ADENDA SOBRE TRATAMIENTO DE DATOS CON CESIÓN DE DATOS

La presente Adenda sobre tratamiento de datos (“**Adenda**”) forma parte del **“CONTRATO ENTRE MUTUA MONTAÑESA, Mutua Colaboradora con la Seguridad Social, núm.7 y………………………..,PARA CONTRATACION DEL SERVICIO DE ……………….. PARA MUTUA MONTAÑESA”** de (“**Contrato Marco**”), de fecha …………………:

De una parte,

D. Alberto Martínez Lebeña, con N.I.F. 20.194.295-L, en nombre y representación de **MUTUA MONTAÑESA**, Mutua colaboradora con la Seguridad Social Nº 7 (en adelante Mutua Montañesa), con C.I.F. nº G-39008321, en calidad de Director Gerente, y con domicilio social en Santander, calle Ataúlfo Argenta, 19; y de conformidad con los poderes conferidos el día 6 de septiembre de 2021, protocolizados ante el Notario de Santander, D. Iñigo Girón Sierra, con el número 2.344 de su protocolo,

Y de otra,

D/Dña………………, con DNI ………, en nombre y representación de la compañía mercantil **………………** domiciliada en ………….(CP……..), C/ ……………………, Nº……, piso……, con CIF……………., en su condición de …………, en virtud de la escritura que tiene otorgada ante el/la Notario/a de ……….., D/Dña………………, el día ………. de………..de ……., con número ………. de su protocolo y debidamente inscrita en el Registro Mercantil de …….; (En adelante el “Encargado del Tratamiento”)

Mutua Montañesa y el Encargado del Tratamiento en adelante se denominarán conjuntamente como las “**Partes**”.

Los términos empleados en esta Adenda tendrán el significado que se establezca en la misma. Los términos en mayúscula cuya definición no figure en el presente documento tendrán el significado que se les atribuye en el Contrato Marco. Salvo que se modifiquen según lo expuesto a continuación, los términos del Contrato Marco permanecerán con pleno vigor y efecto.

En consideración a las obligaciones mutuas establecidas en el presente documento, las partes acuerdan por el presente que los términos y condiciones establecidos a continuación se añadan al Contrato Marco a modo de Adenda.

1. **Definiciones**

A efectos de la presente Adenda, los términos y expresiones expuestos a continuación tendrán el significado siguiente:

* 1. “**ATD**” se refiere al presente Adenda de Tratamiento de Datos.
  2. “**Legislación Aplicable**” se refiere a leyes de la Unión Europea o españolas en materia de protección de datos.
  3. “**Subencargado(s) autorizado(s)**” se refiere a cualquier persona o tercero nombrado por el Encargado del Tratamiento o por alguien en su nombre y que Mutua Montañesa haya aprobado expresamente, estando dicha autorización sujeta al estricto cumplimiento de la presente Adenda sobre protección de datos.
  4. “**Datos Personales de Mutua Montañesa**” hace referencia a cualesquiera Datos Personales tratados por cuenta de Mutua Montañesa por un Encargado del Tratamiento contratado y de conformidad o en relación con el Contrato Marco y la presente Adenda.
  5. “**Encargado del Tratamiento contratado**” se refiere al Encargado del Tratamiento o a un Subencargado autorizado.
  6. “**Legislación en materia de protección de datos**” se refiere a la Legislación en materia de protección de datos de la UE y, en la medida en que sea aplicable, a la legislación sobre protección de datos y privacidad de cualquier otro país.
  7. “**EEE**” se refiere al Espacio Económico Europeo.
  8. “**Legislación en materia de protección de datos de la UE**” se refiere a la Directiva 95/46/CE de la UE, según se haya transpuesto a la legislación nacional de cada Estado miembro y con las oportunas enmiendas, sustituciones o reemplazos, incluido el RGPD y la legislación que aplica o complementa dicho RGPD.
  9. “**RGPD**” se refiere al Reglamento General de Protección de Datos de la UE 2016/679.
  10. “**Filial del Encargado del Tratamiento**” se refiere a una entidad que esté controlada por, controler, o esté bajo el control común del Encargado del Tratamiento.
  11. “**Servicios**” se refiere a los servicios y demás actividades que suministre o lleve a cabo el Encargado del Tratamiento, o un tercero en su nombre, en beneficio de Mutua Montañesa y en virtud del Contrato Marco.
  12. Los términos, “**Comisión**”, “**Empresa**”, “**Interesado**”, “**Estado miembro**”, “**Datos Personales**”, “**Violación de Datos Personales**”, “**Tratamiento**”, “**Delegado de Protección de Datos**” y “**Autoridad de supervisión**” tendrán el mismo significado que en el RGPD.

1. Tratamiento de Datos Personales de Mutua Montañesa
   1. Mutua Montañesa seguirá siendo el Responsable exclusivo del tratamiento de los Datos Personales que se procesen y determinará qué Datos Personales habrá de tratar el Encargado del Tratamiento, las finalidades de dicho Tratamiento y el uso de los Datos Personales por parte del mismo.
   2. El Encargado del Tratamiento solo tratará Datos Personales por cuenta y en beneficio de Mutua Montañesa, de acuerdo con las instrucciones de esta última, y no tendrá derechos independientes con relación a dichos datos.
   3. El Encargado del Tratamiento informará de inmediato a Mutua Montañesa en caso de que, en su opinión, alguna instrucción infrinja el RGPD o la Legislación en materia de protección de datos.
   4. El Encargado del Tratamiento no tratará los Datos Personales en su propio beneficio o para sus propias finalidades, ni cualquiera otra finalidad no prevista, salvo que así lo haya expresamente acordado con Mutua Montañesa. Sin perjuicio de lo anterior, si la Legislación Aplicable a la que estuviera sujeto el Encargado del Tratamiento impusiera cualquier Tratamiento no previsto en el contrato o los servicios contratados, el Encargado del Tratamiento informará de dicho requisito legal a Mutua Montañesa, en la medida permitida por la Legislación Aplicable, antes de proceder al Tratamiento de esos Datos Personales.
   5. En caso de que el Encargado del Tratamiento haya nombrado a un Delegado de Protección de Datos, deberá comunicar a Mutua Montañesa el nombre y los datos de contacto de dicho Delegado de Protección de Datos del Encargado del Tratamiento. En caso de que el Encargado del Tratamiento no haya nombrado a un Delegado de Protección de Datos, deberá comunicar el nombre y los datos de contacto de una persona de contacto que pueda ofrecer más información sobre el tratamiento de Datos Personales.
   6. El Anexo 1 a esta Adenda establece cierta información relativa al Tratamiento de Datos Personales de Mutua Montañesa por parte de los Encargados del tratamiento. Periódicamente, Mutua Montañesa podrá realizar modificaciones al Anexo 1, en la medida de lo razonable, mediante aviso por escrito al Encargado del Tratamiento.
2. Empleados del Encargado del Tratamiento
   1. El Encargado del Tratamiento adoptará medidas razonables para garantizar la fiabilidad de todos sus empleados que accedan a los Datos Personales de Mutua Montañesa, asegurándose en cada caso que el acceso se limita estrictamente a aquellas personas que necesiten conocer/acceder a los correspondientes Datos Personales de Mutua Montañesa, en virtud de lo estrictamente necesario a efectos del Contrato Marco y con el fin de cumplir con la Legislación Aplicable en el contexto de las obligaciones de esa persona para con el Encargado del Tratamiento.
   2. El Encargado del Tratamiento garantiza que las personas autorizadas a tratar los Datos Personales a efectos del Contrato Marco y de la presente Adenda, incluido su personal y el personal de su Subencargado autorizado, en su caso, se han comprometido a mantener la confidencialidad o se someten a la correspondiente obligación de confidencialidad reglamentaria.
   3. El Encargado del Tratamiento se comprometerá a que sus empleados y subcontratistas cumplan con la Legislación Aplicable en materia de protección de datos y que estén debidamente formados en cuanto a sus obligaciones relativas al tratamiento de Datos Personales.

El Encargado del Tratamiento mantendrá registros electrónicos que demuestren el cumplimiento de las obligaciones estipuladas en la presente cláusula.

1. Designación de Subencargados del Tratamiento
   1. El Encargado del Tratamiento no nombrará (ni divulgará Datos Personales de Mutua Montañesa) a un Subencargado del Tratamiento salvo que lo haga con el previo consentimiento explícito y por escrito de Mutua Montañesa.
   2. En caso de que se facilite la autorización, el Encargado del Tratamiento deberá:
      1. Llevar a cabo la correspondiente diligencia debida, antes de que el Subencargado empiece a tratar Datos Personales de Mutua Montañesa, para garantizar que dicho Subencargado del Tratamiento está en condiciones de ofrecer un nivel de protección de los Datos Personales de Mutua Montañesa acorde a lo exigido en la presente Adenda y en el Contrato Marco.
      2. Asegurarse de que el acuerdo entre el Encargado del Tratamiento y el Subencargado se rige por un contrato escrito que incluya unos términos que ofrezcan como mínimo el mismo nivel de protección para los Datos Personales de Mutua Montañesa que el recogido en la presente Adenda y que dispongan las garantías suficientes para la puesta en práctica de las correspondientes medidas técnicas y organizativas de un modo en que el Tratamiento satisfaga los requisitos de la Legislación en materia de protección de datos o los requisitos de Mutua Montañesa. En caso de duda, el Encargado del Tratamiento deberá preguntar a Mutua Montañesa si las medidas técnicas y organizativas que garantiza el Subencargado cumplen las normas establecidas por Mutua Montañesa y por la Legislación en materia de protección de datos.
      3. Prohibir explícitamente a los Subencargados autorizados, en su contrato por escrito con los mismos, que contraten a un (Sub sub) encargado sin el previo consentimiento explícito y por escrito de Mutua Montañesa.
      4. Proporcionar a Mutua Montañesa las copias de los acuerdos de los Encargados del tratamiento con los respectivos Subencargados, para su revisión.
   3. En caso de que el Subencargado autorizado no cumpla sus obligaciones de protección de datos, el Encargado del Tratamiento seguirá siendo plenamente responsable para con Mutua Montañesa de la ejecución de las obligaciones por parte de dicho Subencargado autorizado.
2. Seguridad
   1. El Encargado del Tratamiento garantiza que pondrá en práctica las correspondientes medidas técnicas y organizativas para proteger los Datos Personales de Mutua Montañesa frente a pérdidas y toda forma de tratamiento ilícito o no autorizado. Estas medidas deberán garantizar un nivel apropiado de seguridad, según lo descrito en el Artículo 32 del RGPD.
   2. En la evaluación del nivel apropiado de seguridad, el Encargado del Tratamiento tendrá en cuenta los riesgos que presenta el Tratamiento, en concreto respecto a la destrucción, pérdida o alteración accidentales o ilícitas, así como a la divulgación o acceso no autorizados a Datos Personales transmitidos, almacenados o tratados de cualquier otro modo.
   3. Las medidas que el Encargado del Tratamiento adopte deberán cumplir como mínimo las medidas de seguridad descritas en el Anexo 2 de la presente Adenda.
3. Localización de los Datos Personales de Mutua Montañesa
   1. El Encargado del Tratamiento no transferirá ni tratará Datos Personales de Mutua Montañesa fuera del Espacio Económico Europeo (EEE) sin el previo consentimiento explícito y por escrito de Mutua Montañesa. Si el Encargado del Tratamiento obtuviese dicho consentimiento escrito, deberá asegurarse de que dicha transferencia o dicho acceso estén cubiertos por:
      1. las Cláusulas contractuales tipo publicadas por la Comisión Europea o por una autoridad de supervisión conforme al artículo 46 del RGPD; o
      2. las normas corporativas vinculantes aprobadas por una autoridad de supervisión competente según los términos del artículo 47 del RGPD; o
      3. un código de conducta aprobado de conformidad con el artículo 46 del RGPD; o
      4. un mecanismo de certificación aprobado de conformidad con el artículo 46 del RGPD; o
      5. una decisión de adecuación de la Comisión Europea de conformidad con el artículo 45 del RGPD.
   2. En cualquier caso, el Encargado del Tratamiento deberá facilitar a Mutua Montañesa toda la información relevante que permita a Mutua Montañesa cumplir sus obligaciones en caso de Transferencias de datos. El Encargado del Tratamiento procederá a instaurar las medidas que aporten un nivel adecuado de protección para los Datos Personales de Mutua Montañesa que se transfieran a países terceros u organizaciones internacionales de conformidad con el artículo 44 del RGPD.
4. Derechos del Interesado
   1. Teniendo en cuenta el carácter del Tratamiento, el Encargado del Tratamiento deberá asistir a Mutua Montañesa mediante la puesta en práctica de las correspondientes medidas técnicas y organizativas para colaborar en el cumplimiento de sus obligaciones y a fin de responder a las peticiones de ejercicio de los Derechos del Interesado en virtud de la Legislación en materia de protección de datos.
   2. El Encargado del Tratamiento deberá:
      1. informar con celeridad y no más tarde de veinticuatro horas (24) horas desde su recepción, en caso de recibir una queja o petición de un Interesado en virtud de la Legislación en materia de protección de datos con respecto a Datos Personales de Mutua Montañesa;
      2. prestar plena cooperación y asistencia en relación con cualquier queja o petición de un Interesado relativa al Tratamiento de Datos Personales de Mutua Montañesa;
      3. asegurarse de que el Encargado del Tratamiento no responde a ninguna petición sin respetar estrictamente las instrucciones, por escrito, de Mutua Montañesa o a lo exigido por la Legislación Aplicable a la que esté sujeto el Encargado del Tratamiento, en cuyo caso el Encargado del Tratamiento deberá informar a Mutua Montañesa acerca de dicho requisito legal, en la medida permitida por la Legislación Aplicable, antes de que el Encargado del Tratamiento responda a la petición;
      4. mantener registros electrónicos de todas las quejas o peticiones de Interesados que pretendan ejercer sus derechos en virtud de la Legislación Aplicable en materia de Protección de datos; los registros descritos en la presente cláusula deberán incluir copias de la queja o la petición, detalles de los datos a los que se haya accedido y se hayan compartido, cuando proceda, las medidas adoptadas por el Encargado del Tratamiento para resolver la queja o petición, y la correspondencia o llamadas telefónicas relativas a la queja o la petición.
5. Mantenimiento de registros
   1. Además de las obligaciones de mantenimiento de registros contempladas en las cláusulas 3.4 y 7.2(d), el Encargado del Tratamiento acepta mantener registros electrónicos de todos los Datos Personales de Mutua Montañesa tratados en virtud del Contrato Marco y de la presente Adenda, así como de sus actividades de tratamiento.
   2. El mantenimiento de registros contendrá como mínimo las información siguiente:
      1. las finalidades del tratamiento;
      2. el nombre, la dirección y los datos de contacto del Encargado del Tratamiento, del o de los Subencargados y de Mutua Montañesa;
      3. la identidad y datos de contacto del Delegado de Protección de Datos o de otra persona de contacto de la cual se pueda obtener más información;
      4. la localización de las bases de datos que alojan los Datos Personales de Mutua Montañesa;
      5. el origen de los Datos Personales de Mutua Montañesa, es decir, si han sido recopilados a partir de los Interesados directamente, a partir de terceros o bien generados a partir de redes de comunicación (para Datos de tráfico y Datos de localización);
      6. las categorías de los Datos Tratados y, si procede, las categorías de los Interesados afectados,
      7. las categorías de destinatarios a los cuales puedan revelarse los Datos Personales de Mutua Montañesa;
      8. un resumen de quién tiene acceso a los Datos Personales de Mutua Montañesa y el modo en que se restringe el mismo;
      9. los métodos seguidos a fin de garantizar la implementación de políticas de conservación de la información en relación con el almacenamiento de Datos Personales de Mutua Montañesa;
      10. los medios usados para borrar o eliminar Datos Personales de Mutua Montañesa;
      11. si procede, las transferencias de Datos Personales a un país tercero o una organización internacional, incluida la identificación de dicho país u organización internacional y la documentación de las medidas adecuadas de protección para dichas transferencias de acuerdo con la cláusula 6 de la presente Adenda;
      12. las medidas adoptadas para garantizar la seguridad de los Datos Personales de Mutua Montañesa y el Tratamiento de los mismos; y
      13. cualquier información necesaria y pertinente para que Mutua Montañesa realice una evaluación del impacto de la protección de datos.
   3. Mutua Montañesa se reserva el derecho, en cualquier momento y por si misma o por terceros, a inspeccionar los registros que mantiene el Encargado del Tratamiento de conformidad con las cláusulas 3.4, 7.2(d) y 8, sin coste alguno para Mutua Montañesa.
6. Violación de Datos Personales
   1. El Encargado del Tratamiento tiene la estricta obligación de informar a Mutua Montañesa de cualquier violación de Datos Personales que afecte a Datos Personales de Mutua Montañesa, sin demora injustificada y no más tarde de veinticuatro (24) horas desde el conocimiento de la violación por parte del Encargado del Tratamiento, de conformidad con lo establecido en el artículo 33 del RGPD.
   2. El Encargado del Tratamiento proporcionará a Mutua Montañesa la información suficiente para permitirle que cumpla las obligaciones de notificación a la autoridad de supervisión competente, de acuerdo con el artículo 55 del RGPD o cualquier otra Legislación en materia de protección de datos, y que pueda informar a los Interesados acerca de la Violación de Datos Personales, si procede. El Encargado del Tratamiento usará el Impreso de notificación de violación de datos que se adjunta como **Anexo 3** a la presente Adenda. Este impreso deberá cumplimentarse de la forma más completa posible y deberá incluir siempre:
      1. la identidad y datos de contacto del Delegado de Protección de Datos o de otra persona de contacto de la cual se pueda obtener más información;
      2. el carácter de la violación de seguridad, incluidas las categorías de los interesados afectados y las categorías de Datos Personales de Mutua Montañesa y los registros de datos afectados;
      3. una descripción de las medidas que podría adoptar Mutua Montañesa para atenuar los posibles efectos adversos de la violación de Datos Personales;
      4. las consecuencias de la violación de Datos Personales;
      5. las medidas propuestas o adoptadas por el Encargado del Tratamiento en cooperación con Mutua Montañesa para abordar la violación de Datos Personales.
   3. Si el Encargado del Tratamiento no pudiese comunicar toda la información relativa a la violación de datos de forma inmediata y/o simultánea, deberá entonces proporcionar la información tan pronto como vaya estando disponible.
   4. El Encargado del Tratamiento cooperará con Mutua Montañesa y adoptará las medidas razonables que Mutua Montañesa le indique de cara a asistir en la investigación, atenuación y reparación de cada violación de Datos Personales.
7. Evaluaciones de impacto de la protección de datos
   1. El Encargado del Tratamiento proporcionará a Mutua Montañesa la cooperación y asistencia razonables para cumplir la obligación de esta última, recogida en el RGPD, de llevar a cabo evaluaciones del impacto de las operaciones de tratamiento previstas por el Encargado del Tratamiento sobre la protección de los Datos Personales de Mutua Montañesa, teniendo en cuenta el carácter, el ámbito, el contexto y los efectos del tratamiento de conformidad con el artículo 35 del RGPD. El Encargado del Tratamiento ofrecerá asistencia razonable a Mutua Montañesa en la cooperación o la consulta previa con la Autoridad de supervisión en cuanto a la realización de tareas relacionadas con la cláusula 10.1 del presente ATD.
   2. El Encargado del Tratamiento ofrecerá la cooperación y asistencia razonables de cara a poner en práctica las medidas previstas para abordar los riesgos, incluidas medidas de protección, medidas de seguridad y mecanismos que garanticen la protección de los Datos Personales de Mutua Montañesa y para demostrar el cumplimiento del RGPD, teniendo en cuenta los derechos e intereses legítimos de los interesados y demás personas afectadas.
8. Derechos de auditoría

* 1. El Encargado del Tratamiento pondrá a disposición de Mutua Montañesa, previa petición, toda la información necesaria para demostrar el cumplimiento de la presente Adenda, y deberá permitir y contribuir a las auditorías, incluidas inspecciones, que Mutua Montañesa o un auditor con un mandato de Mutua Montañesa en relación con el Tratamiento de los Datos Personales de Mutua Montañesa por parte del Encargado del Tratamiento y de los Subencargados autorizados.
  2. Además de lo anterior, el Encargado del Tratamiento se comprometerá a auditar los sistemas de Tratamiento de datos que utilice, así como las medidas de seguridad, al menos una vez al año. El resultado de la auditoría realizada por el Encargado del Tratamiento se facilitará a Mutua Montañesa junto con un informe de seguridad anual por escrito, que incluya el estado del sistema de Tratamiento de Datos Personales, las medidas de seguridad, el tiempo registrado de inactividad por medidas técnicas de seguridad, el cumplimiento o incumplimiento establecido de medidas de la organización, incidentes de seguridad y/o violaciones de datos, amenazas detectadas para la seguridad y los Datos, así como las mejoras necesarias o recomendadas.
  3. Los costes razonables por la contratación de auditores de Mutua Montañesa correrán a cargo de Mutua Montañesa. El Encargado del Tratamiento es responsable de sus propios costes a este respecto. En el supuesto de que se detectasen incidentes relacionados con las medidas de seguridad que se vayan a poner en práctica o a ejecutar, los costes serán asumidos plena y exclusivamente por el contratista, así como cualesquiera costes vinculados a la propia auditoría y la reparación de los incidentes.

1. Extinción del Contrato
   1. Las partes acuerdan que tras el vencimiento o extinción del Contrato Marco o tras la finalización de la prestación de servicios de tratamiento de datos, el Encargado del Tratamiento deberá cesar de inmediato dicho Tratamiento de los Datos Personales de Mutua Montañesa y deberá devolver a Mutua Montañesa todos los Datos Personales de Mutua Montañesa y copias de los mismos en un plazo no superior a un mes desde el vencimiento o finalización de la prestación de servicios de tratamiento de datos.
   2. Una vez que el Encargado del tratamiento haya devuelto los Datos Personales de Mutua Montañesa a la misma, dicho Encargado del tratamiento deberá destruir todos los Datos Personales y certificar a Mutua Montañesa haber procedido a ello, a menos que la legislación impuesta sobre el Encargado del Tratamiento le impida devolver o destruir la totalidad o parte de los Datos Personales. En tal caso, el Encargado del Tratamiento garantiza que se asegurará la confidencialidad de los Datos Personales transferidos y que dejará de tratar activamente los Datos Personales. El Encargado del Tratamiento contratado cumplimentará y firmará el Anexo 4 antes de la extinción del contrato.

La presente Adenda se suscribe y pasa a formar parte del Contrato Marco de forma vinculante con efecto y vigor a partir de la fecha indicada arriba.

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

**ANEXO 1. DETALLES DEL TRATAMIENTO DE DATOS PERSONALES DE MUTUA MONTAÑESA**

Este Anexo 1 incluye ciertos detalles del Tratamiento de Datos Personales de Mutua Montañesa conforme a lo exigido en el artículo 28(3) del RGPD.

1. Objeto y duración del Tratamiento de Datos Personales de Mutua Montañesa

El objeto y la duración del Tratamiento de Datos Personales de Mutua Montañesa se establecen en el Contrato Marco y en la presente Adenda.

1. **El carácter y la finalidad del Tratamiento de Datos Personales de Mutua Montañesa** “indicar objeto de contrato”
2. Los tipos de Datos Personales de Mutua Montañesa objeto del tratamiento

|  |  |  |  |
| --- | --- | --- | --- |
| **Categorías de Interesados a quienes se refiere el Tratamiento** | **Categorías de Datos Personales** | **Grupos de empleados del Encargado del Tratamiento con acceso a los Datos Personales de Mutua**  **Montañesa** | **Actividades que pueden realizar dichos empleados con los Datos Personales** |
|  |  |  |  |

ANEXO 2. MEDIDAS TÉCNICAS Y ORGANIZATIVAS

1. El tratamiento de Datos Personales de Mutua Montañesa debe tener lugar en sistemas de tratamiento de datos en los cuales se hayan implantado medidas técnicas y organizativas de protección de Datos Personales. En este contexto, el Encargado del Tratamiento garantiza a Mutua Montañesa que adoptará todas las medidas necesarias para el tratamiento de los Datos Personales de Mutua Montañesa en los sistemas de tratamiento de datos del Encargado del Tratamiento conformes a las medidas indicadas en la siguiente tabla:

|  |  |
| --- | --- |
| **Descripción de medida de seguridad** | **Descripción de la implementación por parte del Encargado del**  **Tratamiento** |
| **Control de acceso al equipo**: denegar a personas no autorizadas el acceso al equipo de tratamiento de datos utilizado para el tratamiento de  Datos Personales |  |
| **Control de soportes de datos**: impedir la lectura, copia, modificación o retirada de soportes datos de forma  no autorizada |  |
| **Control de almacenamiento**: impedir la introducción no autorizada de Datos Personales y la inspección, modificación o borrado no autorizados  de Datos Personales almacenados |  |
| **Control de usuario**: impedir el uso de sistemas de tratamiento automático de datos por parte de personas no autorizadas a través de equipos de  comunicación de datos |  |
| **Control de acceso a datos**: garantizar que las personas autorizadas a usar un sistema de tratamiento automático de datos solo  tengan acceso a los Datos Personales que abarque su autorización de acceso |  |
| **Control de comunicación**: garantizar que se puede comprobar y establecer a qué personas se han transmitido o puesto a disposición los Datos Personales, o podrían transmitirse o ponerse a disposición, a través del  equipo de comunicación de datos |  |
| **Control de entrada**: garantizar que se puede posteriormente comprobar y establecer qué Datos Personales se han introducido en sistemas de tratamiento automático de datos y  cuándo y quién ha procedido a ello |  |
| **Control de transporte:** impedir la lectura, copia, modificación o borrado no autorizados de Datos Personales durante las transferencias de dichos datos o durante el transporte de  soportes de datos |  |
| **Recuperación:** garantizar que los sistemas instalados podrían restablecerse en caso de interrupción |  |
| **Integridad:** garantizar que funcionan las funciones del sistema, que se comunica la aparición de fallos en dichas funciones (fiabilidad) y que los Datos Personales almacenados no pueden corromperse por culpa del mal  funcionamiento del sistema |  |

1. El Encargado del Tratamiento ofrecerá a Mutua Montañesa un plan exhaustivo y actualizado de protección y seguridad de datos para el tratamiento de datos conforme a los términos de la presente Adenda, y que será compartido con Mutua Montañesa en cuanto esta Adenda entre en vigor. Además, Mutua Montañesa podrá solicitar en cualquier momento una copia de este plan de seguridad.
2. El Encargado del Tratamiento no nombrará a persona alguna para el tratamiento de los Datos Personales a menos que dicha persona:
   1. sea competente y esté cualificada para realizar las tareas específicas que se le asignen;
   2. haya sido autorizada por el Encargado del Tratamiento; y
   3. haya sido totalmente formada por el Encargado del Tratamiento en cuanto a los procedimientos y reglamentos vigentes pertinentes para el cumplimiento de las obligaciones del Encargado del Tratamiento en virtud de la presente Adenda sobre tratamiento de datos.
3. Se prohíbe realizar copias de cualesquiera Datos Personales de Mutua Montañesa que esta hubiese transmitido al Encargado del Tratamiento. No obstante, este último podrá conservar copias de Datos Personales que se le hayan facilitado en sus servidores a efectos de copias de seguridad y archivado en virtud del contrato correspondiente y hasta la finalización de los servicios indicados en la presente Adenda sobre tratamiento de datos.

ANEXO 3. IMPRESO DE NOTIFICACIÓN DE VIOLACIÓN DE DATOS

**Introducción**

El Reglamento general de protección de datos (RGPD) introduce la obligación para todas las organizaciones de notificar violaciones de Datos Personales a la autoridad de supervisión pertinente y, en algunos casos, a las personas físicas afectadas. Una violación de Datos Personales se refiere a un fallo de seguridad que entraña la destrucción, pérdida o alteración, accidentales o ilícitas, o la divulgación o el acceso no autorizados, de Datos Personales que se hayan transmitido, almacenado o tratado de cualquier otro modo. En estos casos, las organizaciones podrán notificar la violación en un plazo de 72 horas desde la detección del fallo. La decisión de notificación deberá ser tomada por varias personas en el seno de Mutua Montañesa y siguiendo un procedimiento predeterminado. Para asegurarse de que se adoptan los pasos adecuados, Mutua Montañesa tiene que tener constancia de cada posible violación de datos. Este impreso se utilizará para informar de posibles violaciones de datos a la persona de contacto indicada a continuación:

Todo impreso deberá enviarse a [dpo@mutuamontanesa.es](mailto:dpo@mutuamontanesa.es)

Definiciones principales:

|  |  |
| --- | --- |
| **Término** | **Definición** |
| Violación (incidente que activa la notificación) | Un fallo de seguridad que entraña la destrucción, pérdida o alteración, accidentales o ilícitas, o la divulgación o el acceso no autorizados de Datos Personales  que se hayan transmitido, almacenado o tratado de cualquier otro modo. |
| Datos Personales | Datos Personales hace referencia a cualquier  información relativa a una persona física identificada o identificable |
| Interesado | La persona física a la cual pertenecen los Datos Personales |
| Encargado del Tratamiento | La persona que trata los Datos Personales por cuenta del Responsable del tratamiento |

1. **DETALLES DE LA PERSONA QUE INFORMA DE LA VIOLACIÓN DE DATOS**

**(“USTED”)**

|  |  |
| --- | --- |
| Nombre completo | Haga clic aquí para introducir el texto. |
| Dirección de correo electrónico | Haga clic aquí para introducir el texto. |
| Número de teléfono | Haga clic aquí para introducir el texto. |
| Puesto de trabajo | Haga clic aquí para introducir el texto. |
| Grupo | Haga clic aquí para introducir el texto. |
| Entidad para la que trabaja o que ha contratado sus servicios (p. ej.: nombre de la unidad de negocio  central): | Haga clic aquí para introducir el texto. |

1. **DETALLES DE LA VIOLACIÓN DE DATOS**

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| ¿Se ha visto afectada información de carácter personal  *(p. ej.: datos de clientes, datos de empleados, datos de un cliente o datos sobre proveedores o socios*  *comerciales)?* | * Sí * No * Se desconoce | | | | | |
| Explique en sus propias palabras qué ha sucedido o qué ha llevado al incidente. Incluya detalles como la disponibilidad eventual de registros, aportando un análisis de la secuencia de eventos que haya dado como resultado la violación de datos. De ser posible, asegúrese de incluir información sobre la confidencialidad,  integridad y disponibilidad de la información. | Haga clic aquí para introducir el texto. | | | | | |
| ¿La violación ha ocurrido en una herramienta propiedad de Mutua Montañesa o propiedad de un 3o? En este último caso, especifique el  nombre del 3o. | Haga clic aquí para introducir el texto. | | | | | |
| Indique el nombre de la aplicación o aplicaciones o sistemas implicados en la violación, es decir, la fuente del fallo. | Haga clic aquí para introducir el texto. | | | | | |
| Fecha de inicio de la violación de datos (si se conoce) | Haga clic aquí para indicar una fecha.   * No sabemos cuándo se inició la violación de datos | | | | | |
| Hora del incidente (en términos de 24 horas) | Haga clic aquí para indicar una hora.   * No sabemos a qué hora se inició la violación de datos | | | | | |
| Fecha de finalización de la violación de datos (si ha terminado) | Haga clic aquí para indicar una fecha.   * La violación de datos todavía no ha terminado | | | | | |
| ¿En qué país y grupo ha tenido lugar la violación de datos? | Haga clic aquí para introducir el texto. | | | | | |
| ¿Ha impactado la violación en otros países/grupos? | Haga clic aquí para introducir el texto. | | | | | |
| ¿Qué cree que ha causado la violación de datos? | Haga clic aquí para introducir el texto.   * No sabemos qué ha causado la violación de datos. | | | | | |
| ¿Cuál es el número (estimado) de personas físicas afectadas?  *Rogamos facilite una indicación general* | Mín.: Haga clic aquí para introducir el texto. Máx.: Haga clic aquí para introducir el texto.   * No sabemos cuántas personas físicas se han visto afectadas. | | | | | |
| ¿Podría clasificar el grupo de personas afectadas por la violación?  *Seleccione una o más categorías.* | * Clientes * Empleados * Socios comerciales * Participantes en ensayos clínicos / de investigación * Otros: Haga clic aquí para introducir el texto. | | | | | |
| ¿Podría clasificar el tipo de Datos Personales afectados por el incidente?  *Seleccione una o más categorías.* | * Nombre y dirección * Números de teléfono * Direcciones de correo electrónico * Información financiera, como información salarial, de pagos. * Información sobre la situación económica * Número de servicio al ciudadano * Copias del pasaporte o carné de identidad * Género * Fecha de nacimiento o edad * Nombres de usuario, contraseñas y demás información de conexión * Datos reveladores del origen racial o étnico * Datos reveladores de opiniones políticas * Datos reveladores de creencias religiosas o filosóficas * Datos sobre afiliaciones sindicales * Datos relativos a la salud o la vida sexual * Datos genéticos * Condenas y delitos penales * Otros, *indíquense todos los demás tipos de Datos Personales no enumerados*   *anteriormente*: Haga clic aquí para introducir el texto. | | | | | |
| ¿Cuáles son las consecuencias potenciales para las personas físicas afectadas?  *Seleccione una o más categorías, si procede.* | Por ejemplo:   * Fraude de identidad * Pérdida económica * Uso no autorizado de Datos Personales * Perjuicio a la reputación * Puede resultar en discriminación | | | | | |
|  | * Otros, introducir | *indíquense*: el texto. | Haga | clic | aquí | para |

1. **MEDIDAS ADOPTADAS PARA ABORDAR LA VIOLACIÓN DE DATOS**

|  |  |
| --- | --- |
| ¿Se ha notificado la violación de datos a alguna persona ajena a Mutua Montañesa  *p. ej.: interesados afectados, autoridades de protección de datos, terceros?* Incluir si se ha enviado notificación a las autoridades. *P. ej.: declaración de*  *portátil robado.* | * No * Sí, *especifíquese*: Haga clic aquí para introducir el texto. |
| ¿Se han recuperado los Datos Personales afectados? | * No * Sí * Parcialmente, *especifíquese*: Haga clic aquí para introducir el texto. |
| ¿Se han adoptado medidas técnicas y organizativas para atenuar las consecuencias? | * No se han adoptado medidas * Sí, *indíquense todas las medidas*   *adoptadas*: Haga clic aquí para introducir el texto. |
| *Si procede*: ¿los datos afectados estaban cifrados? | * No * Sí, indíquense qué métodos de cifrado se   aplicaron: Haga clic aquí para introducir el texto. |

**ANEXO 4. DECLARACIÓN DE ELIMINACIÓN SEGURA DE DATOS PERSONALES**

* 1. El Encargado del Tratamiento certifica que ha eliminado de forma segura todos los Datos Personales de Mutua Montañesa, incluidos, entre otros, los Datos Personales de Mutua Montañesa en forma impresa, los Datos Personales de Mutua Montañesa almacenados en servidores, los Datos Personales de Mutua Montañesa en sistemas y en copias de seguridad de Datos Personales de Mutua Montañesa de acuerdo con el artículo 12 de la Adenda.
  2. En la medida en que la ley obligue al Encargado del Tratamiento a almacenar los Datos Personales de Mutua Montañesa durante un plazo de tiempo determinado, el artículo 1 se complementará con el texto siguiente:

El Encargado de tratamiento ha conservado una copia de los Datos Personales de Mutua Montañesa con el fin de cumplir la Legislación Aplicable y almacenará los siguientes Datos Personales durante el plazo de tiempo determinado tras el cual el Encargado del Tratamiento certifica que eliminará de forma segura los Datos Personales de Mutua Montañesa.

|  |  |  |  |
| --- | --- | --- | --- |
| **Categorías de Interesados a quienes se refiere el Tratamiento** | **Categorías de Datos Personales** | **Plazo límite para el borrado** | **Base legal** |
| Cumplimentar una categoría por punto | Cumplimentar una categoría por punto | Cumplimentar el plazo límite por categoría de Datos  Personales | Cumplimentar la Legislación Aplicable por categoría de Datos  Personales |

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 …………………….

**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)