ACUERDO GENERAL DE ENCARGO DEL TRATAMIENTO DE DATOS

Artículo 28 del Reglamento (UE) 2016/679 («RGPD»)

Entre

El Cliente, tal como se identifica en el Contrato («Responsable del Tratamiento»), representado por su representante legal con los poderes necesarios, en calidad de**,**

Responsable del Tratamiento

y

El Proveedor, tal como se identifica en la Propuesta Comercial y en el Anexo A de las Condiciones Generales, representado por su representante legal investido de los poderes necesarios («Encargado del Tratamiento» o «Proveedor»), representado por su representante legal con los poderes necesarios, en calidad de

Encargado del Tratamiento

Asimismo, el Responsable del Tratamiento y el Encargado del Tratamiento podrán denominarse conjuntamente las **«Partes**» e individualmente la «**Parte**».

CONSIDERANDO

I. Que las Partes han suscrito uno o varios contratos («**Contrato**») para la prestación de Servicios («**Servicios**»);
II. Que el Contrato implica el tratamiento de información definida por la ley como Datos Personales, por lo que las Partes pretenden regular, en el presente Acuerdo General de Encargo del Tratamiento de Datos («**Acuerdo**»), los términos y condiciones para el tratamiento de Datos Personales llevado a cabo por el Encargado del Tratamiento en el marco de la prestación de los Servicios en virtud del Contrato;
III. Que los detalles y características específicas o condiciones particulares del tratamiento de los Datos Personales se recogen en las denominadas «**Hojas de Tratamiento**» relativas a uno o varios servicios activados por el Cliente, que se adjuntarán al presente Acuerdo de forma periódica.
IV. Estas Hojas de Tratamiento detallarán los métodos operativos de tratamiento en relación con el Servicio específico, indicando, en su caso, la lista de Subencargados del Tratamiento y las medidas de seguridad adicionales aplicadas. Las Hojas de Tratamiento, una vez firmadas, se incorporarán como Anexos adicionales al presente Acuerdo y formarán parte integrante y sustancial del mismo;
V. Que, con carácter previo a confiar al Encargado del Tratamiento la ejecución de los Servicios, el Responsable del Tratamiento ha verificado la experiencia, capacidad y fiabilidad del Encargado del Tratamiento, y ha evaluado que este ofrece garantías suficientes para aplicar medidas técnicas y organizativas adecuadas y garantizar una protección adecuada de los datos tratados y de los derechos de los interesados;
VI. Que el Encargado del Tratamiento debe llevar a cabo las operaciones de Tratamiento de conformidad con las instrucciones facilitadas por escrito por el Responsable del Tratamiento mediante un contrato u otro acto jurídico vinculante que especifique la duración, naturaleza y finalidades del Tratamiento, las categorías de Datos Personales tratados y las categorías de interesados afectados por el Tratamiento, así como las obligaciones y derechos del Encargado del Tratamiento en relación con el Tratamiento;
VII. Que, mediante el presente Acuerdo, el Responsable del Tratamiento pretende designar al Encargado del Tratamiento indicado en el preámbulo como encargado del tratamiento y facilitar todas las instrucciones necesarias para el Tratamiento de los Datos Personales que subyacen a la prestación de los Servicios;
VIII. Que el Responsable del Tratamiento autoriza al Encargado del Tratamiento, así como a las personas autorizadas por este, a acceder únicamente a los Datos Personales estrictamente necesarios para la ejecución del Contrato («**Datos Personales**»);
IX. Que el presente Acuerdo no conlleva ningún derecho del Encargado del Tratamiento a honorarios y/o indemnizaciones y/o reembolsos específicos, distintos de los ya eventualmente previstos en el Contrato, salvo en el caso de implementaciones adicionales solicitadas y acordadas expresamente entre las Partes mediante un acuerdo escrito independiente;
X. Que la prestación efectiva de los Servicios cubiertos por el Contrato podrá llevarse a cabo, para cada Servicio, por una sociedad específica del Grupo Namirial, identificada en la Hoja

de Tratamiento correspondiente como «Entidad Prestadora». Cuando la Entidad Prestadora no coincida con el Encargado del Tratamiento, actuará en virtud de acuerdos intragrupo entre las sociedades del Grupo Namirial, conformes con el artículo 28 del RGPD, preexistentes y separados del presente Acuerdo, sin perjuicio de cualquier otro rol distinto en materia de protección de datos que se especifique expresamente en la Hoja de Tratamiento correspondiente;

XI. Que, en el supuesto de que el Cliente actúe como Encargado del Tratamiento por cuenta de otro responsable (el «**Cliente Fina**l»), el propio Cliente asumirá, en relación con dicho tratamiento específico, las obligaciones y responsabilidades de un encargado del tratamiento frente al Proveedor, que en este contexto asumirá el papel de Subencargado del Tratamiento. En tal supuesto, se aplicarán las disposiciones relativas al tratamiento de datos y a las obligaciones del Encargado del Tratamiento previstas en el presente Acuerdo, actuando el Cliente como Encargado del Tratamiento por cuenta del Cliente Final y el Encargado del Tratamiento como Subencargado del Tratamiento por cuenta del Cliente;

XII. Que, en cualquier caso en que el Cliente actúe como Responsable o Encargado del Tratamiento por cuenta del Cliente Final, el Encargado del Tratamiento acepta actuar como Encargado del Tratamiento y/o Subencargado del Tratamiento y, en consecuencia, se compromete a tratar los Datos Personales de conformidad con las instrucciones recibidas del Cliente y de manera que se garantice la protección de los propios Datos Personales, conforme a las medidas de seguridad establecidas en el presente Acuerdo y en las Hojas de Tratamiento adjuntas al mismo.

POR LO TANTO, LAS PARTES ACUERDAN Y ESTIPULAN LO SIGUIENTE

1. VALIDEZ DE LOS ANTECEDENTES Y ANEXOS. DEFINICIONES

1.1. Los antecedentes y los Anexos constituyen parte integrante y sustancial del presente Acuerdo.

1.2. Salvo que se disponga otra cosa en el presente Acuerdo, todos los términos con mayúscula inicial utilizados en el presente Acuerdo y en los Anexos tendrán el significado que se les atribuye en el Contrato y se entenderán expresados tanto en singular como en plural. De conformidad con las definiciones contenidas en la normativa aplicable, se utilizan los términos y definiciones establecidos en el Anexo I – Definiciones del presente Acuerdo, al que se remite.

1.3. Las Hojas de Tratamiento relativas a los Servicios utilizados por el Cliente podrán pasar a formar parte del presente Acuerdo, incluso con posterioridad, en caso de ampliación del Contrato para la activación de nuevos Servicios. En tal caso, los Anexos, firmados por las Partes junto con la adenda contractual, se incorporarán al presente Acuerdo.

2. DERECHOS Y OBLIGACIONES DEL RESPONSABLE DEL TRATAMIENTO

2.1. El Responsable del Tratamiento encomienda al Encargado del Tratamiento la totalidad -y exclusivamente- de las operaciones de Tratamiento de Datos Personales necesarias para la plena ejecución del Contrato.

2.2. El Responsable del Tratamiento declara cumplir todas las obligaciones previstas por la Normativa Aplicable dentro de su ámbito de competencia en relación con el Tratamiento de Datos Personales en virtud del presente Acuerdo. En particular, el Responsable del Tratamiento:

a. tiene el derecho y la obligación de tomar decisiones sobre las finalidades y los medios del Tratamiento, incluida la identificación de la base jurídica correcta para el Tratamiento;
b. declara que los Datos Personales son pertinentes y no excesivos en relación con las finalidades para las que fueron recogidos y posteriormente tratados, y que se transmiten cumpliendo todos los requisitos previstos por la Normativa Aplicable;
c. elabora y -cuando sea necesario- pone a disposición del Encargado del Tratamiento información adecuada y completa sobre el Tratamiento de los Datos Personales conforme a los arts. 13 y/o 14 del RGPD.

2.3. El Responsable del Tratamiento se compromete a notificar formalmente al Encargado del Tratamiento cualquier cambio que pueda resultar necesario en relación con las operaciones de Tratamiento de Datos Personales. El Encargado del Tratamiento y sus Personas Autorizadas no llevarán a cabo operaciones de Tratamiento de Datos Personales distintas de las indicadas por el Responsable del Tratamiento en virtud del presente artículo.

2.4. El Responsable del Tratamiento garantiza que las infraestructuras y sistemas que eventualmente ponga a disposición el propio Responsable del Tratamiento y/o terceros designados por este, sobre los que el Encargado del Tratamiento deba llevar a cabo el Tratamiento (los «Sistemas del Responsable del Tratamiento»), son adecuados y cumplen las normas de referencia y la normativa sectorial, y son capaces de garantizar la prestación regular de los Servicios de conformidad con el presente Acuerdo. Por ello, el Responsable del Tratamiento se compromete a indemnizar y mantener indemne al Encargado del Tratamiento frente a cualquier interrupción, daño o alteración en la ejecución del Tratamiento que pueda derivarse de la inadecuación, anomalías y/o cualquier mal funcionamiento de los Sistemas del Responsable del Tratamiento sobre los que el Encargado del Tratamiento deba operar.

3. OBLIGACIONES DEL ENCARGADO DEL TRATAMIENTO

3.1. Dentro de los límites de su competencia en virtud del Contrato y del presente Acuerdo, el Encargado del Tratamiento estará obligado, tanto respecto de sí mismo como de sus Personas Autorizadas, a cumplir lo dispuesto por la Normativa Aplicable, en particular por lo previsto en el RGPD, así como las medidas aplicables de las Autoridades de Control competentes que impongan obligaciones específicas a los encargados del tratamiento;

3.2. En particular, el Encargado del Tratamiento llevará a cabo las operaciones de Tratamiento que le sean asignadas de conformidad con las instrucciones dadas por el Responsable del Tratamiento contenidas en el presente Acuerdo, así como las notificadas posteriormente por escrito por el Responsable del Tratamiento con una antelación razonable.

3.3. El Encargado del Tratamiento llevará a cabo las operaciones de Tratamiento funcionales a las tareas que le sean asignadas de conformidad con el presente Acuerdo y con las finalidades para las que se recogen y tratan los Datos Personales. Cualquier tratamiento que se aparte del presente Acuerdo solo tendrá lugar siguiendo instrucciones documentadas del Responsable, o cuando el Encargado esté obligado a ello por el Derecho de la Unión o del Estado miembro; en tal caso, el Encargado informará previamente al Responsable, salvo que la ley lo prohíba.

3.4. El Encargado del Tratamiento está obligado a gestionar la documentación relativa al Tratamiento que le ha sido encomendado mediante procedimientos adecuados, con arreglo a criterios de eficiencia y garantizando la custodia, la no alteración y la fácil recuperación de cualquier documento pertinente para el cumplimiento de los requisitos impuestos por el RGPD.

3.5. El Encargado del Tratamiento pone a disposición del Responsable del Tratamiento toda la información y documentos necesarios para demostrar el cumplimiento de las obligaciones previstas en el art. 28 del RGPD, y permite y contribuye a las actividades de auditoría, incluidas las inspecciones notificadas con una antelación razonable, llevadas a cabo por el Responsable del Tratamiento o por un tercero designado por este, de conformidad con los términos, límites y procedimientos establecidos en el Artículo 10.

3.6. El Encargado del Tratamiento informará inmediatamente al Responsable del Tratamiento si, en su opinión, una instrucción vulnera el RGPD u otras disposiciones de la Normativa Aplicable. Asimismo, el Encargado del Tratamiento asiste al Responsable del Tratamiento, a solicitud de este, en los procedimientos ante la Autoridad de Control competente o la autoridad judicial, en relación con las actividades de Tratamiento dentro de su competencia, en particular poniendo a disposición cualquier información y documento útil para demostrar el cumplimiento de las obligaciones previstas por la Normativa Aplicable en materia de Tratamiento de Datos Personales.

3.7. El Encargado del Tratamiento informará al Responsable del Tratamiento, a la dirección de Correo Electrónico de Notificación, sin dilación indebida y, en todo caso, en un plazo de 48 (cuarenta y ocho) horas, de cualquier objeción, inspección o solicitud jurídicamente vinculante procedente de una Autoridad de Control, autoridad judicial u otra autoridad pública relativa a los Datos Personales tratados por cuenta del Responsable del Tratamiento. En caso de solicitud de divulgación, se informará al Responsable del Tratamiento antes de que el Encargado del Tratamiento la satisfaga y, en la medida legalmente permitida, la notificación identificará a la autoridad solicitante, la base jurídica, el alcance de la solicitud y los Datos Personales afectados. El Encargado del Tratamiento no dará cumplimiento a solicitudes que no sean jurídicamente vinculantes.

Dicha información podrá omitirse o limitarse únicamente en la medida y durante el período en que el Derecho de la Unión o de un Estado miembro aplicable al Encargado del Tratamiento, o una orden vinculante dictada en virtud de dicho Derecho, lo prohíba por motivos importantes de interés público. En tal caso, el Encargado del Tratamiento documentará la restricción, revelará únicamente los Datos Personales estrictamente necesarios e informará al Responsable del Tratamiento en cuanto cese la restricción. Las solicitudes procedentes de autoridades de terceros países se evaluarán asimismo con arreglo al artículo 48 y al Capítulo V del RGPD.

3.8. El Encargado del Tratamiento identifica, dentro de su estructura organizativa, a las Personas Autorizadas para llevar a cabo las operaciones de Tratamiento de Datos Personales. En el momento de su designación, el Encargado del Tratamiento facilita a las Personas Autorizadas instrucciones escritas adecuadas sobre los métodos de Tratamiento, de conformidad con lo dispuesto en el art. 29 del RGPD y en el presente Acuerdo. A modo de ejemplo y sin carácter exhaustivo, el Encargado del Tratamiento, al designar por escrito a las Personas Autorizadas, dispone que estas tengan acceso únicamente a los Datos Personales cuyo conocimiento sea estrictamente necesario para el desempeño de las tareas que les sean asignadas (principio de necesidad de conocer). El Encargado del Tratamiento también debe verificar que las Personas Autorizadas aplican todas las medidas de seguridad relativas a la custodia de las credenciales de acceso en caso de Tratamiento realizado por medios electrónicos. El Encargado del Tratamiento verifica asimismo que las Personas Autorizadas custodian de forma segura los soportes no informáticos que contengan cualquier copia de los Datos Personales, en particular si pertenecen a Categorías Especiales. Por último, el Encargado del Tratamiento garantiza que las Personas Autorizadas están sujetas a obligaciones de confidencialidad efectivas, incluso durante el período posterior a la finalización de la relación laboral con el Encargado del Tratamiento, en relación con las operaciones de Tratamiento de Datos Personales que hayan llevado a cabo.

3.9. En las relaciones internas entre las Partes, en caso de daños derivados del Tratamiento, el Encargado responderá conforme al artículo 82 del RGPD únicamente en la medida en que dichos daños sean causados por un incumplimiento que le sea imputable de las obligaciones del RGPD dirigidas específicamente a los encargados del tratamiento, o por haber actuado al margen de o en contra de las instrucciones lícitas del Responsable. La responsabilidad del Encargado se limita a la parte del daño correspondiente a su contribución efectiva a su causación, y está sujeta a los límites de responsabilidad previstos en el Contrato.

3.10. Cuando resulte aplicable, y en la medida exigida por las leyes, reglamentos o medidas vinculantes de la Autoridad de Control competente aplicables al Servicio o a la Entidad Prestadora correspondiente, el Encargado del Tratamiento implementará las medidas oportunas para la identificación, autorización, instrucción y supervisión del personal con acceso privilegiado o administrativo a los sistemas utilizados para el Tratamiento de Datos Personales. Cualquier requisito específico de cada país, incluidos los relativos a los administradores de sistemas, se establecerá en la Hoja de Tratamiento correspondiente.

3.11. De conformidad con el artículo 28, apartado 3, letra a), del RGPD, el Responsable del Tratamiento incluye entre las instrucciones al Encargado del Tratamiento la ejecución de operaciones de tratamiento estrictamente necesarias para las siguientes actividades destinadas a mejorar los Servicios cubiertos por el Contrato: pruebas, medición y optimización del rendimiento, calibración y validación de modelos/algoritmos, mejora de la precisión/fiabilidad/usabilidad, seguridad y prevención del fraude, corrección de errores y anomalías, en la medida en que sean funcionales para la correcta prestación de los Servicios al Responsable del Tratamiento. Queda excluido cualquier uso para fines autónomos del Encargado del Tratamiento o de sus Subencargados del Tratamiento, incluidos la mercadotecnia, la elaboración de perfiles o el desarrollo de productos/servicios no relacionados.

3.12. Las actividades de mejora a que se refiere el párrafo anterior se llevarán a cabo únicamente en la medida estrictamente necesaria para la prestación, el mantenimiento y la seguridad de los Servicios, o, en su defecto, sobre datos anonimizados/agregados, salvo instrucción distinta y justificada legalmente por el Responsable del Tratamiento. El Encargado del Tratamiento podrá recurrir a Subencargados del Tratamiento, siempre que imponga una prohibición de reutilización de los datos y de entrenamiento de modelos de uso general, así como la obligación de eliminar los datos una vez finalizadas las actividades.

4. SEGURIDAD DEL TRATAMIENTO

4.1. Dentro de los límites de su competencia en virtud del Contrato y del presente Acuerdo, el Encargado del Tratamiento está obligado, tanto respecto de sí mismo como de sus Personas Autorizadas, a implementar las Medidas de Seguridad previstas por la Normativa Aplicable, así como las indicadas por el Responsable del Tratamiento, asistiendo a este último para garantizar el cumplimiento del art. 32 del RGPD.

4.2. En el marco de las actividades de tratamiento de los Datos Personales relacionadas con la prestación de los Servicios, el Proveedor se compromete a adoptar medidas técnicas y organizativas adecuadas para impedir el tratamiento ilícito o no autorizado, así como para proteger los Datos Personales frente a su destrucción, alteración, pérdida, acceso no autorizado o divulgación, tal como se detalla en el Anexo II – Medidas Técnicas y Organizativas de Seguridad del presente Acuerdo.

4.3. El **Anexo II** describe las medidas adoptadas por el Proveedor para garantizar la confidencialidad, integridad, disponibilidad y resiliencia de los sistemas y Servicios, así como los procedimientos para restaurar de forma oportuna el acceso a los Datos Personales en caso de incidente de seguridad. Las medidas implementadas («Medidas de Seguridad») se definen en función del nivel de riesgo asociado a los Datos Personales tratados, teniendo en cuenta el estado de la técnica, los costes de implementación y la naturaleza, el contexto y las finalidades del tratamiento. El Cliente reconoce y acepta que dichas medidas son adecuadas para garantizar un nivel de seguridad conforme a los requisitos normativos aplicables sin perjuicio de las obligaciones del Proveedor conforme al artículo 32 del RGPD.

4.4. El Proveedor se reserva el derecho de actualizar o modificar las Medidas de Seguridad para garantizar una adaptación constante a la evolución tecnológica y normativa, siempre que dichos cambios no reduzcan el nivel global de protección de los Servicios.

4.5. Si el Cliente solicita la adopción de medidas de seguridad adicionales específicas distintas de las previstas, el Proveedor evaluará la viabilidad técnica y operativa de dichas solicitudes, reservándose la posibilidad de aplicar costes adicionales por cualquier implementación.

4.6. En el caso de productos instalados en las instalaciones del Cliente o de terceros designados por el Cliente (por ejemplo, soluciones on-premises), las Medidas de Seguridad adoptadas por el Proveedor se aplicarán exclusivamente a los Servicios que impliquen el tratamiento de Datos Personales por parte del Proveedor o de sus subencargados del tratamiento (por ejemplo, actividades de soporte y asistencia remota o servicios de migración).

4.7. En caso de que los Servicios permitan la integración con software o aplicaciones de terceros, el Proveedor no será responsable de las Medidas de Seguridad aplicadas por dichos terceros ni de las vulnerabilidades derivadas de la integración realizada directamente por el Cliente o por proveedores terceros salvo que la integración haya sido proporcionada por el Proveedor.

4.8. Sin perjuicio de las obligaciones de seguridad del Proveedor, el Cliente es responsable de adoptar todas las medidas necesarias para garantizar la protección de los Datos Personales tratados en el marco del uso de los Servicios por su personal o por cualesquiera partes autorizadas.

4.9. El Cliente se compromete a utilizar los Servicios de conformidad con las mejores prácticas de seguridad y a garantizar un nivel adecuado de protección frente a los riesgos asociados al tratamiento de los Datos Personales.

4.10. El Cliente debe implementar todas las medidas adecuadas para proteger las credenciales de autenticación, dispositivos y sistemas utilizados para acceder a los Servicios, así como para realizar copias de seguridad periódicas de los Datos Personales, con el fin de garantizar su restauración de conformidad con la normativa aplicable sin perjuicio de las eventuales obligaciones de copia de seguridad y restauración expresamente acordadas a cargo del Proveedor.

4.11. El Proveedor no será responsable de la protección de los Datos Personales que el Cliente o terceros traten fuera de los sistemas del Proveedor y de sus subencargados del tratamiento, incluidos los datos almacenados en papel o en las infraestructuras informáticas internas del Cliente (por ejemplo, centros de datos privados o servidores on-premises).

5. SUBENCARGADOS DEL TRATAMIENTO

5.1. Exclusivamente a efectos de la prestación de los Servicios cubiertos por el Contrato, y de conformidad con lo dispuesto en el presente Acuerdo, los Datos Personales podrán ser tratados por Subencargados del Tratamiento identificados por el Encargado del Tratamiento.

5.2. El Encargado del Tratamiento podrá recurrir, para la prestación efectiva de uno o varios Servicios, a otras sociedades pertenecientes al Grupo Namirial. La sociedad del Grupo Namirial que presta efectivamente un Servicio específico (la «**Entidad Prestadora**») se identifica para cada Servicio en la Hoja de Tratamiento correspondiente. Cuando la Entidad Prestadora no coincida con el Encargado del Tratamiento, actuará en virtud de acuerdos intragrupo entre las sociedades del Grupo Namirial, conformes con el artículo 28 del RGPD, preexistentes y separados del presente Acuerdo. El Responsable del Tratamiento así lo reconoce al firmar el presente Acuerdo. Cuando la Entidad Prestadora coincida con el Encargado del Tratamiento, los Subencargados del Tratamiento indicados en la Hoja de Tratamiento de Datos son contratados directamente por el propio Encargado del Tratamiento. En cualquier caso, el Encargado del Tratamiento seguirá siendo plenamente responsable frente al Responsable del Tratamiento por las actividades de Tratamiento llevadas a cabo por la Entidad Prestadora y sus Subencargados del Tratamiento por cuenta del Responsable del Tratamiento en virtud del presente Acuerdo.

5.3. Cualquier actividad de tratamiento en la que la Entidad Prestadora actúe con un rol distinto en materia de protección de datos se identificará en la Hoja de Tratamiento correspondiente y no se regirá por el presente Acuerdo, salvo que se disponga expresamente lo contrario.

5.4. El Encargado del Tratamiento se compromete a seleccionar a sus Subencargados del Tratamiento entre personas cuya experiencia, capacidad y fiabilidad ofrezcan garantías suficientes para implementar Medidas de Seguridad adecuadas, de forma que el Tratamiento cumpla todos los requisitos de la Normativa Aplicable y garantice la protección de los derechos del Interesado. En consecuencia, el Encargado del Tratamiento se compromete a celebrar contratos específicos u otros actos jurídicos vinculantes con los Subencargados del Tratamiento, mediante los cuales el Encargado del Tratamiento describa detalladamente sus tareas y les exija cumplir las mismas obligaciones impuestas por el Responsable del Tratamiento al Encargado del Tratamiento en virtud de la Normativa Aplicable y del presente Acuerdo.

5.5. En cualquier caso en que un Subencargado del Tratamiento incumpla sus obligaciones en materia de protección de Datos Personales, el Encargado del Tratamiento reconoce que conserva plena responsabilidad frente al Responsable del Tratamiento por el comportamiento de dicho Subencargado del Tratamiento. En consecuencia, el Encargado del Tratamiento se compromete a indemnizar y mantener indemne al Responsable del Tratamiento frente a cualquier daño, reclamación o solicitud de indemnización que pueda formularse contra el Responsable del Tratamiento como consecuencia del incumplimiento de sus obligaciones por parte del Subencargado del Tratamiento y, en general, de cualquier infracción de la Normativa Aplicable por parte del Subencargado del Tratamiento y de cualquiera de sus subcontratistas y/o personas autorizadas.

5.6. Las Hojas de Tratamiento identifican y enumeran los Subencargados del Tratamiento designados por el Encargado del Tratamiento y ya aprobados por el Responsable del Tratamiento. El Encargado del Tratamiento también se compromete a informar por escrito al Responsable del Tratamiento de cualquier cambio o sustitución previsto respecto de los Subencargados del Tratamiento, dando al Responsable del Tratamiento la posibilidad de oponerse a dichos cambios en un plazo de 30 (treinta) días desde la recepción de la comunicación correspondiente.

5.7. La comunicación a que se refiere el párrafo anterior podrá cumplirse alternativamente mediante la publicación de la lista actualizada de Subencargados del Tratamiento en la sección «Documentación» del sitio web del Proveedor, accesible a través de los datos de contacto indicados en el Anexo A de las Condiciones Generales.

6. TRANSFERENCIA DE DATOS PERSONALES

6.1. El Encargado del Tratamiento declara que no transferirá Datos Personales fuera del EEE, salvo que haya sido previamente y específicamente autorizado por escrito por el Responsable del Tratamiento. En caso de autorización, el Encargado del Tratamiento solo podrá transferir Datos Personales siguiendo instrucciones documentadas del Responsable del Tratamiento y, en particular, en pleno cumplimiento de los arts. 44, 45, 46 y 49 del RGPD. Se considerarán autorizadas las transferencias y los Subencargados no pertenecientes al EEE indicados en la Ficha de Tratamiento suscrita por las Partes.

6.2. Cuando una transferencia a un tercer país o a una organización internacional venga exigida por el Derecho de la Unión o de un Estado miembro al que esté sujeto el Encargado del Tratamiento, sin haber recibido instrucciones específicas del Responsable del Tratamiento, se aplicarán las obligaciones de notificación, verificación y documentación establecidas en el Artículo 3.7, junto con el artículo 48, cuando proceda, y el Capítulo V del RGPD.

6.3. En cualquier caso de transferencia de Datos Personales fuera del EEE, en la medida en que no exista una Decisión de Adecuación de la Comisión Europea para el país de destino de los Datos Personales, el Encargado del Tratamiento estará obligado a firmar, y a hacer que los destinatarios de los Datos Personales firmen, las Cláusulas Contractuales Tipo en su última versión adoptada por la Comisión Europea, garantizando que se aseguran las mismas obligaciones contenidas en ellas frente a cualquier otro destinatario ulterior de los Datos Personales en caso de la denominada transferencia posterior. Si y cuando sea necesario, el Encargado del Tratamiento deberá asimismo estipular la adopción de cualesquiera Medidas de Seguridad adicionales de conformidad con las Recomendaciones 01/2020 sobre medidas que complementan los instrumentos de transferencia para garantizar el cumplimiento del nivel de protección de los Datos Personales de la UE, así como las directrices aplicables del Comité Europeo de Protección de Datos («CEPD»).

7. ASISTENCIA AL RESPONSABLE DEL TRATAMIENTO

7.1. Teniendo en cuenta la naturaleza del Tratamiento y la información de que dispone, el Encargado del Tratamiento está obligado a prestar apoyo al Responsable del Tratamiento para que este pueda cumplir las obligaciones impuestas por la Normativa Aplicable a los responsables del tratamiento, tales como, a título de ejemplo y no exhaustivo, las obligaciones de:

a. notificar una Violación de la Seguridad de los Datos Personales a la Autoridad de Control competente sin dilación indebida y, cuando sea posible, a más tardar 72 horas después de haber tenido conocimiento de ella, salvo que sea improbable que dicha violación constituya un riesgo para los derechos y libertades de las personas físicas;
b. realizar una evaluación de impacto relativa a la protección de datos (EIPD) en relación con el Tratamiento regulado por el presente Acuerdo, si dicho Tratamiento presenta las características establecidas en el art. 35 del RGPD;
c. consultar a la Autoridad de Control competente en virtud del art. 36 del RGPD, si una EIPD indica que el Tratamiento regulado por el presente Acuerdo entrañaría un alto riesgo en ausencia de medidas adoptadas para mitigarlo;
d. responder a las solicitudes de ejercicio de los Derechos del Interesado, de conformidad con el Capítulo III del RGPD. Cuando el Encargado del Tratamiento reciba directamente dichas solicitudes, el Encargado del Tratamiento deberá (i) informar sin demora por escrito al Responsable del Tratamiento, adjuntando copia de la solicitud; y (ii) teniendo en cuenta la naturaleza del Tratamiento, asistir al Responsable del Tratamiento mediante las medidas técnicas y organizativas adecuadas dentro de su competencia para dar cumplimiento a dichas solicitudes.

8. VIOLACIONES DE LA SEGURIDAD DE LOS DATOS PERSONALES

8.1. En caso de que el Encargado del Tratamiento tenga conocimiento de una Violación de la Seguridad de los Datos Personales que afecte o pueda afectar, incluso indirectamente, a los sistemas y operaciones de Tratamiento utilizados por cuenta del Responsable del Tratamiento, o a los Datos Personales cubiertos por el presente Acuerdo, el Encargado del Tratamiento se compromete a informar al Responsable del Tratamiento mediante comunicación formal enviada a la dirección de Correo Electrónico de Notificación, sin dilación indebida y a más tardar en el plazo de 24 (veinticuatro) horas desde que tenga conocimiento de la Violación de la Seguridad de los Datos Personales.

8.2. Tras la detección de una anomalía o de una sospecha de Violación de la Seguridad de los Datos Personales cubierta por el presente Acuerdo, el Encargado del Tratamiento deberá iniciar un análisis preliminar para recopilar los datos relativos a la anomalía y, en todo caso, toda la información necesaria para la clasificación y gestión de la violación, incluidos los detalles relativos a la naturaleza del incidente, los datos afectados, las medidas adoptadas y los plazos de intervención.

8.3. El Encargado del Tratamiento se compromete a garantizar el cumplimiento de los plazos mencionados y a indemnizar y mantener indemne al Responsable del Tratamiento frente a cualquier daño, reclamación o solicitud de indemnización que pueda formularse contra el Responsable del Tratamiento como consecuencia del incumplimiento de sus obligaciones por parte del Encargado del Tratamiento y, en general, de cualquier infracción de la Normativa Aplicable por parte del Encargado del Tratamiento y de cualquiera de sus subcontratistas y/o personas autorizadas.

8.4. En caso de Violación de la Seguridad de los Datos Personales, el Encargado del Tratamiento se compromete a prestar, dentro del ámbito de su competencia y responsabilidad en virtud del Contrato, la máxima cooperación al Responsable del Tratamiento y a las Autoridades de Control competentes, con el fin de cumplir las obligaciones legales que resulten aplicables (por ejemplo, la obligación de notificación a la Autoridad de Control, la posible comunicación a los Interesados, la aplicación de medidas adecuadas para mitigar o prevenir riesgos y daños). A este respecto, el Responsable del Tratamiento se compromete a facilitar con prontitud al Encargado del Tratamiento prueba de cualquier comunicación intercambiada con las Autoridades de Control competentes en la que el Encargado del Tratamiento se vea implicado o mencionado de cualquier forma.

9. DURACIÓN. SUPRESIÓN Y DEVOLUCIÓN DE LOS DATOS PERSONALES

9.1. La designación como Encargado del Tratamiento en virtud del presente Acuerdo tendrá la misma duración que el Contrato, salvo resolución anticipada, en cuyo caso la designación seguirá siendo eficaz en la medida necesaria para completar las operaciones de Tratamiento requeridas para la terminación de la relación entre las Partes o para cumplir las obligaciones legales que les sean impuestas.

9.2. Una vez finalizadas las operaciones de Tratamiento encomendadas, así como al término, por cualquier causa, de la relación contractual con el Encargado del Tratamiento, este, a discreción del Responsable del Tratamiento, deberá (i) devolver al Responsable del Tratamiento los Datos Personales objeto de Tratamiento, o (ii) proceder a la destrucción completa de los Datos Personales y de todas sus copias, salvo en los casos en que la conservación de los datos sea exigida por el Derecho de la Unión o del Estado miembro (p. ej., obligaciones contables o fiscales) o sea necesaria para la formulación, el ejercicio o la defensa de reclamaciones. Los datos conservados en virtud de las excepciones anteriores, así como las copias de seguridad que no puedan suprimirse de inmediato por razones técnicas, se conservarán de forma protegida, no serán objeto de tratamiento ulterior y se suprimirán al vencimiento del correspondiente plazo de conservación o conforme a los ciclos normales de sobrescritura. En ambos casos, el Encargado deberá facilitar al Responsable una declaración escrita que acredite la devolución o supresión efectuada, indicando las eventuales excepciones mencionadas.

10. AUDITORÍAS E INSPECCIONES

10.1. El Encargado del Tratamiento pone a disposición del Responsable del Tratamiento toda la información necesaria para demostrar el cumplimiento de sus obligaciones en virtud del presente Acuerdo y de la Normativa Aplicable, y permitirá y contribuirá a las actividades de auditoría, incluidas las inspecciones llevadas a cabo por el Responsable del Tratamiento y/o un tercero designado por este.

10.2. Las actividades de auditoría se llevarán a cabo preferentemente en formato documental o mediante entrevistas, incluso a través de cuestionarios, solicitudes de información, revisión de certificaciones, informes de auditoría, políticas, procedimientos y demás documentación de cumplimiento facilitada por el Encargado del Tratamiento.

10.3. Salvo en caso de una Violación de la Seguridad de los Datos Personales con impacto material en los Datos Personales tratados por cuenta del Responsable del Tratamiento, o cuando una Autoridad de Control competente haya impuesto una sanción o medida vinculante contra el Encargado del Tratamiento directamente relacionada con los Servicios, el Responsable del Tratamiento deberá:

(a) facilitar al Encargado del Tratamiento un preaviso por escrito de al menos treinta (30) días;
(b) no realizar más de una auditoría por año natural;
(c) garantizar que la auditoría no exceda de dos (2) días laborables completos; y
(d) realizar la auditoría de manera que no perturbe de forma injustificada las operaciones ordinarias del negocio del Encargado del Tratamiento.

10.4. El Responsable del Tratamiento asumirá todos los costes, gastos y honorarios relativos a la auditoría, incluidos los costes en que incurran los auditores designados por el Responsable del Tratamiento. Cuando la auditoría requiera un tiempo o unos recursos que excedan los límites establecidos en el Artículo 10.3, el Encargado del Tratamiento informará de ello con antelación al Responsable del Tratamiento, y las Partes acordarán de buena fe reducir el alcance de la auditoría o asignar los costes adicionales al Responsable del Tratamiento.

10.5. Cuando la auditoría se lleve a cabo mediante cuestionarios, formularios o solicitudes documentales, se concederá al Encargado del Tratamiento un plazo razonable para responder, que no será inferior a treinta (30) días desde la recepción de la solicitud completa. Dicho plazo podrá ampliarse cuando sea razonablemente necesario, teniendo en cuenta la complejidad de la solicitud y la disponibilidad del personal del Encargado del Tratamiento.

10.6. El Responsable del Tratamiento, y cualquier tercero designado por este, utilizarán la información obtenida durante la auditoría exclusivamente con el fin de verificar el cumplimiento del presente Acuerdo y mantendrán dicha información en estricta confidencialidad.

11. COMUNICACIONES ENTRE LAS PARTES

11.1. A los efectos del presente Acuerdo, el Encargado del Tratamiento declara haber designado un Delegado de Protección de Datos y/o identificado el contacto de privacidad correspondiente, en su caso, de conformidad con la Normativa Aplicable. Los datos de contacto pertinentes del Encargado del Tratamiento, incluidos los del DPD o del contacto de privacidad, son los indicados para el Proveedor correspondiente en el Anexo A de las Condiciones Generales, según se identifica en la Propuesta Comercial. Dichos datos de contacto se utilizarán para todas las comunicaciones relativas a cuestiones de privacidad y protección de datos en virtud del presente Acuerdo.

11.2. El Encargado del Tratamiento se pondrá en contacto con el Responsable del Tratamiento, en todos los casos previstos en el presente Acuerdo, mediante comunicación enviada a la dirección de Correo Electrónico de Notificación facilitada por el Responsable del Tratamiento.

11.3. Las Partes se comprometen a notificarse mutuamente y con prontitud cualquier cambio en sus direcciones de contacto. En ausencia de dicha notificación oportuna, las comunicaciones enviadas a la dirección desactualizada se considerarán válidas y eficaces.

ANEXO I

DEFINICIONES

a) «**Acuerdo**» significa el presente Acuerdo de Encargo del Tratamiento de Datos, incluidos los antecedentes y los Anexos;

b) «**Administradores de Sistemas**» significa las Personas Autorizadas responsables de la gestión y mantenimiento de un sistema de tratamiento o de sus componentes, según se identifica en el artículo 32 del RGPD y en los requisitos nacionales aplicables relativos a la asignación de las funciones de administrador de sistemas, tal y como se detalle además, en su caso, en la Hoja de Tratamiento aplicable;

c) «**Autoridad de Control**» significa cualquier autoridad de control independiente en virtud del Capítulo VI del RGPD, competente para supervisar y garantizar la aplicación de las disposiciones legales en materia de protección de Datos Personales, en relación con el Tratamiento de Datos Personales llevado a cabo en la ejecución del Contrato;

d) «**Categorías Especiales de Datos Personales**» significa los Datos Personales que revelen el origen racial o étnico, las opiniones políticas, las convicciones religiosas o filosóficas, o la afiliación sindical, así como el tratamiento de datos genéticos, datos biométricos dirigidos a identificar de manera unívoca a una persona física, datos relativos a la salud o datos relativos a la vida sexual o la orientación sexual de una persona física, según se identifica en el art. 9 del RGPD;

e) «**Cláusulas Contractuales Tipo**» significa las cláusulas adoptadas por la Comisión Europea mediante la Decisión 2021/914/UE, de 4 de junio de 2021, para la transferencia de Datos Personales desde un responsable del tratamiento establecido en la Unión Europea («UE») / Espacio Económico Europeo («**EEE**») a una entidad no perteneciente a la UE o al EEE que actúe como encargado del tratamiento;

f) «**Contrato**» significa el contrato suscrito entre las Partes para la prestación de los Servicios;

g) «**Datos Personales**» significa cualquier información sobre una persona física identificada o identificable (Interesado) tratada por el Encargado del Tratamiento, por cuenta del Responsable del Tratamiento, en relación con la ejecución del Contrato;

h) «**Derechos de los Interesados**» significa los derechos reconocidos al Interesado por la Normativa Aplicable. Dentro de los límites de aplicabilidad del RGPD, «Derechos del Interesado» significa, por ejemplo, el derecho a solicitar al responsable del tratamiento el acceso, la rectificación o la supresión de los Datos Personales, el derecho a limitar el Tratamiento de los datos del Interesado o el derecho de oposición al Tratamiento, así como el derecho a la portabilidad de los datos;

i) «**Correo Electrónico de Notificación**» significa la dirección (o direcciones) de correo electrónico facilitada por el Cliente en el momento de la firma del Contrato, o proporcionada a través de otro canal oficial al Encargado del Tratamiento, a la que el Cliente desea recibir las notificaciones del Encargado del Tratamiento;

j) «**Normativa Aplicable**» significa todas las leyes y reglamentos sobre protección de Datos Personales aplicables al Tratamiento de Datos Personales en virtud del Contrato, incluido el Reglamento (UE) 2016/679 («RGPD»), las leyes y reglamentos nacionales de protección de datos aplicables de los Estados miembros de la UE, según sean aplicables conforme a su ámbito territorial y de aplicación, y cualesquiera medidas, decisiones, directrices o instrucciones vinculantes emitidas por la Autoridad de Control competente;

k) «**Medidas de Seguridad**» significa las medidas técnicas y organizativas, conforme al art. 32 del RGPD, adecuadas para garantizar un nivel de seguridad apropiado de los Datos Personales, así como todas las medidas necesarias para prevenir o al menos minimizar cualquier riesgo razonablemente previsible de destrucción, pérdida, alteración, divulgación o acceso no autorizados, accidental o ilícito, a los Datos Personales tratados;

l) «**Personas Autorizadas**» significa las personas físicas dentro de la estructura organizativa del Encargado del Tratamiento específicamente identificadas por escrito y autorizadas para acceder y tratar Datos Personales en el marco de la ejecución del Contrato, y que actúan bajo el control y siguiendo las instrucciones del Encargado del Tratamiento;

m) «**Encargado del Tratamiento**» significa, con carácter general, la persona física o jurídica, autoridad pública, servicio u otro organismo que trate Datos Personales por cuenta de un responsable del tratamiento;

n) «**Servicios**» significa los servicios prestados en virtud del Contrato;

o) «**Sistemas del Responsable del Tratamiento**» significa las infraestructuras y sistemas que eventualmente ponga a disposición el Responsable del Tratamiento y/o terceros designados por este, sobre los que el Encargado del Tratamiento deba llevar a cabo el Tratamiento;

p) «**Subencargado del Tratamiento**» significa una entidad identificada por el Encargado del Tratamiento que lleva a cabo, total o parcialmente, el Tratamiento de Datos Personales encomendado al Encargado del Tratamiento, de conformidad con las obligaciones e

instrucciones establecidas por el Responsable del Tratamiento, y que ha sido expresamente autorizada por este último;

q) «**Subencargado del Tratamiento Intragrupo**» significa la sociedad perteneciente al Grupo Namirial que actúa como Subencargado del Tratamiento para la prestación efectiva de uno o varios Servicios, en virtud de acuerdos intragrupo preexistentes entre las sociedades del Grupo Namirial, conformes con el artículo 28 del RGPD y separados del presente Acuerdo;

r) «**Entidad Prestadora**» significa la sociedad del Grupo Namirial que presta efectivamente el Servicio específico cubierto por cada Hoja de Tratamiento de Datos. La Entidad Prestadora podrá coincidir con el Encargado del Tratamiento o actuar como su Subencargado del Tratamiento Intragrupo. En ambos casos, se identifica en la Hoja de Tratamiento correspondiente;

s) **«Responsable del Tratamiento»** significa, con carácter general, la persona física o jurídica, autoridad pública, servicio u otro organismo que, solo o junto con otros, determine los fines y medios del tratamiento de datos personales**;**

t) **«Tratamiento»** significa cualquier operación o conjunto de operaciones realizadas sobre Datos Personales o conjuntos de Datos Personales, ya sea por procedimientos automatizados o no, como la recogida, el registro, la organización, la estructuración, la conservación, la adaptación o modificación, la extracción, la consulta, la utilización, la comunicación por transmisión, difusión o cualquier otra forma de habilitación de acceso, el cotejo o interconexión, la limitación, la supresión o la destrucción.

ANEXO II

MEDIDAS TÉCNICAS Y ORGANIZATIVAS DE SEGURIDAD

1. MEDIDAS ORGANIZATIVAS DE SEGURIDAD

TIPO DE MEDIDA	DESCRIPCIÓN
Políticas y Normativas Internas	El Encargado del Tratamiento ha adoptado un conjunto de políticas, procedimientos y normativas internas, vinculantes para todo el personal autorizado a tratar Datos Personales. Estas políticas y directrices definen las normas para el uso seguro de los recursos informáticos y establecen una normativa interna específica para la gestión de la información, de obligado cumplimiento para todos los usuarios. El objetivo es garantizar el cumplimiento de los principios de confidencialidad, integridad y disponibilidad de los Datos Personales, minimizando los riesgos de acceso no autorizado o uso indebido de la información en todas las sociedades del grupo.
Autorización de Acceso y Controles Lógicos	El Encargado del Tratamiento define perfiles de acceso conforme al principio de mínimo privilegio necesario para el desempeño de las tareas asignadas. Los perfiles de autorización se identifican y configuran antes del inicio del tratamiento, para limitar el acceso únicamente a los Datos Personales necesarios para realizar las operaciones de tratamiento. Para las operaciones más sensibles se adopta la autenticación de dos factores (MFA) para reforzar la seguridad del acceso. Estos perfiles están sujetos a comprobaciones periódicas para verificar que subsisten las condiciones para mantener los perfiles asignados.
Supervisión de Accesos	El acceso a los sistemas que tratan Datos Personales se registra y supervisa, con análisis periódico de los registros para identificar cualquier anomalía o actividad sospechosa.
Gestión de Cambios	El Encargado del Tratamiento ha adoptado un procedimiento específico que regula el proceso de Gestión de Cambios, en consideración de la introducción de innovaciones tecnológicas o de cambios en su estructura organizativa.
Gestión de Incidentes y Continuidad de Negocio	El Encargado del Tratamiento ha implementado un procedimiento específico de Gestión de Incidentes para garantizar el restablecimiento de las operaciones normales del servicio con la mayor celeridad posible, manteniendo los mejores niveles de servicio. Los incidentes se clasifican por gravedad e impacto en los Datos Personales. El personal recibe formación para gestionar eventos de seguridad y ejecutar procedimientos de contención. Se realizan pruebas periódicas sobre la capacidad de respuesta de la organización ante incidentes. Se ha implementado un Plan de Continuidad de Negocio para garantizar la resiliencia del servicio incluso en situaciones de emergencia.
Medidas para Garantizar una Conservación Limitada de los Datos	El Encargado del Tratamiento sigue los principios de protección de datos desde el diseño y por defecto. Medidas técnicas: no se recopilan más Datos Personales de los necesarios para la finalidad correspondiente; uso de configuraciones predeterminadas que respetan la protección de datos. Medidas organizativas: política de protección de datos conforme a los principios de «privacidad desde el diseño / por defecto» incluida en la Política de Privacidad y Protección de Datos Personales del Grupo (SCS-P14); se realizan comprobaciones de seguridad

	OWASP para el desarrollo móvil seguro (véase la Política de Codificación Segura del Grupo, SCS-P08); análisis perimetral de aplicaciones web.
Violación de la Seguridad de los Datos	El Encargado del Tratamiento ha implementado un procedimiento específico para la gestión de eventos e incidentes con potencial impacto en los Datos Personales, que define funciones y responsabilidades, el proceso de detección (sospechada o confirmada), la aplicación de contramedidas, la respuesta y contención del incidente/violación, así como los métodos para comunicar con prontitud al Responsable del Tratamiento las violaciones de la seguridad de los Datos Personales. Por lo que respecta al Encargado del Tratamiento, este procedimiento identifica al menos: la naturaleza de la violación de la seguridad de los Datos Personales, incluyendo, cuando sea posible, las categorías y el número aproximado de interesados afectados, así como las categorías y el número aproximado de registros de Datos Personales afectados; las posibles consecuencias de la violación de la seguridad de los Datos Personales; las medidas adoptadas o propuestas para hacer frente a la violación de la seguridad de los Datos Personales y, en su caso, para mitigar sus posibles efectos adversos.
Formación	Para garantizar un nivel adecuado de concienciación, el Encargado del Tratamiento facilita formación periódica sobre el correcto tratamiento de los Datos Personales y la seguridad de la información. La formación es obligatoria para todo el personal que accede a Datos Personales. Se realizan pruebas y comprobaciones para evaluar el nivel de comprensión de las políticas de seguridad. Se organizan campañas simuladas de ciberataques (por ejemplo, pruebas de phishing) para formar al personal sobre las amenazas más comunes. La formación se actualiza periódicamente para reflejar la evolución normativa y tecnológica.
Gestión de Subencargados del Tratamiento	Cuando el Encargado del Tratamiento recurre a Subencargados del Tratamiento, se implementan controles estrictos para verificar su cumplimiento de las medidas de seguridad exigidas. Cada Subencargado del Tratamiento debe cumplir estándares de seguridad equivalentes a los del Encargado del Tratamiento. Se realizan auditorías e inspecciones periódicas para verificar el cumplimiento por parte del proveedor. El Encargado del Tratamiento mantiene un registro actualizado de Subencargados del Tratamiento.
Copia de Seguridad y Recuperación de Datos	Para garantizar la disponibilidad de los datos y la resiliencia ante fallos, el Encargado del Tratamiento implementa un sistema de copia de seguridad y recuperación ante desastres que incluye: copias de seguridad periódicas con políticas de conservación definidas; protección de las copias de seguridad mediante cifrado y acceso controlado; pruebas periódicas para garantizar una rápida recuperación de datos cuando sea necesario; replicación de datos en centros de datos seguros para evitar la pérdida de información crítica.
Procedimientos para Probar, Verificar y Evaluar Periódicamente la Eficacia de las Medidas Técnicas y Organizativas para Garantizar la Seguridad del Tratamiento	Las políticas internas relativas a las medidas de seguridad se revisan periódicamente y se confirma su adecuación y eficacia mediante auditorías internas continuas y, anualmente, por organismos de certificación independientes, externos y acreditados, en el marco de las auditorías de seguimiento y recertificación de las normas ISO 9001 e ISO 27001.
Designación del CISO	Para garantizar un nivel adecuado de seguridad de la información y el cumplimiento de la normativa aplicable, el Encargado del Tratamiento ha designado un Responsable de Seguridad de la Información (CISO), cuya función principal consiste en: supervisar la implementación y eficacia de las

	medidas de seguridad adoptadas para la protección de los Datos Personales; hacer seguimiento de la evolución de las amenazas cibernéticas y promover la actualización continua de las políticas de seguridad; coordinar las actividades de respuesta a incidentes de seguridad; definir estrategias de mejora de la seguridad para la protección de los activos corporativos. El CISO opera en sinergia con las demás funciones corporativas implicadas en la seguridad y la gestión de la protección de datos.
Certificaciones de Cumplimiento	La lista completa de las certificaciones que posee el Proveedor está disponible en la siguiente dirección: https://www.namirial.com/ es/compania/certificaciones/

2. MEDIDAS TÉCNICAS DE SEGURIDAD

TIPO DE MEDIDA	DESCRIPCIÓN
Planificación de Capacidad y Supervisión del Rendimiento	El Encargado del Tratamiento implementa un proceso continuo de análisis y optimización de los recursos informáticos para garantizar un rendimiento adecuado en la prestación de los Servicios y en la gestión de los Datos Personales. El sistema incluye la supervisión proactiva de la capacidad de procesamiento, el almacenamiento y el ancho de banda de la red. Se proyectan las necesidades futuras para garantizar la escalabilidad y la continuidad operativa. Se realizan pruebas periódicas de carga y resiliencia para prevenir problemas derivados de sobrecargas o picos de uso.
Seguridad y Hardening de Sistemas	Para minimizar las vulnerabilidades y mejorar la protección de la infraestructura informática, el Encargado del Tratamiento aplica medidas de hardening a los sistemas operativos, al software de aplicaciones y a las redes corporativas. Los sistemas se configuran siguiendo las mejores prácticas de seguridad para limitar la exposición a riesgos. Se deshabilitan las funcionalidades innecesarias y se restringe el acceso a los servicios de red. Las configuraciones se revisan y actualizan periódicamente conforme a la evolución de las amenazas.
Gestión de Parches y Actualizaciones de Seguridad	El Encargado del Tratamiento mantiene un proceso estructurado de gestión de actualizaciones para garantizar la protección frente a vulnerabilidades del software. Las actualizaciones de seguridad se aplican con prontitud en función de la gravedad de las vulnerabilidades. Existen procedimientos de prueba previos a la publicación para evitar impactos negativos en la continuidad del servicio. Los sistemas críticos están sujetos a comprobaciones periódicas para identificar cualquier vulnerabilidad no resuelta.
Protección de la Red y de los Sistemas	Los Datos Personales están protegidos mediante soluciones avanzadas de seguridad perimetral y detección de intrusiones, entre las que se incluyen: cortafuegos de nueva generación para un filtrado avanzado del tráfico; sistemas IDPS (Intrusion Detection & Prevention System) para identificar y bloquear actividades sospechosas; segmentación de red para limitar los riesgos de propagación en caso de ataque.
Protección contra Malware y Amenazas Cibernéticas	El Encargado del Tratamiento emplea herramientas avanzadas de protección para mitigar los riesgos derivados de malware y ciberataques: antivirus y antimalware actualizados

	regularmente para detectar y bloquear amenazas en tiempo real; sistemas de sandboxing para analizar y aislar archivos sospechosos antes de su ejecución; supervisión de amenazas para prevenir ataques de día cero.
Seguridad de las Comunicaciones y Protección de la Transmisión de Datos	El Encargado del Tratamiento adopta protocolos de seguridad avanzados para garantizar la integridad y confidencialidad de las comunicaciones: cifrado de extremo a extremo para proteger los datos en tránsito; autenticación y certificados digitales para verificar la integridad de las comunicaciones; segmentación mediante VPN y redes privadas para reducir los riesgos de interceptación.
Protección Física de las Infraestructuras Informáticas	El acceso a las instalaciones en las que se almacenan o tratan Datos Personales está sujeto a medidas reforzadas de seguridad física: acceso controlado mediante sistemas de tarjetas de identificación, registro de entradas y autorización previa. Videovigilancia 24 horas y alarmas antiintrusión. Medidas de seguridad medioambiental, incluidos sistemas de protección contra incendios, redundancia de los sistemas eléctricos y de climatización, SAI y generadores de reserva para garantizar la continuidad operativa. Procedimientos de emergencia y recuperación ante desastres, con simulacros periódicos para probar los planes de respuesta a incidentes.
Gestión de Credenciales y Acceso a Sistemas	Para impedir el acceso no autorizado, el Encargado del Tratamiento implementa un estricto sistema de autenticación y gestión de credenciales: Autenticación Multifactor para los usuarios con acceso a Datos Personales e información sensible; política de contraseñas avanzada con requisitos de longitud, complejidad y caducidad periódica; revocación inmediata del acceso en caso de finalización de la relación laboral o cambio de funciones.
Gestión de los Administradores de Sistemas	Los Administradores de Sistemas, en su condición de sujetos con privilegios elevados, están sometidos a un control y supervisión estrictos. El Encargado del Tratamiento mantiene una lista actualizada y documentada de los Administradores de Sistemas. Las actividades administrativas se registran y quedan documentadas mediante registros protegidos e inalterables. Se realizan auditorías periódicas para verificar las acciones de los administradores y la correcta aplicación de las políticas de seguridad.