKY
INTEL CORE 2 6400 2,13 GHz	4 GB	222 GB	HP ELITE DISPLAY E231	23''	WINDOWS 10	OFFICE 365	KASPERSKY
INTEL CORE I5 7500 3,40 GHz	8 GB	1 TB	HP LA2205WG	22''	WINDOWS 10	OFFICE 365	KASPERSKY
INTEL CORE I5-3470 3,20 GHz	4 GB	237 GB (SSD)	HP LE2201W	22''	WINDOWS 10	OFFICE 365	KASPERSKY
					WINDOWS 10	OFFICE 365	KASPERSKY
INTEL CORE 2 6400 2,13 GHz	4 GB	240 GB	HP L1940T	19''	WINDOWS 10	OFFICE 365	KASPERSKY
INTEL CORE 2 DUO E8300 2,83 GHz	4 GB	150 GB	HP L1940T	19''	WINDOWS 10	OFFICE 365	KASPERSKY
INTEL CORE 2 6300 1,87 GHz	4 GB	250 GB	HP2201W	22''	WINDOWS 10	OFFICE 365	KASPERSKY
INTEL CORE I3 M350 2,27GHz	3 GB	280 GB	HP LE2201W	22''	WINDOWS 10	OFFICE 365	KASPERSKY
					WINDOWS	OFFICE 365	KASPERSKY

					10		
					WINDOWS 10	OFFICE 365	KASPERSKY
					WINDOWS 10	OFFICE 365	KASPERSKY
					WINDOWS 10	OFFICE 365	KASPERSKY
INTEL ORE I5-2400 2,60 GHz	4GB	458 GB	HP 2311X	23''	WINDOWS 10	OFFICE 365	KASPERSKY
INTEL CORE 2 6400 2,13 GHz	4 GB	222 GB	HP1940T	19''	WINDOWS 10	OFFICE 365	KASPERSKY
INTEL CORE 2 DUO E8300 2,83 GHz	4 GB	150 GB	HP L1940T	19''	WINDOWS 10	OFFICE 365	KASPERSKY
INTEL CORE 2 6400 2,13 GHz	4 GB	240 GB	HP 1940T	19''	WINDOWS 10	OFFICE 365	KASPERSKY
					WINDOWS 10	OFFICE 365	KASPERSKY
INTEL CORE 2 6400 2,13GHz	2 GB	240 GB	HP L1908WI	19''	WINDOWS 10	OFFICE 365	KASPERSKY
Intel Core I5-2400 3,10 GHz	16 GB	459 GB	HP Compaq LA2306x (x2)	23''	WINDOWS 10	OFFICE 365	KASPERSKY
INTEL CORE 2 6400 2,13 GHz	4 GB	240 GB	HP L1940T y HP W2072A	19'' y 20''	WINDOWS 10	OFFICE 365	KASPERSKY
INTEL CORE I5 7500 3,40 GHz	8 GB	1 TB	HP L1908W	19''	WINDOWS 10	OFFICE 365	KASPERSKY
INTEL CORE 2 6400 2,13 GHz	4 GB	240 GB	HP LA1951G	19''	WINDOWS 10	OFFICE 365	KASPERSKY
INTEL CORE 2 6400 2,13 GHz	4 GB	224 GB	HP1940T	19''	WINDOWS 10	OFFICE 365	KASPERSKY
					WINDOWS 10	OFFICE 365	KASPERSKY
INTEL CORE 2 6400 2,13 GHz	1 GB	240 GB	HP L1940T	19''	WINDOWS XP	OFFICE 365	KASPERSKY
INTEL CORE 2 DUO E8400 3,0GHz	1 GB	148 GB	HP L1908W	19''	WINDOWS XP	OFFICE 365	KASPERSKY
INTEL CORE 2 6400 2,13GHz	4 GB	240 GB	HP 1908 WI	19''	WINDOWS 10	OFFICE 365	KASPERSKY
					WINDOWS 10	OFFICE 365	KASPERSKY
INTEL CORE 2 DUO E8300 2,83 GHz	2 GB	150 GB	HP LA2306X	23''	WINDOWS 10	OFFICE 365	KASPERSKY
INTEL CORE 2 6300 1,87 GHz	4 GB	240 GB	HP 1908WI y HP1940T	19'' y 19''	WINDOWS 10	OFFICE 365	KASPERSKY
Intel Pentium 4 CPU 3.20 GHz	1 GB	74.5 GB	HP Compaq LA2205wg	22''	WINDOWS XP		KASPERSKY
INTEL CORE 2 6400 2,13 GHz	4 GB	222 GB	HP L1940T	19''	WINDOWS 10	OFFICE 365	KASPERSKY
Intel(R) Core(TM) i5-3470 CPU @ 3.20GHz	8 GB	455 GB	HP Compaq LA2306x	23''	WINDOWS 10	OFFICE 365	KASPERSKY
CORE i5-7500 3,40 GHz	8 GB	913 GB	HP COMPAQ LA2306x + HP ELITEDISPLAY E232	23''	WINDOWS 10	OFFICE 365	KASPERSKY
INTEL CORE I5-4210M 2,60 GHz	4GB	450 GB		17''	WINDOWS 10	OFFICE 365	KASPERSKY
INTEL CORE 2 DUO E8400 3,0GHz	2 GB	150 GB	HP W2072A	20''	WINDOWS 10	OFFICE 365	KASPERSKY
					WINDOWS 10	OFFICE 365	KASPERSKY
INTEL CORE 2 6400 2,13 GHz	4 GB	222 GB	HP 1908WI	19''	WINDOWS 10	OFFICE 365	KASPERSKY
					WINDOWS 10	OFFICE 365	KASPERSKY
INTEL CORE 2 6400 2.13 GHz	4 GB	240 GB	HP W2072A	20''	WINDOWS 10	OFFICE 365	KASPERSKY
					WINDOWS 10	OFFICE 365	KASPERSKY
INTEL PENTIUM D 3200 GHz	4 GB	232 GB	HP 1740	17''	WINDOWS 10	OFFICE 365	KASPERSKY

					WINDOWS 10	OFFICE 365	KASPERSKY
INTEL CORE 2 6400 2,13 GHz	4 GB	222 GB	HP 1940T	19''	WINDOWS 10	OFFICE 365	KASPERSKY
INTEL CORE 2 DUO E8400 3,0GHz	2 GB	148 GB	HP W2072A (2x)	20''	WINDOWS 10	OFFICE 365	KASPERSKY
INTEL CORE 2 6400 2,13 GHz	4 GB	222 GB	HP 1908WI	19''	WINDOWS 10	OFFICE 365	KASPERSKY
INTEL CORE 2 6400 2,13 GHz	4 GB	240 GB	HP 1908WI	19''	WINDOWS 10	OFFICE 365	KASPERSKY
INTEL CORE 2 6400 2,13GHz	4 GB	240 GB	HP 1940T	19''	WINDOWS 10	OFFICE 365	KASPERSKY
INTEL CORE 2 6400 2,13 GHz	2 GB	240 GB	HP1940T	19''	WINDOWS 10	OFFICE 365	KASPERSKY

ANEXO 4: MODELOS

4.1) Autorización de salidas de datos o soportes.

AUTORIZACIÓN DE SALIDAS DE DATOS O SOPORTES	
Fecha y hora de salida del dato/soporte	
Nombre del Fichero	
Persona responsable	
Cargo/puesto	
Información que contiene	
Destinatario	
Observaciones	
Firma del Responsable de tratamiento	

4.2) Autorización de entradas de datos o soportes.

AUTORIZACIÓN DE ENTRADAS DE DATOS O SOPORTES	
Fecha y hora de entrada del dato/soporte	
Nombre del Fichero	
Persona responsable de la recepción	
Cargo/puesto	
Información que contiene	
Tercero emisor	
Observaciones	
Firma del Responsable de tratamiento	

4.3) Modelo de notificación de incidencias.

NOTIFICACIÓN DE INCIDENCIAS	
Número de incidencia	
Fecha y hora en la que se produjo la incidencia	
Tipo de incidencia	
Fecha de notificación	
Persona que realiza la notificación	
Firma de la persona que realiza la comunicación	

4.4) Modelo de autorización de recuperación de datos.

AUTORIZACIÓN DE RECUPERACIÓN DE DATOS

El responsable, _____ del fichero denominado _____ (nombre del fichero) vista que la incidencia núm. _____ exige proceder a la ejecución de un procedimiento de recuperación de los datos en los términos que se describen en el registro de la misma, procede a autorizar la citada recuperación.

Fdo:

4.5) Modelo de Alta de Responsable del Fichero.

D. CARLOS FOSSATI MEDEL, mayor de edad, declara haber recibido un manual de usuario y haber sido informado de las obligaciones que como usuario del citado sistema le corresponden.

MANUAL DE USUARIO

- **Obligaciones**

⇒ Guardar todos los soportes físicos y/o documentos que contengan información con datos de carácter personal en un lugar seguro, cuando estos no sean usados, fuera de la jornada laboral.
⇒ Guardar el necesario secreto respecto a cualquier tipo de información de carácter personal conocida en función del trabajo desarrollado, incluso una vez concluida la relación laboral con la organización.
⇒ Queda prohibido el traslado de cualquier soporte, listado o documento con datos de carácter personal en los que se almacene información de titularidad de la organización fuera de los locales de la misma, sin autorización previa del Responsable de seguridad.
⇒ Únicamente las personas autorizadas en un listado de accesos podrán introducir, modificar o anular los datos contenidos en los ficheros o documentos objeto de protección. Los permisos de acceso de los usuarios son concedidos por el Responsable de seguridad.
⇒ Comunicar al Responsable de Seguridad, conforme al procedimiento de notificación, las incidencias de seguridad de las que tenga conocimiento.

- **Obligaciones respecto de los ficheros Automatizados**

⇒ Cambiar las contraseñas a petición del sistema.
⇒ Guardar todos los ficheros con datos de carácter personal en la carpeta indicada por el Responsable de Seguridad correspondiente.
⇒ Los usuarios tienen prohibido el envío de información de carácter personal de nivel alto, salvo autorización expresa del Responsable de seguridad.
⇒ Cerrar o bloquear todas las sesiones al término de la jornada laboral.

- **Obligaciones respecto de los ficheros no Automatizados**

⇒ Cerrar con llave las puertas de los despachos al término de la jornada laboral o cuando deba ausentarse temporalmente de esta ubicación, a fin de evitar accesos no autorizados.
⇒ Asegurarse de que no quedan documentos impresos que contengan datos de carácter personal impresos en la bandeja de salida o fax.
⇒ Mantener custodiadas las llaves de acceso a la organización, a sus despachos, armarios y archivadores.

⇒ Guardar todos los soportes físicos o documentos que contengan información con datos de carácter personal en un lugar seguro, cuando estos no sean usados.

El incumplimiento por parte de los usuarios de cualquiera de las obligaciones aquí establecidas será considerado como una falta grave, imponiéndose las sanciones para este tipo de faltas las previstas en la normativa laboral de aplicación a la organización.

Todo lo cual declaro bajo mi responsabilidad en _____ a ___ de _____ del 2019.

Fdo:

4.6) Modelos de solicitud de Ejercicio de Derechos.

Derecho de Acceso

DATOS DEL RESPONSABLE DEL FICHERO

- Nombre/Razón Social:

- Domicilio:

DATOS DEL AFECTADO

D./Dª._____
_____, mayor de edad, con domicilio en la C/_____, nº_____, Localidad_____ , Provincia_____, código postal_____, con D.N.I _____, del que se acompaña fotocopia, por medio del presente escrito manifiesta su deseo de ejercer su derecho de Acceso, de conformidad con lo dispuesto en el artículo 15 del Reglamento (UE) de Protección de Datos 2016/679.

SOLICITA: Que se me facilite el derecho de acceso y toda la información sobre mi persona contenida en el fichero, en el plazo de un mes desde la recepción de esta solicitud, y que se me notifique de forma escrita a la dirección arriba indicada la siguiente información:

-Copia de mis datos personales que son objeto de tratamiento por ese responsable.
-Los fines del tratamiento así como las categorías de datos personales que se traten.
-Los destinatarios o categorías de destinarios a los que se han comunicado mis datos personales, o serán comunicados, incluyendo, en su caso, destinatarios en terceros u organizaciones internacionales.
-Información sobre las garantías adecuadas relativas a la transferencia de mis datos a un tercer país o a una organización internacional, en su caso.
-El plazo previsto de conservación, o de no ser posible, los criterios para determinar este plazo.
-Si existen decisiones automatizadas, incluyendo la elaboración de perfiles, información significativa sobre la lógica aplicada, así como la importancia y consecuencias previstas de dicho tratamiento.
-Si mis datos personales no se han obtenido directamente de mí, la información disponible sobre su origen.
-La existencia del derecho a solicitar la rectificación, supresión o limitación del tratamiento de mis datos personales, o a oponerme a dicho tratamiento. -El derecho a presentar una reclamación ante una autoridad de control.

En _____, a ____ de _____ del _____.

Fdo:

Derecho de Rectificación

DATOS DEL RESPONSABLE DEL FICHERO

- Nombre/Razón Social:

- Domicilio:

DATOS DEL INTERESADO

D./Dª._____ _____, mayor de edad, con domicilio en la C/_____, nº_____, Localidad_____ , Provincia_____, código postal_____, con D.N.I _____, del que se acompaña fotocopia, por medio del presente escrito manifiesta su deseo de ejercer su derecho de Rectificación, de conformidad con lo dispuesto en el artículo 16 del Reglamento (UE) de Protección de Datos 2016/679.

SOLICITA:

⇒ Que se proceda a la efectiva corrección de los datos inexactos relativos a mi persona que se encuentran en sus ficheros.
⇒ Los datos que hay que rectificar se enumeran en la hoja anexa, haciendo referencia a los documentos que se acompañan a esta solicitud y que acreditan, en caso de ser necesario, la veracidad de los nuevos datos.
⇒ Que me comuniquen de forma escrita a la dirección arriba señalada, la rectificación de los datos una vez realizada. Que en caso de que se acuerde que no procede practicar la rectificación solicitada, se me comunique motivadamente a fin de, en su caso, reclamar ante la Autoridad de control que corresponda.

En _____, a ____ de _____ de _____.

Fdo:

Derecho de Supresión

DATOS DEL RESPONSABLE DEL FICHERO

- Nombre/Razón Social:

- Domicilio:

DATOS DEL INTERESADO

D./Dª._____ _____, mayor de edad, con domicilio en la C/_____, nº_____, Localidad_____ , Provincia_____, código postal_____, con D.N.I. _____, del que se acompaña fotocopia, por medio del presente escrito manifiesta su deseo de ejercer su derecho de supresión, de conformidad con lo dispuesto en el artículo 17 del Reglamento (UE) de Protección de Datos 2016/679.

SOLICITA:

- ⇒ Que se proceda a la efectiva supresión en el plazo de diez días a contar desde a recepción de esta solicitud, de cualquier dato relativo a mi persona que se encuentren en sus ficheros al no existir vinculación jurídica o disposición legal que justifique su mantenimiento.
- ⇒ Que me comuniquen de forma escrita a la dirección arriba indicada la cancelación de los datos una vez realizada.

Que los datos a cancelar son los siguientes: _____

En _____, a __ de _____ de _____.

Fdo:

Derecho de Limitación

DATOS DEL RESPONSABLE DEL FICHERO

- Nombre/Razón Social:

- Domicilio:

DATOS DEL INTERESADO

D./Dª._____ _____, mayor de edad, con domicilio en _____,nº_____,localidad_____ _____ , Provincia_____, código postal_____, con D.N.I. _____, del que se acompaña fotocopia, por medio del presente escrito manifiesta su deseo de ejercer su derecho de acceso, de conformidad con lo dispuesto en el artículo 18 del Reglamento (UE) de Protección de Datos 2016/679.

SOLICITA:

Que se me facilite el derecho de limitación de tratamiento de toda la información de que dispongan sobre mi persona contenida en sus ficheros, en el plazo de un mes desde la recepción de esta solicitud y que se me notifique de forma escrita a la dirección arriba indicada.
Que la limitación solicitada corresponde a la siguiente: _____

En _____, a __ de _____ del _____.

Fdo:

Derecho de Oposición

DATOS DEL RESPONSABLE DEL FICHERO

- Nombre/Razón Social:

- Domicilio:

DATOS DEL INTERESADO

D./Dª._____ _____, mayor de edad, con domicilio en la C/_____, nº_____, Localidad_____ , Provincia_____, código postal_____, con D.N.I _____, del que se acompaña fotocopia, por medio del presente escrito manifiesta su deseo de ejercer su derecho de Oposición, de conformidad con lo dispuesto en el artículo 21 del Reglamento (UE) de Protección de Datos 2016/679.

EXPONGO

Describa la situación en la que se produce el tratamiento y enumerar los motivos por los que se opone al mismo. Asimismo se debe acreditar la situación descrita, acompañando copia de documentación:

_____
_____
_____
_____
_____
_____

SOLICITO, que sea atendido mi ejercicio de derecho de oposición en los términos anteriormente expuestos.

En _____, a ____ de _____ de _____.

Fdo:

4.7) Cláusulas de información.

INFORMACIÓN SOBRE PROTECCIÓN DE DATOS A CLIENTES

Nombre del Cliente:

La información de carácter personal por usted comunicada a partir de este momento, y en su caso, durante la duración del servicio prestado, será incluida en un fichero titularidad privada de MARTINEZ CENTRO DE GESTIÓN, S.L. a fin de evacuar las actuaciones que resulten necesarias para el correcto cumplimiento del servicio prestado.

Se han adoptado las medidas de seguridad de protección de los Datos Personales legalmente requeridos en el Reglamento Europeo de Protección de Datos 2016/679 y en la Ley Orgánica de Protección de Datos y garantía de los derechos digitales de fecha 3/2018, de 5 de Diciembre.

Los datos no se cederán a terceros salvo en los casos en que exista una obligación legal. Mientras no nos comunique lo contrario, entenderemos que sus datos no han sido modificados, que se compromete a notificarnos cualquier variación y que tenemos su consentimiento para utilizarlos para las finalidades mencionadas. Procederemos a tratar los datos de manera lícita, leal, transparente, adecuada, pertinente, limitada, exacta y actualizada. Es por ello por lo que nos comprometemos a adoptar todas las medidas razonables para que estos se supriman o rectifiquen sin dilación cuando sean inexactos

Conforme a lo dispuesto en el Reglamento Europeo de Protección de Datos 2016/679, el Cliente podrá ejercitar los derechos de acceso, rectificación, supresión, limitación, y en su caso portabilidad, enviando una solicitud por escrito, acompañada de la fotocopia de su D.N.I., dirigida a C/ ALBACETE, Nº 10 (VALENCIA) . Para el caso de que quiera realizarnos alguna consulta o sugerencia lo puede realizar en la siguiente dirección de correo electrónico: **info@grupo-mcg.es.**

El Cliente autoriza: Al tratamiento de sus datos para los fines que justifican el encargo solicitado así como para poder prestarle los servicios: ☐**SI** ☐ **NO**

Fdo:

INFORMACIÓN NUEVO REGLAMENTO DE PROTECCIÓN DE DATOS A EMPLEADOS

Nombre y Apellidos del Trabajador:

En cumplimiento del Nuevo Reglamento de Protección de datos de carácter personal 2016/679, y en la Ley Orgánica de Protección de Datos y garantía de los derechos digitales de fecha 3/2018, de 5 de Diciembre se le informa que los datos personales que nos ha facilitado, serán (o han sido) incorporados en ficheros titularidad de MARTINEZ CENTRO DE GESTIÓN, S.L. (En adelante, el RESPONSABLE DEL TRATAMIENTO), siendo los datos y finalidades correspondientes a los mismos los que se detallan a continuación:

- **PERSONAL**

En el mismo se almacenan los datos necesarios para la elaboración de las nóminas de los trabajadores y el cálculo de las retenciones correspondientes al IRPF y control de pólizas de seguro contratadas, en su caso, por el RESPONSABLE, transferencias de nóminas, gestión de costes de empresa derivados directamente de su plantilla y control del trabajo.

- **RECURSOS HUMANOS**

Datos relativos a la formación académica, planificación de vacaciones, verificación del cumplimiento de la jornada laboral y horas extras, salarios, ascensos, absentismo, movimiento de plantilla y de sección, altas y bajas de trabajadores en la entidad.

- **PREVENCIÓN DE RIESGOS**

Información relativa al puesto de trabajo y situaciones de riesgo que conlleva el mismo, situación laboral del trabajador, formación recibida en materia de prevención de riesgos, material de protección entregado, cambios de sección del trabajador motivados por causas laborales o no laborales, accidentes laborales producidos –control de siniestralidad- y medidas correctoras tomadas por el RESPONSABLE para evitar su repetición, etc.

- **SERVICIO MÉDICO**

Este fichero contiene la información necesaria para lograr el efectivo control de la vigilancia de la salud de los trabajadores, revisiones periódicas, partes de baja, accidentes laborales... Los datos contenidos en este fichero son tratados, exclusivamente, por personal sanitario o sometido a un estricto deber de secreto, no teniendo el RESPONSABLE acceso a la información almacenada, conforme establece la Ley de Prevención de Riesgos Laborales.

Queda terminantemente prohibida la comunicación de los datos objeto de tratamiento, a terceras personas, salvo las legalmente establecidas o las necesarias para el cumplimiento de las finalidades de la relación contractual.

La información de salud facilitada directamente por el trabajador o indirectamente a través de la Mutua de accidentes de trabajo y Enfermedades Profesionales que se encargue a su vez de la vigilancia de la salud, será incluida en un fichero titularidad del RESPONSABLE y tratado por la Mutua o empresa que en esos momentos preste el servicio con el objeto de cumplir con las finalidades anteriormente detalladas.

La información obtenida de las pruebas médicas a las que sea sometido el trabajador será comunicada al RESPONSABLE, a fin de que proceda a la emisión del correspondiente informe de aptitud, y a efectos de un seguimiento y control de las prestaciones.

Los datos económicos de su nómina serán cedidos a la entidad financiera con la que el RESPONSABLE trabaje, para el correspondiente pago de nóminas a los trabajadores.

La información de carácter fiscal y laboral recabada será comunicada a la Agencia Tributaria, Seguridad Social e INEM en los supuestos exigidos por la normativa aplicable.

Si durante la vigencia de la relación laboral con el RESPONSABLE, Ud. es seleccionado para asistir a cursos de formación, sus datos personales serán cedidos al centro correspondiente donde se impartirán los mismos, a efectos de mantener un control de los asistentes y un adecuado desarrollo del curso.

Se le informa que conforme a lo dispuesto en el Reglamento de Protección de Datos 2016/679, está obligado a informar de las variaciones que puedan experimentar sus datos facilitados. Asimismo, y si quiere ejercer sus derechos de acceso rectificación, cancelación u oposición, puede hacerlo enviando una solicitud dirigida a la siguiente dirección C/ ALBACETE, Nº 10 (VALENCIA) .

Fecha y Firma:

INFORMACIÓN SOBRE PROTECCIÓN DE DATOS EN EL CORREO ELECTRÓNICO

De conformidad con lo establecido en la normativa vigente en Protección de Datos de Carácter Personal, le informamos que sus datos serán incorporados al sistema de tratamiento titularidad de MARTINEZ CENTRO DE GESTIÓN, S.L. con NIF B46953170 y domicilio social en C/ ALBACETE, Nº 10 (VALENCIA) (España) con la finalidad de atender su solicitud de información sobre nuestros servicios.

Conservaremos sus datos mientras se mantenga la finalidad para la que han sido recabados. Mientras no nos comunique lo contrario, entenderemos que sus datos no han sido modificados, que se compromete a notificarnos cualquier variación y que tenemos su consentimiento para utilizarlos para las finalidades mencionadas.

Procederemos a tratar los datos de manera lícita, leal, transparente, adecuada, pertinente, limitada, exacta y actualizada. Es por ello por lo que nos comprometemos a adoptar todas las medidas razonables para que estos se supriman o rectifiquen sin dilación cuando sean inexactos.

De acuerdo con los derechos que te confiere la normativa vigente en protección de datos podrá ejercer los derechos de acceso, rectificación, supresión, revocación, portabilidad, oposición y limitación de tratamiento, recogidos en el RGPD (UE) 2016/679 y en la Ley Orgánica de Protección de Datos y garantía de los derechos digitales de fecha 3/2018, de 5 de Diciembre, mediante correo electrónico o correo ordinario a nuestro domicilio social o por cualquier otro medio que permita reconocer la identidad del cliente que ejercite cualquiera de los anteriores derechos.

Consulte todas las formas de contacto, el aviso legal y la cláusula informativa sobre protección de datos en: **www.grupo-mcg.es**

INFORMACIÓN SOBRE PROTECCIÓN DE DATOS EN FACTURAS

Sus datos serán incorporados al sistema de tratamiento titularidad de MARTINEZ CENTRO DE GESTIÓN, S.L. con las finalidades de atender su solicitud de información sobre nuestros servicios y su facturación.

Conservaremos sus datos mientras se mantenga la finalidad para la que han sido recabados. Mientras no nos comunique lo contrario, entenderemos que sus datos no han sido modificados, que se compromete a notificarnos cualquier variación y que tenemos su consentimiento para utilizarlos para las finalidades mencionadas. Procederemos a tratar los datos de manera lícita, leal, transparente, adecuada, pertinente, limitada, exacta y actualizada. Es por ello por lo que nos comprometemos a adoptar todas las medidas razonables para que estos se supriman o rectifiquen sin dilación cuando sean inexactos.

De acuerdo con los derechos que te confiere la normativa vigente podrá ejercer los derechos de acceso, rectificación, supresión, revocación, portabilidad, oposición y limitación de tratamiento, recogidos en el RGPD (UE) 2016/679 y en la Ley Orgánica de Protección de Datos y garantía de los derechos digitales de fecha 3/2018, de 5 de Diciembre, mediante correo electrónico o correo ordinario a nuestro domicilio social o por cualquier otro medio que permita reconocer la identidad del cliente o usuario que ejercite cualquiera de los anteriores derechos. Consulte todas las formas de contacto y el aviso legal en **www.grupo-mcg.es**

ACUERDO DE CONFIDENCIALIDAD Y DEBER DE SECRETO DE LOS EMPLEADOS/PERSONAS CON ACCESO A DATOS

En _____, a___ de _____ del _____,

De una parte, ANTONIO MARTÍNEZ FERRERO, en nombre y representación de MARTINEZ CENTRO DE GESTIÓN, S.L. provisto de N.I.F. B46953170 y con domicilio fiscal en C/ ALBACETE, Nº 10 (VALENCIA), en adelante el Responsable del Fichero.

Y de otra parte_____, mayor de edad y titular del D.N.I._____ en adelante el TRABAJADOR.

MANIFIESTAN

I.- Que en virtud de la prestación de servicios profesionales que el TRABAJADOR viene realizando a favor del Responsable del Fichero, el TRABAJADOR puede tener acceso a recursos donde se contiene información relativa a datos de carácter personal.

II.- Que de conformidad con el nuevo Reglamento de Protección de Datos 2016/679, y en la Ley Orgánica de Protección de Datos y garantía de los derechos digitales de fecha 3/2018, de 5 de Diciembre, quienes intervienen en cualquier fase del tratamiento de los datos de carácter personal están obligados al secreto profesional respecto de los mismos y al deber de custodiarlos.

III.- Que a tales efectos, el TRABAJADOR viene obligado a cumplir y respetar el presente ACUERDO DE CONFIDENCIALIDAD Y DEBER DE SECRETO, el cual expresamente acepta mediante la suscripción de este documento, compuesto de las siguientes,

OBLIGACIONES

PRIMERA.- Cumplir con las normas y políticas determinadas por el RESPONSABLE DEL FICHERO que afectan al desarrollo de sus funciones, así como todas aquellas medidas de seguridad, técnicas u organizativas que el RESPONSABLE DEL FICHERO establezca para garantizar la confidencialidad y deber de secreto de toda información que tenga la consideración de información confidencial. A los efectos antedichos, el RESPONSABLE DEL FICHERO pone en conocimiento del trabajador que por información confidencial se entenderá toda información numérica, alfabética, gráfica, fotográfica, visual acústica o de cualquier otro topo, susceptible de tratamiento que permita identificar directa o indirectamente la identidad de la persona física afectada.

SEGUNDA.- Acceder a la información confidencial del RESPONSABLE DEL FICHERO contenida, tanto en el sistema informática, como en cualquier otro soporte, solo si tal acceso fuera necesario para la prestación de los servicios para los que ha sido contratado.

TERCERA.- El TRABAJADOR se compromete a mantener en el más estricto secreto profesional toda la información confidencial que pueda llegar a su conocimiento como consecuencia de sus funciones dentro de la organización empresarial, comprometiéndose el TRABAJADOR a no divulgarla, publicarla, cederla o ponerla a disposición de terceros, ni siquiera de sus propios familiares ni otros trabajadores de la empresa que no estén autorizados a acceder a la citada información, cualquiera que sea el soporte en el que se encuentre la información.

CUARTA.- La duración de las obligaciones contenidas en este acuerdo es de carácter indefinido y se mantendrá en vigor incluso con posterioridad a la finalización, por cualquier causa, de la relación entre TRABAJADOR Y RESPONSABLE DEL FICHERO, por lo que el trabajador garantiza que, tras la terminación de la relación, guardará el mismo secreto profesional respecto de la información confidencial y de los datos de carácter personal a que haya tenido lugar durante el desempeño de sus funciones.

De conformidad con lo expuesto, el TRABAJADOR declara haber leído y comprendido en su totalidad el contenido del presente documento, y acepta su cumplimiento. Y para que así conste, se extiende este acuerdo en dos ejemplares, en el lugar y fecha arriba indicados.

Fdo: _____

EL TRABAJADOR

INFORMACIÓN SOBRE PROTECCIÓN DE DATOS A INCLUIR EN DOCUMENTOS

MARTINEZ CENTRO DE GESTIÓN, S.L., ha adoptado las medidas y niveles de seguridad de protección de los datos personales exigidos por el Reglamento de Protección de Datos de Carácter Personal 2016/679 y en la Ley Orgánica de Protección de Datos y garantía de los derechos digitales de fecha 3/2018, de 5 de Diciembre.

Los datos personales proporcionados por usted son objeto de tratamiento tanto automatizado como no automatizado y se incorporan a un fichero titularidad de MARTINEZ CENTRO DE GESTIÓN, S.L., que es asimismo la entidad responsable del mismo.

Usted podrá ejercitar los derechos de acceso, rectificación, cancelación y en su caso, oposición, enviando una solicitud por escrito, dirigida a C/ ALBACETE, Nº 10 (VALENCIA).

Para el caso de que quiera realizarnos alguna consulta o sugerencia lo puede realizar en la siguiente dirección de correo electrónico: info@grupo-mcg.es.

Consulte nuestro aviso legal en la página web: https://www.grupo-mcg.es

ALTA PERSONAL INFORMÁTICO

D/Dña: _____ (nombre del personal informático) mayor de edad, por la presente declara haber sido formado e informado de las obligaciones que como usuario del citado sistema me corresponden de conformidad con el nuevo de Protección de Datos 2016/679 y en la Ley Orgánica de Protección de Datos y garantía de los derechos digitales de fecha 3/2018, de 5 de Diciembre.

Corresponde al Personal Informático:

Debido al especial acceso que tiene el persona informático se le atribuyen unas responsabilidades complementarias:

1. Guardar secreto de toda la información de carácter personal, o que afecte a ésta, de la que tenga conocimiento en el desarrollo de su de trabajo, aún después de acabada la relación con la organización.

2. Aunque debido a sus funciones disponga de un acceso privilegiado a ciertos recursos, se compromete a acceder únicamente a los datos necesarios para desarrollar sus funciones.

3. En el caso que detecten, deficiencias de seguridad en el sistema de información, lo deberán comunicar al Responsable de Seguridad correspondiente.

4. Colaborar con el Responsable/s de Seguridad en la resolución de las incidencias que se le encarguen.

5. Desempeñar sus funciones con estricta observancia de las obligaciones dispuestas por la legislación sobre protección de datos.

El incumplimiento por parte del mismo de las obligaciones aquí establecidas será considerado como una falta grave, imponiéndose las sanciones previstas para este tipo de faltas especificadas en la normativa laboral o funcionarial de aplicación al responsable del fichero.

Todo lo cual declaro bajo mi responsabilidad, en_____, a ____ de _____ del _____

Fdo:

AUTORIZACIÓN DE SALIDAS Y ENTRADAS DE DATOS

AUTORIZACIÓN DE SALIDAS DE DATOS O SOPORTES	
Fecha y hora de salida del dato/soporte	
Nombre del Fichero	
Persona responsable	
Cargo/puesto	
Información que contiene	
Destinatario	
Observaciones	
Firma del Responsable de Tratamiento	

AUTORIZACIÓN DE ENTRADAS DE DATOS O SOPORTES	
Fecha y hora de entrada del dato/soporte	
Nombre del Fichero	
Persona responsable de la recepción	
Cargo/puesto	
Información que contiene	
Tercero emisor	
Observaciones	
Firma del Responsable de Tratamiento	

CLAUSULA INFORMACIÓN CANDIDATOS

Nombre de la empresa: MARTINEZ CENTRO DE GESTIÓN, S.L., con NIF: B-97914766 Dir. Postal: C/ ALBACETE, Nº 10 (VALENCIA) Teléfono: 963172254 y correo electrónico: info@grupo-mcg.es.

En nombre de la empresa tratamos la información que nos facilita con el fin de mantenerle informado de las distintas vacantes a un puesto de trabajo que se produzcan en nuestra organización. Los datos proporcionados se conservarán hasta la adjudicación de un puesto de trabajo o hasta que usted ejerza su derecho de cancelación por tanto tiene derecho a acceder a sus datos personales, rectificar los datos inexactos o solicitar su supresión cuando los datos ya no sean necesarios. Los datos no se cederán a terceros.

Fdo: _____

4.8) Modelos de Contratos de Acceso a Datos por Cuenta de Terceros.

En _____, a ____ de _____ del _____.

REUNIDOS

De una parte, ANTONIO MARTÍNEZ FERRERO, en nombre y representación de MARTINEZ CENTRO DE GESTIÓN, S.L. provisto de N.I.F. B97914766 y con domicilio fiscal en C/ ALBACETE, Nº 10 (VALENCIA) , en adelante el Responsable del Fichero.

Y de otra, _____, con N.I.F. _____y domicilio, a efectos del presente contrato, en _____, en adelante, el Encargado del tratamiento.

INTERVIENEN

Ambas partes se declaran, según intervienen, con capacidad suficiente para suscribir el presente **CONTRATO DE ACCESO A DATOS POR CUENTA DE TERCEROS,** y puestas previamente de acuerdo,

MANIFIESTAN

I.- Que el Encargado del tratamiento se halla, en la actualidad, prestando determinados servicios que se detallan a continuación.

II.- Para el correcto cumplimiento de estos servicios, el Encargado trata datos de carácter personal titularidad del Responsable del fichero.

III.- En cumplimiento de lo dispuesto en el Reglamento de Protección de Datos 2016/679 (en adelante, RGPD), y en la Ley Orgánica de Protección de Datos y garantía de los derechos digitales de fecha 3/2018, de 5 de Diciembre, es intención de ambas partes establecer las obligaciones y responsabilidades que corresponden a cada una de ellas en el tratamiento de los datos de carácter personal, con arreglo a las siguientes,

ESTIPULACIONES

PRIMERA.- Objeto del encargo del tratamiento

Mediante las presentes cláusulas se habilita al Encargado del Tratamiento para tratar por cuenta del Responsable del tratamiento, los datos de carácter personal necesarios para prestar el servicio que en adelante se especifican**.**

El tratamiento consistirá en:

☐ Recogida Registro ☐ Contabilidad

☐ Conservación Extracción ☐ Fiscalidad

☐ Difusión Interconexión ☐ Destrucción de Papel

☐ Supresión Destrucción ☐ Prevención de Riesgos Laborales

☐ Asesoramiento laboral, gestión de nóminas, contratos y representación ante la Seguridad Social.

Otros:.....

SEGUNDA.- Identificación de la información afectada

Para la ejecución de las prestaciones derivadas del cumplimiento del objeto de este encargo, el responsable del tratamiento, pone a disposición del Encargado del Tratamiento la información disponible en los equipos informáticos que dan soporte a los tratamientos de datos realizados por el responsable.

TERCERA.- Duración

El presente acuerdo tiene una duración de _____, renovable ☐**SI** ☐**NO**
Una vez finalice el presente contrato, el encargado del tratamiento debe devolver al responsable los datos personales, y suprimir cualquier copia que mantenga en su poder. No obstante, podrá mantener bloqueados los datos para atender posibles responsabilidades administrativas o jurisdiccionales.

CUARTA.- Obligaciones del encargado del tratamiento

El encargado del tratamiento y todo su personal se obliga a:

- ✓ Utilizar los datos personales a los que tenga acceso sólo para la finalidad objeto de este encargo. En ningún caso podrá utilizar los datos para fines propios.
- ✓ Tratar los datos de acuerdo con las instrucciones del responsable del tratamiento.

  Si el encargado del tratamiento considera que alguna de las instrucciones infringe el RGPD o cualquier otra disposición en materia de protección de datos, el encargado informará inmediatamente al responsable.
- ✓ No comunicar los datos a terceras personas, salvo que cuente con la autorización expresa del responsable del tratamiento, en los supuestos legalmente admisibles.
- ✓ Mantener el deber de secreto respecto a los datos de carácter personal a los que haya tenido acceso en virtud del presente encargo, incluso después de que finalice el contrato.
- ✓ Garantizar que las personas autorizadas para tratar datos personales se comprometan, de forma expresa y por escrito, a respetar la confidencialidad y a cumplir las medidas de seguridad correspondientes, de las que hay que informarles convenientemente.
- ✓ Mantener a disposición del responsable la documentación acreditativa del cumplimiento de la obligación establecida en el apartado anterior.

- ✓ Garantizar la formación necesaria en materia de protección de datos personales de las personas autorizadas para tratar datos personales.
- ✓ Notificación de violaciones de la seguridad de los datos

  El encargado del tratamiento notificará al responsable del tratamiento, sin dilación indebida y a través de la dirección de correo electrónico que le indique el responsable, las violaciones de la seguridad de los datos personales a su cargo de las que tenga conocimiento, juntamente con toda la información relevante para la documentación y comunicación de la incidencia.

  Se facilitará, como mínimo, la información siguiente:

  a) 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.

  b) Datos de la persona de contacto para obtener más información.

  c) Descripción de las posibles consecuencias de la violación de la seguridad de los datos personales. Descripción de las medidas adoptadas o propuestas 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.

     Si no es posible facilitar la información simultáneamente, y en la medida en que no lo sea, la información se facilitará de manera gradual sin dilación indebida.

- ✓ Poner disposición del responsable toda la información necesaria para demostrar el cumplimiento de sus obligaciones, así como para la realización de las auditorías o las inspecciones que realicen el responsable u otro auditor autorizado por él.
- ✓ Auxiliar al responsable de tratamiento a implantar las medidas de seguridad necesarias para:

  a) Garantizar la confidencialidad, integridad, disponibilidad y resiliencia permanentes de los sistemas y servicios de tratamiento.

  b) Restaurar la disponibilidad y el acceso a los datos personales de forma rápida, en caso de incidente físico o técnico.

  c) Verificar, evaluar y valorar, de forma regular, la eficacia de las medidas técnicas y organizativas implantadas para garantizar la seguridad del tratamiento.

- ✓ Destino de los datos

  El responsable del tratamiento no conservará datos de carácter personal relativos a los tratamientos del encargado salvo que sea estrictamente necesario para la prestación del servicio, y solo durante el tiempo estrictamente necesario para su prestación.

QUINTA.- Obligaciones del responsable del tratamiento

Corresponde al responsable del tratamiento:

a) Facilitar al encargado el acceso a los equipos a fin de prestar el servicio contratado.

b) Velar, de forma previa y durante todo el tratamiento, por el cumplimiento del RGPD por parte del encargado.

c) Supervisar el tratamiento.

SEXTA.- Finalidad que justifica el tratamiento

Queda terminantemente prohibida la aplicación o utilización de los datos contenidos en estos ficheros con fines distintos a los aquí previstos, salvo autorización expresa, manifestada por escrito, del Responsable. Se prohíbe, asimismo, la comunicación de los datos objeto de tratamiento, ni siquiera para su conservación a otras personas, salvo las cesiones legalmente establecidas y las que resulten necesarias para el cumplimiento de las finalidades de la relación contractual.

TRATAMIENTO REALIZADO POR EL ENCARGADO:	
DATOS PERSONALES QUE CONTIENE:	
FINALIDAD QUE JUSTIFICA EL TRATAMIENTO:	

Fdo.: _____ POR EL RESPONSABLE	Fdo.: _____ POR EL ENCARGADO

NOTAS