# ADENDA DE ACUERDO DE CONFIDENCIALIDAD, USO DE LAS COMUNICACIONES Y MEDIDAS GENERALES DE SEGURIDAD APLICABLES AL TRATAMIENTO EN EL CONTRATO ENTRE MUTUA MONTAÑESA, MUTUA COLABORADORA CON LA SEGURIDAD SOCIAL Nº 7 Y ………., PARA LA PRESTACIÓN DE LOS SERVICIOS DE …………..

**Mutua Montañesa,** como organización que maneja datos confidenciales y de carácter personal, debe establecer los principios de actuación que le permitan mantener la debida confidencialidad e integridad de los recursos de información almacenados en cualquier tipo de soporte.

Los recursos de información se encuentran sujetos a amenazas generadas por diferentes tipos de riesgos a los que están expuestos. Por lo tanto es necesario implementar controles para prevenir, detectar o corregir los ataques de las amenazas y para disminuir los riesgos. Muchos de los controles deben ser aplicados por parte de todos los profesionales, dado que conductas negligentes o permisivas por parte de cada uno de ellos pueden generar a **Mutua Montañesa**:

* Pérdida de integridad de la información.
* Pérdida de confidencialidad de los datos.
* Incumplimientos de GDPR.
* Problemas con el funcionamiento de la Red Corporativa o con el propio equipo
* Perjuicios económicos (sanciones de la Administración, inspecciones de la AEPD,…).
* Pérdida de productividad en todos los puestos.

**Normas de uso y obligaciones que tiene el usuario de los sistemas de información**

En relación a la confidencialidad de los datos a los que está teniendo acceso dentro del desarrollo y cumplimiento del contrato de arrendamiento de servicios profesionales o acuerdo de colaboración que vincula a la empresa/organismo abajo consignada y Mutua Montañesa se le informa que:

1. Los datos a los que está teniendo acceso son propiedad de Mutua Montañesa. No se encuentra permitido sacar de las instalaciones y oficinas información, ya sea impresa en papel o mediante soporte informático, con datos de carácter personal y/o confidenciales propiedad de Mutua Montañesa, salvo autorización por el Responsable (\*).
2. Las claves de acceso al sistema informático de Mutua Montañesa que le han podido ser facilitadas por nuestros servicios técnicos son personales, intransferibles y secretas.
3. Esto significa que no se puede comunicar en ningún caso a otras personas dicha información.
4. El puesto de trabajo se encuentra bajo la responsabilidad del propio usuario, siendo su obligación el que la información que obre en su poder no pueda ser visible por personal no autorizado.

El responsable del fichero (Mutua Montañesa) y quienes intervengan en cualquier fase del tratamiento de los datos de  carácter personal están obligados al **secreto** **profesional** respecto a los mismos y al deber de guardarlos, obligaciones que subsistirán aun después de  finalizar sus relaciones con el titular del fichero, o en su caso con el responsable del mismo.

1. Está terminantemente prohibido acceder a bases de datos, ficheros o información que no tenga relación directa con el trabajo encomendado, aún cuando físicamente el nivel de autorización lo permita.
2. Existe obligación de comunicar con inmediatez a Mutua Montañesa cualquier incidencia que afecte a la seguridad o a la debida conservación de los datos de carácter personal y de los ficheros que contengan los mismos.
3. Se aplicarán las normas de seguridad y directrices que nos indique, verbalmente o por escrito, Mutua Montañesa. Cualquier vulneración de dichas directrices será exclusivamente responsabilidad del propio usuario.
4. da totalmente prohibido suministrar datos confidenciales y de carácter personal[[1]](#footnote-1) tanto a profesionales de Mutua Montañesa como a los clientes, excepto los casos que las peticiones vengan por parte del responsable[[2]](#footnote-2) o se encuentren dentro de las funciones encomendadas al profesional por parte de Mutua Montañesa.
5. Una vez terminada la relación de servicios para Mutua Montañesa no podrá hacer uso de la información propiedad de Mutua Montañesa ni de las claves de acceso que se le han facilitado.

Las actividades dentro de los sistemas de **Mutua Montañesa** se encuentran sujetas al control y registro por parte del personal Administrador.

# PROTECCIÓN DE DATOS DE CARÁCTER PERSONAL

En cumplimiento del Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016 (Reglamento General de Protección de Datos), le informamos que sus datos personales serán tratados por:

Responsable del Tratamiento de Datos: MUTUA MONTAÑESA, Mutua colaboradora de la Seguridad Social nº 7.CIF: G39008321

Domicilio social: calle Ataúlfo Argenta, 19, 39004. Santander.

Delegado de Protección de Datos: [lopd@mutuamontanesa.es](mailto:lopd@mutuamontanesa.es)

**Finalidad del tratamiento:** Le informamos que los datos personales facilitados por usted en este documento serán susceptibles de tratamiento estrictamente confidencial con la única finalidad de proceder a facilitar su acceso a aquellas aplicaciones corporativas de Mutua Montañesa que resulten estrictamente necesarias para la consecución del proyecto en el cual usted o su empresa figuren como proveedores o colaboradores de Mutua Montañesa.

Le informamos que sobre la base de estos datos no se elaborarán perfiles ni se tomarán decisiones automatizadas.

**Conservación de los datos**: Los datos proporcionados se conservarán mientras se mantenga la relación contractual y ejecución del proyecto o colaboración. Una vez finalizado serán destruidos y se inhabilitarán, en su caso, las claves de acceso y usuarios que se hayan podido facilitar.

**Base legal:** La base legal para el tratamiento de sus datos personales reside en la ejecución de contrato, y/o acuerdo de colaboración para la ejecución del proyecto.

**Destinatarios:** Adicionalmente se le informa que el responsable del fichero, en el marco de la finalidad anteriormente indicada, no cederá sus datos a terceros.

**Derechos:** Tiene el derecho de acceder a sus datos y solicitar la rectificación y/o borrado de los datos personales o la restricción del tratamiento de éstos. Asimismo, tiene derecho a oponerse al tratamiento de sus datos y a solicitar su la portabilidad.

Para ejercer sus derechos, puede contactar con el Delegado de Protección de Datos mediante carta dirigida a C/Ataulfo Argenta 19 -39004 Santander-, o al email [dpo@mutuamontanesa.es](mailto:dpo@mutuamontanesa.es).

Tiene el derecho de presentar una reclamación a la Autoridad de Control, esto es, la Agencia Española de Protección de Datos, a la cual puede acceder mediante el siguiente enlace: <https://www.agpd.es/portalwebAGPD/CanalDelCiudadano/derechos/index-ides-idphp.php>

# MEDIDAS GENERALES DE SEGURIDAD APLICABLES AL TRATAMIENTO

Sin perjuicio de lo previsto en la Adenda sobre el tratamiento de datos del Anexo III, el responsable del tratamiento mediante el presente documento da traslado e informa al encargado del tratamiento de sus estándares generales de seguridad, de forma que el encargado del tratamiento queda obligado a aplicar como mínimo aquellas medidas de seguridad que correspondan en función del riesgo de los tratamientos llevados a cabo por el mismo y las obligaciones asumidas en virtud de las estipulaciones del contrato principal y la señalada Adenda sobre el tratamiento de datos

1. **MEDIDAS COMUNES**

Independientemente de si el tratamiento se realiza en centros del responsable del tratamiento o bien en centros del encargado del tratamiento, éste deberá en ambos casos cumplir las siguientes medidas:

1. Registro de actividades de tratamiento. Llevar un registro de todas las categorías de actividades de tratamiento efectuadas por cuenta de Mutua Montañesa, conforme artículo 30.2 del (RGPD) y artículo 31 de la LOPD.
2. Recursos humanos.
3. Confidencialidad del personal: el encargado se asegura de que todo el personal bajo su dependencia comprenda sus responsabilidades y obligaciones relacionadas con el tratamiento de datos personales, y el deber de confidencialidad y secreto.
4. Formación: el encargado garantiza que todo el “personal autorizado” esté adecuadamente informado y formado sobre los controles de seguridad del sistema de TI y de las medidas de seguridad que le son de aplicación, y las obligaciones legales en materia de protección de datos. Realizando formación específica o campañas de concienciación.
5. Subcontratación

En el caso de que esté autorizada expresamente por el responsable del tratamiento la subcontratación, se deberán cumplir los siguientes requisitos:

1. Comunicar al Área de Protección de Datos de Mutua Montañesa, con carácter previo al inicio de la actividad por el subcontratista/subencargado de tratamiento, su nombre o denominación y la fecha de inicio de la actividad, en dpo@mutuamontanesa.es
2. El subcontratista, que también tendrá la condición de encargado del tratamiento, estará obligado igualmente a cumplir las obligaciones establecidas en este documento para el encargado del tratamiento y las instrucciones que dicte el responsable del tratamiento. Corresponderá al encargado del tratamiento regular contractualmente la nueva relación, de forma que el nuevo encargado del tratamiento (o subencargado) quede sujeto a las mismas condiciones que obran en el presente contrato (instrucciones, obligaciones, medidas de seguridad y resto de condiciones establecidas) y con los mismos requisitos formales que él,

en lo referente al adecuado tratamiento de los datos personales y a la garantía de los derechos de las personas afectadas. En el caso de incumplimiento por parte del subencargado, el encargado del tratamiento inicial seguirá siendo plenamente responsable ante el responsable del tratamiento en lo referente al cumplimiento de las obligaciones y las consecuencias que se deriven del incumplimiento de las mismas.

1. El subencargado deberá cumplir con las presentes medidas de seguridad y así se reflejará en el contrato que firme con el encargado.
2. En el contrato con la subencargado, se debe recoger que el incumplimiento de cualquier obligación contenida en el mismo, dará lugar a la resolución del contrato principal (entre subcontratista/Encargada de Tratamiento-subcontratada).
3. El encargado del tratamiento deberá controlar la calidad y el nivel de cumplimiento de las obligaciones de la subcontratista respecto a los datos personales de Mutua Montañesa, y en concreto a la aplicación de las medidas de seguridad de tratamiento y uso y finalidad de los datos conforme la normativa aplicable en esta materia, con la misma diligencia que debe emplear en el cumplimiento de sus propias obligaciones. Si Mutua Montañesa, como responsable de tratamiento llegara al convencimiento de que la subcontratada no cumple con los requisitos exigibles en cuanto al tratamiento de sus datos personales podrá solicitar al encargado del tratamiento la resolución del contrato con la subcontratista, y en su caso las responsabilidades que se deriven de las obligaciones del presente contrato.
4. Los trabajadores de la subcontratista que vayan a realizar sus servicios y tener acceso a ficheros de Mutua Montañesa, y con carácter previo a empezar el tratamiento de datos, deberán suscribir un compromiso expreso de confidencialidad.

Tanto el contrato como demás documentación que evidencia el cumplimiento de las obligaciones en materia de subcontratación debe estar disponible por si fuera requerida por el responsable de tratamiento, dentro de su función de verificación del cumplimiento de las obligaciones en materia de protección de datos.

1. **MEDIDAS APLICABLES EN CASO DE TRATAMIENTO EN CENTRO O INSTALACIONES DEL RESPONSABLE DE TRATAMIENTO**

No se especifican medidas concretas. El responsable de tratamiento indicará en función del tratamiento que vaya a realizar el encargado del tratamiento, las instrucciones concretas que precise, estableciendo el responsable las medidas de seguridad que procedan.

El encargado del tratamiento deberá cumplir con las instrucciones y procedimientos que le indique el responsable de tratamiento, siendo especialmente diligente con los accesos en remoto, volcado de datos, y las claves de acceso facilitadas para desarrollar el mismo.

1. **MEDIDAS APLICABLES EN CASO DE TRATAMIENTO EN CENTRO O INSTALACIONES PROPIAS DEL ENCARGADO DE TRATAMIENTO**
2. **Medidas de seguridad organizativas.**
   * 1. Gestión de la seguridad
     2. Política de seguridad y procedimientos:
   * El encargado debe documentar una política de seguridad con respecto al tratamiento de los datos personales.
   * Análisis de riesgos relativos al tratamiento objeto de encargo e implantar las medidas técnicas y organizativas de seguridad que resulten de aplicación a la luz de los resultados de dicho análisis. Que en su caso incluya:
   * La seudonimización y el cifrado de datos personales.
   * La capacidad de garantizar la confidencialidad, integridad, disponibilidad y resiliencia permanentes de los sistemas y servicios de tratamiento.
   * La capacidad de restaurar la disponibilidad y el acceso a los datos personales de forma rápida en caso de incidente físico o técnico.
   * Un proceso de verificación, evaluación y valoración regulares de la eficacia de las medidas técnicas y organizativas para garantizar la seguridad del tratamiento.

Al evaluar la adecuación del nivel de seguridad se tendrán particularmente en cuenta los riesgos que presente el tratamiento de datos, en particular como consecuencia de la destrucción, pérdida o alteración accidental o ilícita de datos personales transmitidos, conservados o tratados de otra forma, o la comunicación o accesos no autorizados a dichos datos.

c. Funciones y responsabilidades：

* + Las funciones y responsabilidades relacionadas con el tratamiento de datos personales están claramente definidas y asignadas de acuerdo con la política de seguridad.
  + Durante las reorganizaciones internas o despidos y el cambio de empleo, se define claramente la revocación de los derechos y responsabilidades con los respectivos procedimientos de traspaso.

d. Política de control de acceso: los derechos específicos de control de acceso se asignan a cada función involucrada en el tratamiento de datos personales, siguiendo el principio de “necesidad de saber”.

e. Gestión de recursos / activos: el encargado tiene un registro de los recursos de TI utilizados para el tratamiento de datos personales (hardware, software y red). A una persona específica se le asigna la tarea de mantener y actualizar el registro (por ejemplo, el responsable de TI).

f. Gestión de cambios: el encargado se asegura de que todos los cambios en el sistema de TI sean registrados y supervisados por una persona específica (por ejemplo, un técnico de TI o de seguridad). Se lleva a cabo el seguimiento regular de este proceso.

1. **Respuesta ante incidentes y continuidad de negocio.**
   * 1. Gestión de incidentes/violación de seguridad de datos personales:
   * Se define un plan de respuesta a incidentes con procedimientos detallados para garantizar una respuesta eficaz y ordenada a los incidentes relacionados con los datos personales.
   * El encargado informará sin dilación indebida al responsable de cualquier incidente de seguridad que haya resultado en la pérdida, uso indebido o adquisición no autorizada de datos personales.
     1. Continuidad del negocio: el encargado establece los principales procedimientos y controles que se deben seguir para asegurar el nivel requerido de continuidad y disponibilidad del sistema informático que trata los datos personales (en el caso de un incidente / violación de seguridad de datos personales).
2. **Medidas de seguridad técnicas.**
   * 1. Control de acceso y autenticación:
     + Se implementa un sistema de control de acceso aplicable a todos los usuarios que acceden al sistema de TI. El sistema permite crear, aprobar, revisar y eliminar cuentas de usuario.
     + Se evita el uso de cuentas de usuario comunes. En los casos en que esto sea necesario, se garantiza que todos los usuarios de la cuenta común tengan las mismas funciones y responsabilidades.
     + Al otorgar acceso o asignar funciones de usuario, se debe observar el "principio de necesidad de saber" para limitar el número de usuarios que tienen acceso a datos personales a sólo aquellos que lo soliciten para lograr los propósitos de tratamiento del encargado.
     + Cuando los mecanismos de autenticación se basan en contraseñas, el encargado solicita que la contraseña tenga al menos ocho caracteres de longitud y se ajuste a parámetros de control de contraseñas muy sólidos, como la longitud, la complejidad del carácter y la no repetitividad.
     + Las credenciales de autenticación (como la identificación de usuario y la contraseña) nunca se transmitirán sin protección a través de la red, y son personales y confidenciales, con lo que el usuario no debe comunicarla a nadie.
     + Garantizará que solo acceda a los datos personales el “personal autorizado” para dicho tratamiento, realizando control de accesos informáticos
     1. Registro y seguimiento: los archivos de registro se activan para cada sistema/aplicación utilizada para el tratamiento de datos personales. Incluyen todos los tipos de acceso a datos (vista, modificación, eliminación).
     2. Seguridad de los datos en reposo.

* Seguridad del servidor/base de datos:
* Los servidores de bases de datos y aplicaciones están configurados para ejecutarse utilizando una cuenta separada, con privilegios mínimos de sistema operativo para funcionar correctamente.
* Los servidores de bases de datos y aplicaciones sólo tratan los datos personales que realmente se necesitan para lograr sus fines de tratamiento.
* Se implementan medidas de índole técnica y organizativas necesarias que garanticen la seguridad de los datos personales y eviten su alteración, pérdida, tratamiento o acceso no autorizado, habida cuenta del estado de la tecnología, la naturaleza de los datos almacenados y los riesgos a que están expuestos, ya provengan de la acción humana o del medio físico natural.
* Aplicará las medidas necesarias para que ninguna persona no considerada personal autorizado acceda, visualice o trate los datos personales.
  + 1. No comunicará los datos personales a ningún tercero, a excepción de autorización expresa del responsable del tratamiento, y no registrará datos en ficheros que no reúnan las condiciones de seguridad así como deberá poner la debidas medidas de protección y seguridad a su almacenamiento.
    2. Seguridad de la estación de trabajo:
* Los usuarios no pueden desactivar u omitir la configuración de seguridad.
* Las aplicaciones antivirus y las firmas de detección se configuran de forma regular.
* Los usuarios no tienen privilegios para instalar o desactivar aplicaciones de software no autorizadas.
* El sistema tiene tiempos de espera de sesión cuando el usuario no ha estado activo durante un cierto período de tiempo.
* Las actualizaciones de seguridad críticas lanzadas por el desarrollador del sistema operativo se instalan regularmente.
  + 1. Seguridad de red / comunicación:
* Cuando el acceso se realiza a través de Internet, la comunicación se cifra a través de protocolos criptográficos.
* El tráfico hacia y desde el sistema de TI se sigue y controla a través de cortafuegos y sistemas de detección de intrusos.
* En el caso de que se acceda a los datos en remoto, el encargado del tratamiento deberá instruir al personal desplazado sobre las medidas de seguridad establecidas por el Responsable del fichero, además del deber de secreto de las claves facilitadas, y deberá exigir su cumplimiento. Los datos a los que el encargado del tratamiento acceda de forma remota no podrán ser incorporados en soportes o sistemas distintos de los autorizados por el responsable del fichero, y deberán ser descargados siguiendo las instrucciones de seguridad del responsable.
  + 1. Copias de seguridad:
* Los procedimientos de recuperación y restauración de datos están definidos, documentados y claramente vinculados con las funciones y las responsabilidades.
* Las copias de seguridad reciben un nivel apropiado de protección física y ambiental consistente con los estándares aplicados en los datos de origen y se supervisa para garantizar que esté completa
  + 1. Dispositivos móviles/portátiles: Los procedimientos de administración de dispositivos portátiles y móviles se definen y documentan estableciendo reglas claras para su uso adecuado. Los dispositivos móviles que tienen permiso para acceder al sistema de información están pre registrados y pre autorizados.
    2. Seguridad del ciclo de vida de la aplicación: Durante el ciclo de vida del desarrollo, se siguen las mejores prácticas, el estado del arte y las prácticas o estándares de desarrollo seguros reconocidos.
    3. Borrado/eliminación de datos:
* La sobrescritura basada en software se realizará en los medios antes de su eliminación. En los casos en que esto no sea posible (CDs, DVDs, etc.), se realizará una destrucción física.
* Se lleva a cabo la trituración de papel y medios portátiles utilizados para almacenar datos personales.

1. Seguridad física: el personal no autorizado no puede acceder al perímetro físico de la infraestructura del sistema de TI. Se deben establecer medidas técnicas apropiadas (por ejemplo, sistema de detección de intrusión, torniquete operado con tarjeta chip, sistema de entrada de seguridad de una sola persona, sistema de cierre) o medidas organizativas (por ejemplo, guardia de seguridad) para proteger las áreas de seguridad y sus puntos de acceso personas no autorizadas.

**MUTUA MONTAÑESA, MCSS Nº 7 …………………………………….**

1. Datos confidenciales y de carácter personal: datos que sean propiedad de **Mutua Montañesa** o que contengan cualquier información concerniente a personas físicas identificadas o identificables (DNI, nombre, apellidos, etc., con especial hincapié en la gestión de los datos de salud). [↑](#footnote-ref-1)
2. Responsable. Puede ser cualquiera de los siguientes puestos:

   * Responsable de seguridad.
   * Analista responsable.
   * Coordinador de los Servicios de desarrollo o comunicaciones y microinformática..
   * Responsable del fichero (coordinador de Afiliación, Prestaciones, etc.) o personas en que deleguen los mismos.

   [↑](#footnote-ref-2)