TÉRMINOS Y CONDICIONES GENERALES DE CONTRATACIÓN

Última actualización: 23 de junio de 2026

El presente documento (en adelante, el "**Contrato**" o los "**Términos y Condiciones**") regula la contratación y el uso de las soluciones informáticas, software y servicios asociados (en adelante, las "**Soluciones**") comercializadas por FLEXXIBLE INFORMATION TECHNOLOGY, S.L. (en adelante, "**FLEXXIBLE**" o el "**PROVEEDOR**"), ya sea directamente o a través de terceros autorizados por FLEXXIBLE para la comercialización de sus Soluciones (en adelante, "**PARTNER**"")

La aceptación de estos Términos y Condiciones, así como el uso de las Soluciones, implica que usted (en adelante, el "**CLIENTE**"), ha leído, entiende y acepta vincularse legalmente por este Contrato en su totalidad.

El presente Contrato se perfecciona y entra en vigor en el momento en que el CLIENTE acepta estos Términos y Condiciones y realiza el pago.

El CLIENTE, con carácter previo a la contratación, ha sido informado expresamente de la existencia de estos Términos y Condiciones y se ha puesto a disposición un ejemplar en un soporte que permite su descarga, almacenamiento y reproducción, pudiendo el CLIENTE conservarlo.

1. IDENTIFICACIÓN DE LAS PARTES

FLEXXIBLE INFORMATION TECHNOLOGY, S.L., con N.I.F. B-63002927 y domicilio social en C/ de Vallhonrat, 45, Terrassa, 08221, Barcelona, inscrita en el Registro Mercantil de Barcelona al Tomo 47338, Folio 92, Sección 8ª, Hoja B-259301.

Teléfono de contacto: +34 937 880 333

Correo electrónico: info@flexxible.com

CLIENTE: La persona jurídica o profesional que contrata las Soluciones ofrecidas por FLEXXIBLE y cuyos datos identificativos y de facturación son proporcionados durante el proceso de contratación. El CLIENTE garantiza que tiene la capacidad legal y la representación suficiente para vincularse por estos Términos y Condiciones.

2. DESCRIPCIÓN Y ALCANCE DE LAS SOLUCIONES Y SERVICIOS

2.1. OBJETO

El presente Contrato otorga al CLIENTE licencia de uso sobre las Soluciones, cuyos derechos de explotación exclusivos son titularidad de FLEXXIBLE, y regula las condiciones de su utilización según el Plan Contratado por parte de los Usuarios que designe el CLIENTE (en adelante, podrán ser referidos conjuntamente como "**USUARIOS**" o individualmente como el "**USUARIO**").

2.2. ALCANCE DE LAS SOLUCIONES DE FLEXXIBLE

El alcance, las características, funcionalidades, requisitos de funcionamiento y demás aspectos relativos a las distintas Soluciones de FLEXXIBLE se corresponderán con el Plan Contratado seleccionado por el CLIENTE durante el proceso de contratación con FLEXXIBLE o con un PARTNER.

2.3. MODIFICACIÓN DE LAS SOLUCIONES Y/O SERVICIOS

FLEXXIBLE se reserva el derecho a modificar las características de las Soluciones con el fin de adaptarlas a cambios en las necesidades comerciales de FLEXXIBLE, cambios normativos o avances técnicos que resulten necesarios para mejorar la funcionalidad, seguridad y eficiencia de las Soluciones. Dichas modificaciones podrán consistir, de forma ejemplificativa pero no limitativa, en actualizaciones, mejoras, parches de seguridad y cualquier otra alteración que FLEXXIBLE considere pertinente para mantener la calidad de las Soluciones.

FLEXXIBLE notificará al CLIENTE por correo electrónico cualquier modificación significativa o la cancelación de las Soluciones con al menos quince (15) días de antelación.

También podrán modificarse las condiciones de prestación de los Servicios o cancelarse parte de los mismos de forma unilateral por FLEXXIBLE, debiendo notificar de estos cambios al CLIENTE de forma previa a la entrada en vigor de los mismos con al menos quince (15) días de antelación.

Las anteriores modificaciones podrán ser realizadas a instancia de FLEXXIBLE, siempre y cuando dichas modificaciones sean necesarias para cumplir con los requisitos técnicos, de seguridad, de cumplimiento normativo o para mejorar la experiencia del Cliente. El CLIENTE podrá resolver el Contrato en caso de desacuerdo con la modificación de las Soluciones y/o los Servicios durante el plazo de preaviso remitiendo una comunicación fehaciente a FLEXXIBLE. En el supuesto de contratación directa por el CLIENTE con FLEXXIBLE, FLEXXIBLE abonará al CLIENTE la parte proporcional del precio por el tiempo que medie desde la resolución del Contrato hasta la finalización del plazo de vigencia, con exclusión de los costes no recuperables (entre otros, alta, configuración, puesta en marcha, licencias activadas)

El CLIENTE reconoce y acepta que FLEXXIBLE no será

responsable de ningún perjuicio que pueda derivarse de las modificaciones o de la cancelación de las Soluciones o de los Servicios, siempre y cuando se haya otorgado el plazo de preaviso previsto en la presente Cláusula.

3. INICIO Y DURACIÓN DEL CONTRATO

La duración del Contrato será la establecida en el Plan Contratado por el CLIENTE. Salvo que se indique lo contrario en las condiciones del plan, el Contrato se prorrogará automáticamente por períodos de igual duración, a menos que cualquiera de las Partes notifique a la otra su voluntad de no renovar con una antelación mínima de quince (15) días a la fecha de vencimiento.

4. DEMO o PROOF OF CONCEPT

En el caso que se haya ofrecido al CLIENTE una Proof of Concept (en adelante, "PoC") de carácter gratuito, el CLIENTE tendrá el acceso a las Soluciones con el alcance que se determine en la PoC, siendo los presentes Términos y Condiciones igualmente aplicables.

En cualquier caso, FLEXXIBLE podrá, a su sola discreción cancelar la utilización de las Soluciones en el periodo de PoC.

5. PROPIEDAD DE LA INFORMACIÓN ALMACENADA EN LAS SOLUCIONES Y SEGURIDAD DE LA INFORMACIÓN

Toda la información almacenada y tratada en las Soluciones de FLEXXIBLE será tratada como confidencial. Toda la información se guarda de manera segura y solo un Usuario autorizado y calificado puede acceder a ella.

El CLIENTE es titular de todos los derechos de propiedad intelectual e industrial sobre la información, los contenidos y los datos que él o sus Usuarios autorizados introduzcan, almacenen, procesen o generen a través de las Soluciones (en adelante, el "**Contenido del Cliente**"). El presente Contrato no transfiere a FLEXXIBLE ningún derecho de propiedad sobre el Contenido del Cliente.

El CLIENTE autoriza a FLEXXIBLE para acceder y utilizar el Contenido del Cliente y los datos generados por el uso de las Soluciones en la medida necesaria para (i) prestar los Servicios; (ii) mantener, asegurar y mejorar las Soluciones; (iii) cumplir obligaciones legales; y (iv) atender incidencias y soporte, todo ello de conformidad con lo estipulado en el presente Contrato y en el Anexo I. Contrato de Tratamiento de Datos.

El CLIENTE será el responsable de cumplir con toda la normativa que pueda aplicarse al tratamiento de la información, incluida la información confidencial, y los datos personales almacenados y tratados por las Soluciones.

FLEXXIBLE y el CLIENTE se obligan al cumplimiento de lo establecido en la Política de Ciberseguridad para las Soluciones y Servicios Flexxible, incorporado al Contrato como Anexo II, en aquellos supuestos en que FLEXXIBLE sea proveedor de servicios en la nube.

El CLIENTE se obliga a no eludir, desactivar o interferir de ninguna manera con las funciones de seguridad de las Soluciones, que podrían poner en peligro la seguridad de las informaciones y datos almacenados en dichas Soluciones**.** El CLIENTE asume la total responsabilidad por el incumplimiento por parte de los Usuarios de las obligaciones anteriores.

El CLIENTE acepta que FLEXXIBLE pueda acceder, almacenar y procesar cualquier información del CLIENTE, de sus empleados y de sus colaboradores autorizados que queden almacenados en las Soluciones contratadas para su mantenimiento y actualización y la prestación del resto de Servicios asociados a las Soluciones.

Al enviar sugerencias u otro tipo de comentarios en relación con las Soluciones, el CLIENTE acepta que FLEXXIBLE pueda utilizar y compartir estos comentarios para cualquier propósito sin que se le deba compensar por ello al CLIENTE.

6. PRECIO, PAGO Y FACTURACIÓN

La presente Cláusula sólo será aplicable en los supuestos de contratación directa de las Soluciones por parte del CLIENTE a FLEXXIBLE.

En el supuesto que el CLIENTE contratase las Soluciones a través de un PARTNER, se aplicarán las condiciones acordadas entre el CLIENTE y PARTNER.

6.1. PRECIO

El precio por la concesión de la licencia sobre las Soluciones y por la prestación de los Servicios es el que se determina en el Plan Contratado seleccionado en el momento de la contratación.

En caso de prórroga automática, el precio será el notificado por FLEXXIBLE al CLIENTE con antelación al inicio del plazo establecido en la Cláusula 3.

6.2 FACTURACIÓN

FLEXXIBLE emitirá las facturas correspondientes a los Servicios contratados con la periodicidad acordada en el Plan Contratado. El CLIENTE acepta recibir las facturas en formato electrónico, que serán remitidas a la dirección de correo electrónico facilitada durante el proceso de contratación.

6.3. MODALIDADES DE PAGO

El CLIENTE abonará el Precio a través de una de las

modalidades de pago ofrecidas en el proceso de la contratación. Las facturas deberán ser abonadas según el plazo indicado en la factura.

6.4 PAGO MEDIANTE TRANSFERENCIA

En caso de pago por el CLIENTE mediante transferencia bancaria, estos se realizarán en la cuenta indicada en la factura. El CLIENTE recibirá factura electrónica conforme a la normativa vigente de facturación electrónica en España.

El impago o demora en pago generará intereses de demora al tipo legal del dinero vigente incrementado en dos puntos, sin perjuicio de la posibilidad de suspensión del Servicio conforme a la Cláusula 14.

El CLIENTE se obliga a aplicar medidas de diligencia reforzada de comprobación en el supuesto que reciba cualquier comunicación o solicitud de FLEXXIBLE que modifique cualquier aspecto relativo a la facturación o forma de pago, incluyéndose de forma expresa el cambio de cuenta corriente bancaria donde realizar los pagos de las facturas. En tales supuestos, el CLIENTE se obliga a realizar las comprobaciones oportunas para garantizar que tanto las facturas recibidas como las cuentas bancarias de abono son titularidad de FLEXXIBLE. Las facturas solamente se entenderán pagadas si su importe es abonado en una cuenta corriente titularidad de FLEXXIBLE y el CLIENTE. En el supuesto que el CLIENTE realizase el pago, por error o fraude, en una cuenta corriente que no fuese titularidad de FLEXXIBLE, el pago de la factura se tendrá por no hecho, estando FLEXXIBLE indemne de cualquier responsabilidad por el pago o transferencia del CLIENTE en una cuenta corriente que no fuese de su titularidad.

6.5. RETRASO EN EL PAGO

En caso de retraso en el pago, se podrá suspender temporalmente el acceso a las Soluciones y la prestación de los Servicios si, tras haber requerido el pago al CLIENTE, éste no lo hubiera hecho efectivo en un plazo de 15 días desde dicho requerimiento. Transcurrido dicho plazo, se realizará un segundo requerimiento de pago, concediendo al CLIENTE un plazo de 10 días para realizar el correspondiente pago. Pasado este plazo, se resolverá el Contrato, cesando definitivamente el acceso a las Soluciones.

En caso de retraso o impago, el CLIENTE se obliga a reembolsar a FLEXXIBLE un interés de demora equivalente al interés legal del dinero incrementado en dos (2) puntos desde la fecha de vencimiento hasta el completo pago, así como todos los gastos (incluyendo honorarios de abogados y procuradores) incurridos por FLEXXIBLE en el cobro de los pagos atrasados.

No habrá reembolsos por períodos parciales de uso de las Soluciones, salvo resolución por incumplimiento grave imputable exclusivamente a FLEXXIBLE, en cuyo caso se reembolsará el importe equivalente a los días restantes hasta la fecha de finalización del Contrato.

7. OBLIGACIONES DEL CLIENTE

Además de las obligaciones previstas en el Contrato, el CLIENTE se obliga además a:

a. Efectuar un correcto uso de las Soluciones y Servicios, conforme a la licencia concedida y a la documentación técnica facilitada por FLEXXIBLE.

b. Pagar puntualmente el precio, conforme a los términos de facturación acordados.

c. Disponer de los sistemas, equipamiento y conexiones necesarios para el correcto funcionamiento de las Soluciones, así como informar a sus USUARIOS de las condiciones de acceso y los requisitos mínimos.

d. Cooperar con FLEXXIBLE en la implementación, mantenimiento y resolución de incidencias de las Soluciones, proporcionando la información y acceso razonablemente necesario.

e. Hacer un uso de los Servicios y Soluciones de conformidad con la normativa vigente, incluida, a título enunciativo y no limitativo, la de propiedad intelectual e industrial, seguridad de la información, protección de datos (RGPD y LOPDGDD), evitando cualquier uso ilícito o que pueda generar daños y perjuicios a terceros o a FLEXXIBLE.

f. Designar y mantener actualizado el listado de Usuarios autorizados que tendrán acceso a las Soluciones, poniéndolo a disposición de FLEXXIBLE cuando le sea requerido.

g. Notificar a FLEXXIBLE sin dilación indebida cualquier incidencia, brecha de seguridad o uso no autorizado de las Soluciones de la que tenga conocimiento.

h. Colaborar en el cumplimiento de la Política de Ciberseguridad de las Soluciones y Servicios de FLEXXIBLE., en aquellos casos en los que FLEXXIBLE sea proveedor de servicios en la nube.

El incumplimiento de cualquiera de estas obligaciones facultará a FLEXXIBLE a resolver el Contrato conforme a la Cláusula 15, sin perjuicio de la reclamación de daños y perjuicios.

8. OBLIGACIONES DE FLEXXIBLE

FLEXXIBLE se obliga a:

a. Poner a disposición del CLIENTE y sus Usuarios autorizados las Soluciones contratadas.

b. Mantener las Soluciones en condiciones operativas, asegurando los niveles de servicio definidos en el Anexo III, SLA.

c. Proporcionar el servicio de atención al CLIENTE y gestión de incidencias de conformidad con el Plan Contratado.

d. Ejecutar actualizaciones, mejoras y parches de seguridad necesarios para mantener la funcionalidad, seguridad y cumplimiento normativo de las Soluciones.

e. Tratar los datos personales y contenidos del CLIENTE conforme al Reglamento (UE) 2016/679, General de Protección de Datos ("RGPD") y la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y Garantía de los Derechos Digitales (LOPDGDD) en lo relativo a la adopción de medidas técnicas y organizativas adecuadas.

f. Mantener la confidencialidad de la información del CLIENTE conforme a la Cláusula 17.10 y no divulgarla salvo obligación legal o con autorización expresa del CLIENTE.

g. Notificar al CLIENTE sin dilación indebida cualquier brecha de seguridad, incidente o interrupción relevante que afecte a las Soluciones o a los datos del CLIENTE, conforme a lo previsto en el RGPD.

h. Cumplir con la Política de Ciberseguridad de las Soluciones y Servicios, en el supuesto que FLEXXIBLE sea proveedor de servicios en la nube.

9. CONDICIONES DE ACCESO

9. 1. EQUIPAMIENTO MÍNIMO

Los requisitos de equipamiento mínimo son los identificados en el Plan Contratado. Es responsabilidad exclusiva del CLIENTE disponer del equipo mínimo necesario para el uso de las Soluciones.

9. 2. PROCESO DE REGISTRO DEL USUARIO Y CREACIÓN DE CONTRASEÑA

El nombre de usuario y contraseña (en adelante, "Credenciales") de acceso a las Soluciones se asignarán durante el proceso de registro del CLIENTE en las Soluciones.

En este sentido, el nombre de usuario a las Soluciones será una dirección de correo electrónico del CLIENTE. La contraseña para el acceso a las Soluciones deberá ser establecida por el Usuario en el momento del registro.

Se habilitará el número máximo de Usuarios con acceso a las Soluciones según el Plan Contratado. Cada Usuario con acceso a las Soluciones deberá responsabilizarse de asignar una contraseña única, evitando utilizar contraseñas de otros Usuarios del CLIENTE.

La contraseña de acceso a las Soluciones deberá cumplir determinados requisitos mínimos de seguridad de acuerdo con los estándares establecidos por las autoridades competentes:

- La contraseña deberá tener una longitud de, al menos, ocho (8) caracteres;
- La clave de acceso deberá estar compuesta por letras mayúsculas y minúsculas;
- También deberá contener, al menos, un número o carácter especiales (como @, #, €, ! o &).

Asimismo, FLEXXIBLE recomienda al CLIENTE no incluir información personal (como fechas de nacimiento o números de teléfono), palabras o combinaciones comunes.

9.3. USO DILIGENTE Y CUSTODIA DE LAS CREDENCIALES

El CLIENTE se obliga a que los Usuarios utilicen diligentemente las Credenciales de acceso, manteniéndolas en secreto.

FLEXXIBLE no se responsabiliza de la creación, modificación o uso que el CLIENTE, Usuarios o terceros hagan de dichas Credenciales.

FLEXXIBLE no será responsable de los daños y perjuicios causados por un tercero ante un incidente o brecha de seguridad en relación con la información o los datos almacenados en las Solución por falta de diligencia o fallos en la seguridad del CLIENTE o los Usuarios. A título enunciativo y no limitativo, se entiende falta de diligencia la utilización de una contraseña insegura y sistemas desactualizados, entre otros.

En caso de utilización fraudulenta de las Credenciales de acceso, el CLIENTE será responsable de los gastos de cualquier tipo derivados del uso fraudulento de las Soluciones por parte de terceros que utilicen sus Credenciales como consecuencia de un uso no diligente de las mismas por los Usuarios.

El CLIENTE se compromete a informar, sin dilación indebida, a FLEXXIBLE (i) de la pérdida de control sobre las Credenciales de acceso a las Soluciones de cualquier usuario, así como (ii) de los usos indebidos por parte de terceros de dichas Credenciales.

9.4 RESERVA UNILATERAL DE FLEXXIBLE DE MODIFICAR

EL NOMBRE DE USUARIO

FLEXXIBLE estará facultado para modificar el nombre de identificación del Usuario de manera unilateral y en cualquier momento por motivos de la propia operativa de los Servicios o de las Soluciones. FLEXXIBLE deberá informar al CLIENTE de la modificación del nombre de identificación de un usuario para el acceso a las Soluciones.

9.5. SUPUESTOS DE SUSPENSIÓN O REVOCACIÓN DE LAS CREDENCIALES

FLEXXIBLE estará facultado para suspender o revocar las Credenciales de acceso de manera unilateral y en cualquier momento por motivos de la propia operativa de los Servicios o de las Soluciones, así como en caso de detectar usos fraudulentos de las Soluciones. En tales situaciones, se informará al CLIENTE de forma inmediata detallando los motivos que han ocasionado la suspensión o revocación de las credenciales de acceso.

10. SERVICIO DE ATENCIÓN AL CLIENTE Y DE GESTIÓN DE INCIDENCIAS

Dentro del precio por los Servicios, está incluido el servicio de atención al CLIENTE y el servicio de gestión de incidencias.

El servicio de atención al CLIENTE y servicio de gestión de incidencias consiste en un servicio de atención comercial y de asistencia a nivel técnico. Dichos servicios se prestarán en el horario y de conformidad con lo especificado en el Plan Contratado.

La resolución de incidencias no imputables a un funcionamiento defectuoso de las Soluciones o la prestación de soporte al Usuario fuera del uso de las Soluciones puede comportar un coste adicional, el cual será previamente informado al CLIENTE, debiendo mostrar este su aceptación. En cualquier caso, este servicio no comprende la asistencia técnica de incidencias en el equipo informático del CLIENTE.

11. NIVEL DE SERVICIO

Los compromisos relativos al nivel del servicio, incluidos los tiempos de respuesta, niveles de disponibilidad y demás aspectos relacionados, se encuentran definidos en el Anexo III, **SLA**.

Los niveles de servicio referenciados podrán ser alterados en las siguientes situaciones:

i. Operaciones de mantenimiento programadas o recurrentes en las Soluciones;
ii. Operaciones de mantenimiento de la red que impidan el acceso del equipo del CLIENTE a Internet;
iii. Malfuncionamientos de soluciones o servicios de terceros necesarios para el correcto funcionamiento de las Soluciones;
iv. Malfuncionamientos provocados por el propio hardware o software del CLIENTE;
v. El uso de versiones obsoletas de las Soluciones por parte del CLIENTE;
vi. Ataques de denegación de servicio, ataques de piratería, errores en la programación de las Soluciones u otros motivos para los que no existe una solución conocida comercialmente razonable;
vii. Motivos de fuerza mayor o caso fortuito que no estén bajo el control directo de FLEXXIBLE y que no hayan podido ser evitados pese a las medidas adoptador por el mismo;
viii. El incumplimiento por parte del CLIENTE del presente Contrato.

12. RESPONSABILIDAD

12.1. RESPONSABILIDAD DEL CLIENTE

El CLIENTE asume la total responsabilidad sobre la selección del servicio y su uso para alcanzar los resultados esperados, eximiendo a FLEXXIBLE de cualquier garantía de resultados específicos. Asimismo, el CLIENTE es responsable de la correcta instalación de las Soluciones por parte de los Usuarios, así como de los permisos otorgados a los Usuarios para su utilización, incluyendo cualquier uso incorrecto de las Soluciones que pueda derivar en daños o perjuicios.

El CLIENTE reconoce que las Soluciones pueden no estar disponibles en situaciones que excedan el control de FLEXXIBLE, tales como fallos técnicos, interrupciones en la red, o eventos de fuerza mayor, sin generar indemnización de daños y perjuicios a su favor.

En caso de incumplimiento de las obligaciones recogidas en el presente Contrato, el CLIENTE será responsable de los daños y perjuicios que dicho incumplimiento pueda causar a FLEXXIBLE u otros terceros.

El CLIENTE se compromete a mantener indemne a FLEXXIBLE, sus directivos, empleados y subcontratistas frente a cualquier reclamación, demanda, daño, pérdida, responsabilidad, coste o gasto (incluyendo honorarios de abogados y procuradores) que surja o esté relacionado con: (i) el incumplimiento por parte del CLIENTE de cualquiera de las cláusulas de este Contrato; (ii) el uso de las Soluciones por parte del CLIENTE de forma contraria a la ley o a los términos de este Contrato; (iii) cualquier contenido, datos o información que el CLIENTE cargue, transmita o ponga a disposición a través de las Soluciones; o (iv) la infracción de derechos de terceros por parte del CLIENTE en relación con

el uso de las Soluciones.

FLEXXIBLE se reserva el derecho de emprender las acciones legales pertinentes en caso de incumplimiento de las obligaciones por parte del CLIENTE.

12.2. LIMITACIÓN DE RESPONSABILIDAD

Las Soluciones se proporcionan "tal cual" ("*as is*") y "según disponibilidad" ("*as available*"). FLEXXIBLE no otorga ninguna garantía, ya sea expresa, implícita o legal, más allá de las obligaciones de nivel de servicio establecidas en el SLA. Específicamente, FLEXXIBLE no garantiza que las Soluciones: (a) satisfagan la totalidad de los requisitos o expectativas particulares del CLIENTE; (b) estén libres de errores, defectos o interrupciones; o (c) sean compatibles con cualquier otro *software*, *hardware* o sistema del CLIENTE. El CLIENTE reconoce y acepta que asume el riesgo derivado del uso de las Soluciones.

FLEXXIBLE únicamente se hará cargo de los daños y perjuicios ocasionados que le pudieran ser imputables con relación al incumplimiento de sus obligaciones de acuerdo con la Cláusula 8 y de lo establecido en la presente Cláusula.

FLEXXIBLE responderá exclusivamente de los daños causados por culpa o negligencia probados derivados de su actuación, no excediendo, en ningún caso, la indemnización que corresponda del importe correspondiente al Precio abonado por el CLIENTE por la contratación de los Servicios en el momento en que se produjo la causa que motivó la indemnización.

FLEXXIBLE no será responsable, en ningún caso, de daños sufridos por pérdida de beneficios, ingresos o datos.

FLEXXIBLE no será responsable frente al CLIENTE, entre otros supuestos, de los siguientes a título enunciativo (i) en caso de que los Usuarios no utilicen las Soluciones con la diligencia debida y/o de acuerdo a la documentación proporcionada por FLEXXIBLE; (ii) en caso de que el fallo sea provocado por manipulaciones de las Soluciones no autorizadas previamente por FLEXXIBLE o por software de terceros; (iii) en supuestos de fraude; (iv) en eventos de fuerza mayor o caso fortuito que no estén bajo el control directo de FLEXXIBLE y que no hayan podido ser evitados pese a las medidas adoptador por el mismo; (v) situaciones que generen daños como consecuencia de la entrega de datos no veraces por parte del Usuario, supuestos de suplantación de identidad, cuestiones de seguridad o de garantía de privacidad ajenas a FLEXXIBLE (vi) uso con falta de diligencia o custodia indebida de las Credenciales.

FLEXXIBLE no asumirá responsabilidad alguna por el contenido almacenado en las Soluciones. El CLIENTE será el único responsable del contenido almacenado en las Soluciones, de su exactitud e integridad. El CLIENTE acepta de manera expresa exonerar a FLEXXIBLE de toda responsabilidad por dichos contenidos.

13. CONCESIÓN DE LICENCIA

13.1 LICENCIA

FLEXXIBLE, en su condición de licenciante, otorga al CLIENTE una licencia limitada de las Soluciones contratadas, no exclusiva, no transferible y sin derecho a sublicenciar (en adelante, la "Licencia") para acceder y utilizar las Soluciones contratadas para usos internos del CLIENTE y con fines no comerciales dentro de su territorio de actuación, con una duración vinculada al Plan Contratado y al pago del precio.

El acceso y uso de las Soluciones quedará sujeto al cumplimiento de las condiciones establecidas en el presente Contrato y demás pactos entre las Partes.

La presente Licencia confiere al CLIENTE derecho a posibles actualizaciones y mejoras de las Soluciones contratadas. Esta Licencia también permitirá al CLIENTE vincular las Soluciones con cuentas de terceros y a hacer uso de programas de terceros incluidos en las Soluciones. En estos casos pueden resultar de aplicación términos y condiciones distintos a los previstos en este documento.

El CLIENTE no podrá ni directa ni indirectamente: (i) sublicenciar la Licencia, (ii) transmitir la Licencia a un tercero sin la autorización de FLEXXIBLE, (iii) hacer otros usos de las Soluciones distintos a los autorizados en esta Licencia.

El CLIENTE no podrá ni directa ni indirectamente (entendiéndose como tal, entre otros, los Usuarios, empleados del CLIENTE y/o sus representantes), ni de forma total ni parcial:

a) Hacer uso de las Soluciones o cualesquiera de sus elementos integrales, para crear un servicio, software o documentación que realice sustancialmente las mismas funciones que las Soluciones.

b) Desmontar, descompilar, aplicar ingeniería inversa sobre el servicio o software, algoritmos o secretos comerciales en relación con las Soluciones, salvo en la medida permitida por la ley aplicable.

c) Gravar, sublicenciar, transferir, distribuir, alquilar, arrendar, compartir o utilizar las Soluciones en relación con otros contratos de servicios o en beneficio de cualquier tercero.

d) Copiar, reproducir, traducir, adaptar, combinar, crear trabajos derivados o de cualquier otra forma modificar cualquier propiedad de las Soluciones.

e) Compartir las credenciales de acceso con terceros distintos a los Usuarios.

f) Interferir o intentar interferir en el adecuado funcionamiento de las Soluciones de FLEXXIBLE.

g) Eludir las medidas de privacidad establecidas por FLEXXIBLE para prevenir o restringir el acceso a las Soluciones.

h) Vulnerar la confidencialidad de la documentación e información remitida por FLEXXIBLE al CLIENTE en relación con las Soluciones.

i) Cualquier otra actuación contraria a la normativa vigente, la moral o los buenos usos y costumbres.

13.2 DERECHOS DE PROPIEDAD INTELECTUAL

El CLIENTE declara conocer y acepta que las Soluciones, su documentación asociada y cualquier otro software de FLEXXIBLE es propiedad exclusiva de FLEXXIBLE, quien conservará todos los derechos de propiedad intelectual, industrial o cualesquiera otros sobre la misma y que no podrá ser objeto de ulterior reproducción, modificación, transformación, copia, alteración, adaptación o traducción por parte del CLIENTE.

La estructura, características, códigos, métodos de trabajo, sistemas de información, herramientas de desarrollo, know-how, metodologías, procesos, tecnologías o algoritmos de las Soluciones son propiedad exclusiva de FLEXXIBLE, o de sus proveedores, habiendo sido, en este último caso, objeto de licencia o cesión por parte de los mismos, y están protegidos por la normativa nacional e internacional en materia de propiedad intelectual e industrial, y no pueden ser objeto de ulterior modificación, copia, alteración, reproducción, adaptación o traducción por parte del CLIENTE. En consecuencia, queda terminantemente prohibido cualquier uso por el CLIENTE de las Soluciones que se realice sin la autorización de FLEXXIBLE, incluida su explotación, reproducción, difusión, transformación, distribución, transmisión por cualquier medio, posterior publicación, exhibición, comunicación pública o representación total o parcial, las cuales, de producirse, constituirán infracciones de los derechos de propiedad intelectual o industrial de FLEXXIBLE, sancionadas por la legislación vigente.

Cualquier mejora, desarrollo o nueva funcionalidad creada por FLEXXIBLE en ejecución de este Contrato será propiedad de FLEXXIBLE en exclusiva.

Las obligaciones de las Cláusulas 13.1 y 13.2 permanecerán vigentes indefinidamente, especialmente las restricciones de uso y confidencialidad de propiedad de FLEXXIBLE.

14. SUSPENSIÓN DEL CONTRATO

Podrá ser causa de suspensión la demora en el pago por parte del ÇLIENTE, tanto a FLEXXIBLE como al PARTNER a través del cual el CLIIENTE haya contratado las Soluciones.

Además, FLEXXIBLE se reserva la facultad de suspender el acceso a las Soluciones y/o los Servicios, respectivamente, a los Usuarios en caso de detectar cualquier tipo de incumplimiento del Contrato por parte del CLIENTE, del personal a su cargo, de sus colaboradores autorizados o Usuarios que accedan a las Soluciones contratadas.

Ante estas situaciones, el CLIENTE dispondrá del plazo de quince (15) días para subsanar el incumplimiento. Transcurrido dicho plazo sin que se haya subsanado la causa de la suspensión, FLEXXIBLE podrá resolver de forma definitiva el contrato comunicándose al CLIENTE su finalización sin indemnización alguna a favor del CLIENTE por ningún concepto.

15. RESOLUCIÓN

Serán causas de resolución del Contrato los siguientes supuestos:

a. Al finalizar el plazo previsto en el Plan Contratado, si no ha mediado la prórroga automática prevista la Cláusula 3. La resolución del Contrato por la presente causa no generará indemnizaciones ni penalizaciones, salvo obligaciones de pago ya devengadas.

b. Por falta de pago del CLIENTE, tanto a FLEXXIBLE como a cualquier tercero a través del cual se hayan contratado las Soluciones.

c. Por falta de pago del Parner a FLEXXIBLE.

d. Por incumplimiento de las obligaciones contraídas por una de las Partes si dicho incumplimiento ha sido notificado a la otra Parte y la Parte incumplidora no ha procedido a su subsanación en el plazo de quince (15) días, de conformidad con la Cláusula 14.

e. Por ocurrir cualquiera de las siguientes causas: (a) concurso de acreedores, disolución o intervención judicial de la otra Parte; (b) cambio regulatorio que haga imposible la prestación de los Servicios; (c) terminación de licencias esenciales de FLEXXIBLE.

Efectos de la resolución:

FLEXXIBLE suspenderá todo acceso a las Soluciones en las 24 horas siguientes a la notificación efectiva de resolución.

Durante treinta (30) días posteriores a la terminación, el CLIENTE podrá descargar sus datos en formato estructurado sin coste adicional. Transcurrido dicho plazo, FLEXXIBLE eliminará permanentemente los Datos.

El CLIENTE abonará todas las cantidades devengadas hasta la

fecha efectiva de terminación, incluyendo suscripciones prorrateadas y gastos pendientes. FLEXXIBLE emitirá la correspondiente factura final.

FLEXXIBLE mantendrá acceso de lectura al CLIENTE durante los treinta (30) días de exportación de datos, exclusivamente para dicha finalidad.

16. TRATAMIENTO DE DATOS PERSONALES

El CLIENTE es conocedor de que FLEXXIBLE podrá acceder, conservar y procesar la información de su cuenta y el contenido: (i) con el fin de administrar adecuadamente su cuenta de Usuario; y (ii) si así lo requiere la ley o autoridad competente.

El CLIENTE será el único responsable de los contenidos e información almacenados en las Soluciones por sus USUARIOS. Asimismo, FLEXXIBLE no asumirá responsabilidad alguna por cualquier afirmación o declaración que el CLIENTE efectúe sobre su contenido en cualquier área de las Soluciones. El CLIENTE será el único responsable del contenido almacenado en las Soluciones, de su exactitud e integridad; por lo que acepta de manera expresa exonerar a FLEXXIBLE de toda responsabilidad, así como evitar tomar medidas legales en contra de FLEXXIBLE en relación con dichos contenidos.

La ejecución del Contrato requerirá el acceso y tratamiento de datos de interesados del CLIENTE por parte de FLEXXIBLE, en nombre y por cuenta del CLIENTE, en los términos del RGPD y de la LOPDGDD. A estos efectos, las Partes suscriben el Anexo I. **Tratamiento de Datos, que forma parte de**l presente Contrato. En consecuencia, FLEXXIBLE tendrá la consideración de Encargado del Tratamiento de los datos que se incorporen en la/s Solución/es por cuenta del CLIENTE con la única finalidad del procesamiento, estructuración y almacenamiento de los datos, así como por los Servicios prestados por el CLIENTE.

El acceso y uso de los Servicios tiene lugar bajo la única y exclusiva responsabilidad del CLIENTE, quien deberá utilizarlo y hacerlo utilizar de forma diligente, correcta y lícita, de conformidad con la legislación vigente y quedando expresamente prohibido el uso de los Servicios para prestar servicio, retribuido o no, a terceras entidades.

En relación con el tratamiento de los datos del CLIENTE (o, en su caso, sus representantes y personas de contacto), serán únicamente tratados por FLEXXIBLE con el fin de posibilitar la ejecución del presente Contrato. La legitimación del tratamiento de los datos se basa en la ejecución del contrato, el cumplimiento de las obligaciones legales aplicables, y el interés legítimo en el mantenimiento de la relación de conformidad con el artículo 19 de la LOPDGDD. Los datos serán conservados mientras se mantenga vigente el Contrato, el tiempo necesario para cumplir con las obligaciones legales y en el periodo de prescripción de las acciones legales que se puedan derivar de la relación.

Los datos podrán ser cedidos a las administraciones públicas competentes, para el cumplimiento de obligaciones legales; así como a entidades financieras para la gestión de cobros y pagos, y proveedores que tengan la consideración de encargados del tratamiento.

Los sujetos afectados podrán ejercer sus derechos de acceso, rectificación, oposición, limitación, supresión, portabilidad y a no ser objeto de decisiones automatizadas dirigiéndose a la dirección del Delegado de Protección de Datos a **gdpr@flexxible.com**. Asimismo, los sujetos afectados pueden reclamar ante la Agencia Española de Protección de Datos (www.aepd.es), especialmente cuando no hayan obtenido satisfacción en el ejercicio de sus derechos.

17. MISCELÁNIA

17.1. LEY APLICABLE

Cualquier controversia surgida de la interpretación o ejecución del presente Contrato o de cualquiera de sus eventuales modificaciones, así como cualquier incumplimiento, se interpretará de conformidad con la legislación española, que será la ley aplicable

17.2. RESOLUCIÓN DE CONTROVERSIAS

Para solucionar cualquier controversia relacionada con lo dispuesto en el presente Contrato o en ejecución del mismo, las Partes se someten expresamente a los Juzgados y Tribunales de la ciudad de Barcelona, con renuncia a cualquier otro fuero que pudiere corresponderles.

17.3. ACUERDO ÍNTEGRO

En los supuestos de contratación directa entre FLEXXIBLE y el CLIENTE, el presente Contrato constituye un acuerdo íntegro entre las Partes en relación con la materia objeto del mismo, y sustituyen y anulan todas las negociaciones, compromisos, pactos y comunicaciones, ya sean verbales o escritos, que al respecto hubieran alcanzado con anterioridad a la firma de este documento; excluyéndose, asimismo, de mutuo acuerdo, la aplicación de cualesquiera otros términos y condiciones.

Forma parte del Contrato el Plan Contratado, los Términos y Condiciones y sus Anexos, esto es, el I. Contrato de Tratamiento de Datos, el II. Política de Ciberseguridad y el III. SLA.

En supuestos de contratación del CLIENTE a través de un PARTNER, los presentes Términos y Condiciones serán aplicables en aquellos aspectos no acordados entre el PARTNER y el CLIENTE. En caso de duda, el acuerdo o

contrato suscrito entre el CLIENTE y el PARTNER se interpretará de conformidad con lo establecido en los presentes Términos y Condiciones.

17.4. NO RENUNCIA

La falta de ejercicio o el retraso en el ejercicio por parte de FLEXXIBLE de cualquier derecho, facultad o recurso previsto en este contrato o en la ley no se interpretará como una renuncia a dicho derecho, facultad o recurso, ni impedirá su posterior ejercicio. El ejercicio parcial de cualquier derecho, facultad o recurso no impedirá el ejercicio posterior de dicho derecho, facultad o recurso, ni el ejercicio de cualquier otro derecho, facultad o recurso.

17.5. MODIFICACION DE LOS TÉRMINOS Y CONDICIONES

FLEXXIBLE podrá modificar los presentes Términos y Condiciones en cualquier momento. Dichas modificaciones serán notificadas al CLIENTE por correo electrónico con una antelación mínima de quince (15) días a su entrada en vigor. La continuación en el uso de las Soluciones tras la entrada en vigor de las modificaciones se considerará una aceptación de los nuevos términos. Si el CLIENTE no estuviera de acuerdo, podrá resolver el Contrato antes de que la modificación sea efectiva.

17.6. FUERZA MAYOR

Las Partes no serán responsables del incumplimiento de las obligaciones establecidas en el presente Contrato en la medida en que tal incumplimiento sea debido a causas razonablemente fuera de control de la Parte incumplidora, tales como, sin carácter limitativo, incendios, inundaciones, epidemias y pandemias, huelgas, conflictos laborales u otros desórdenes sociales, escasez o indisponibilidad de combustible o energía eléctrica, indisponibilidad o funcionamiento anómalo de las redes de comunicaciones, accidentes, guerras (declaradas o no declaradas), embargos comerciales, bloqueos, disturbios o insurrecciones.

La parte afectada por un evento de fuerza mayor deberá notificar a la otra parte sin demora y hará esfuerzos razonables para mitigar sus efectos. Si el evento de fuerza mayor persiste por un periodo superior a 45 días, cualquiera de las partes podrá resolver el contrato sin penalización.

17.7. NOTIFICACIONES

Todas las notificaciones en el marco del presente Contrato deberán formularse por escrito y remitirse a las direcciones de las Partes mediante notificación fehaciente por carta o correo electrónico certificado. Toda notificación será eficaz en la fecha de su recepción, incluso en el supuesto de no apertura de un correo electrónico.

Previa notificación a la otra Parte, cualquiera de las Partes podrá modificar la dirección y los destinatarios designados por ella. La modificación surtirá efectos desde que haya sido debidamente notificada a la otra Parte

17.8. SUBCONTRATACIÓN

FLEXXIBLE podrá subcontratar total o parcialmente el cumplimiento de sus obligaciones derivadas del presente Contrato conforme a lo previsto en el Contrato de Tratamiento de Datos sin necesidad de obtener el previo consentimiento por escrito del CLIENTE. FLEXXIBLE continuará, no obstante, siendo plenamente responsable del cumplimiento de estas, en particular por cualesquiera acciones y/u omisiones de sus subcontratistas al respecto, tal y como si se tratara de sus propias acciones y/u omisiones.

17.9. CESIÓN

FLEXXIBLE podrá ceder libremente el presente Contrato, así como sus derechos y obligaciones, a cualquier tercero, incluyendo, entre otros posibles, a sus filiales, sociedades del mismo grupo empresarial o en el marco de una fusión, escisión o cualquier otra modificación estructural, así como la adquisición o venta de activos, sin necesidad de consentimiento del CLIENTE, si bien lo notificará al CLIENTE con la mayor antelación posible.

17.10. CONFIDENCIALIDAD

A efectos de este Contrato, "Información Confidencial" significa toda información, ya sea técnica, comercial, financiera o de cualquier otra índole, revelada por una Parte (la "Parte Reveladora") a la otra (la "Parte Receptora"), de forma oral, escrita o por cualquier otro medio, que esté identificada como confidencial o que, por su naturaleza, deba ser razonablemente considerada como tal. Incluye, sin limitación, el contenido del CLIENTE, datos personales, así como el software, código fuente, algoritmos, metodologías, planes de negocio, información de precios y know-how.

La Parte Receptora se compromete a:

a) Utilizar la Información Confidencial de la Parte Reveladora única y exclusivamente para el cumplimiento de las obligaciones derivadas del presente Contrato.

b) Mantener la Información Confidencial en estricto secreto y protegerla con el mismo grado de diligencia que utiliza para su propia información de naturaleza similar, y en ningún caso con una diligencia inferior a la razonable.

c) No divulgar la Información Confidencial a ningún tercero sin el consentimiento previo y por escrito de la Parte Reveladora, salvo a sus empleados, asesores o subcontratistas que necesiten conocerla para la ejecución del Contrato y que estén sujetos a obligaciones de confidencialidad al menos tan estrictas como las aquí

establecidas.

Las obligaciones de confidencialidad no se aplicarán a aquella información que:

a) Sea o pase a ser de dominio público sin que medie incumplimiento de la Parte Receptora.

b) Ya estuviera en posesión legítima de la Parte Receptora antes de su revelación.

c) Sea revelada por imperativo legal o por requerimiento de una autoridad judicial o administrativa competente. En tal caso, la Parte Receptora notificará a la Parte Reveladora dicho requerimiento, siempre que sea legalmente posible, para que esta pueda adoptar las medidas de protección que estime oportunas.

La obligación de confidencialidad se mantendrá durante toda la vigencia del Contrato y subsistirá con carácter indefinido tras su finalización.

El contenido proporcionado por el CLIENTE en las Soluciones contratadas será estrictamente confidencial, de tal forma que únicamente se emplearán para prestar los Servicios y no se revelarán a terceros diferentes de empleados o subcontratistas de FLEXXIBLE o terceros destinatarios para la correcta prestación de los Servicios los cuales también están sujetos a un deber de confidencialidad. El contenido únicamente podrá revelarse por requerimiento legal o judicial que lo prevea.

17.11. SUBSISTENCIA

Si cualquier cláusula del presente Contrato fuese declarada, total o parcialmente, nula o ineficaz, tal nulidad o ineficacia afectará tan solo a dicha disposición o a la parte de la misma que resulte nula o ineficaz, subsistiendo el Contrato en todo lo demás, teniéndose tal disposición, o la parte de la misma que resultase afectada, por no puesta.

17.12. TERCEROS

El presente Contrato no confiere derecho alguno en beneficio de terceras partes, salvo que expresamente se disponga lo contrario.

17.13. CONTRATACIÓN ELECTRÓNICA

Las Partes consienten que el presente Contrato y cualquier modificación del mismo se suscriba por las Partes mediante un sistema de contratación electrónica dándole ambas Partes plenos efectos a la firma mediante el citado medio.

ANEXO I
CONTRATO DE TRATAMIENTO DE DATOS

En cumplimiento del Reglamento (UE) 2016/679 general de protección de datos (en adelante, "*RGPD*") y de la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales (en adelante, "*LOPDGDD*") las Partes suscriben el presente contrato de encargo del tratamiento. El presente contrato de encargo regula las condiciones a través de las cuales FLEXXIBLE accede a los datos personales facilitados por el CLIENTE.

El CLIENTE (en adelante, el "*Responsable del tratamiento*" o el "*Responsable*") y FLEXXIBLE (en adelante, el "*Encargado del tratamiento*" o el "*Encargado*") conjuntamente referidos como las "*Partes*" e individualmente como la "*Parte*", manifiestan su voluntad de formalizar el presente contrato en materia de protección de datos personales (en adelante, el "***Contrato de encargo***"), como parte del contrato de prestación de servicios (en adelante, indistintamente, el "***Contrato Principal***").

y a tal efecto acuerdan las siguientes

CLÁUSULAS

1. OBJETO.

El objeto del presente Contrato de encargo es habilitar al Encargado del Tratamiento para tratar por cuenta del Responsable del tratamiento los datos personales necesarios para la prestación de los servicios que implican tratamiento de datos personales (en adelante "**Servicios**") y definir las condiciones conforme a las cuales el Encargado del tratamiento tratará los datos personales a los que tiene acceso durante la ejecución del Contrato Principal, estableciendo las obligaciones y responsabilidades derivadas de los tratamientos de datos que realice el Encargado del tratamiento exclusivamente para y con ocasión del cumplimiento de dichos Servicios.

2. DESCRIPCIÓN DEL TRATAMIENTO DE DATOS.

El tratamiento se encuentra descrito en el Anexo I que detalla la siguiente información referida al tratamiento:

- Categorías de interesados cuyos datos personales se tratan
- Categorías de datos personales tratados
- Datos de categorías especiales tratados (si procede) y restricciones o garantías aplicadas
- Naturaleza del tratamiento
- Finalidad(es) del tratamiento de los datos personales por cuenta del responsable del tratamiento
- Duración del tratamiento

3. LIMITACIÓN DE LA FINALIDAD DEL TRATAMIENTO DE LOS DATOS PERSONALES.

Las finalidades con las que se realizarán los antecitados tratamientos de datos son las que se derivan de los Servicios que el Encargado del Tratamiento prestará al Responsable del Tratamiento tal y como se indican en el Anexo I. El Encargado del tratamiento se compromete a tratar los datos personales que trate como consecuencia de este Contrato de Encargo, según el procedimiento que se ajuste a las instrucciones documentadas que en cada momento indique el Responsable del tratamiento y la legislación aplicable, limitándose a realizar las actuaciones necesarias para desarrollar prestar los Servicios, y a no aplicarlos o utilizarlos con un fin distinto al estipulado en el presente Contrato de encargo. En ningún caso el Encargado del tratamiento podrá utilizar los datos para fines propios o diferentes a los previstos.

4. INSTRUCCIONES DEL TRATAMIENTO DE LOS DATOS PERSONALES.

4.1. Las instrucciones para este tratamiento son las detalladas en el Contrato principal en relación con la prestación de los Servicios.

4.2. El Encargado del tratamiento no comunicará los datos personales a terceros, ni siquiera para su conservación, salvo que tenga la autorización previa y expresa del Responsable del tratamiento, en los supuestos legalmente previstos.

4.3. El Encargado del tratamiento seguirá las instrucciones del Responsable del tratamiento inclusive con respecto a las transferencias internacionales de datos personales a un tercer país u organización internacional, salvo que el Encargado del tratamiento esté obligado a ello en virtud del Derecho de la Unión Europea o de los Estados miembros que se aplique al Encargado del tratamiento, en cuyo caso el Encargado del tratamiento informará al Responsable del tratamiento de tal exigencia legal previa al tratamiento, salvo que dicho Derecho lo prohíba por razones importantes de interés público.

4.4. El Encargado del tratamiento informará inmediatamente al Responsable del tratamiento si en su consideración una instrucción infringe el RGPD o cualquier otra disposición en materia de

protección de datos de la Unión Europea o de los Estados miembros que se aplique al Encargado del tratamiento.

5. CONFIDENCIALIDAD.

5.1. La información facilitada por parte del Responsable del tratamiento al Encargado o que el Encargado pueda conocer en el marco de este Contrato de encargo es estrictamente confidencial. El Encargado del tratamiento es responsable de no divulgar a terceros información obtenida como consecuencia de esta relación contractual.

5.2. El Encargado del tratamiento debe mantener el deber de secreto profesional respecto de los datos personales a los que tenga acceso en virtud del Contrato de encargo y el deber de guardarlos, obligaciones que subsistirán aún después de finalizar sus relaciones con el Responsable del tratamiento.

5.3. En este sentido, el Encargado del tratamiento, guardará y mantendrá todos los datos personales en estricta confidencialidad, utilizando el grado de cuidado que sea apropiado para evitar el acceso, uso o divulgación no autorizados.

6. DURACIÓN.

El presente Contrato de encargo iniciará su vigencia en la fecha de firma o aceptación del mismo, desplegando efectos desde que se inicie el tratamiento de los datos personales y estando vigente hasta la resolución de la relación entre las partes. No obstante, la obligación de confidencialidad sobre los datos personales tendrá una duración indefinida.

7. OBLIGACIONES DEL RESPONSABLE DEL TRATAMIENTO.

7.1. El Responsable del tratamiento se compromete a:

7.1.1. Velar por el cumplimiento por parte del Encargado del tratamiento de las obligaciones previstas en este Contrato de encargo y supervisar el tratamiento de los datos personales por parte de éste.

7.1.2. Cumplir con las obligaciones que le correspondan como Responsable del tratamiento en aplicación de la normativa vigente.

7.1.3. Facilitar al Encargado los datos e indicaciones necesarios en tiempo y forma que permitan al Encargado prestar los Servicios de la manera más eficiente.

7.1.4. Garantizar que los datos facilitados al Encargado del Tratamiento se han obtenido lícitamente y que son adecuados, pertinentes y limitados a los fines del tratamiento.

8. OBLIGACIONES DEL ENCARGADO DEL TRATAMIENTO.

El Encargado del tratamiento se obliga a:

8.1. Llevar, por escrito, un registro de las actividades de tratamiento efectuadas por cuenta del Responsable del tratamiento, que cumpla con los requerimientos fijados en el artículo 30.2 del RGPD.

8.2. Ofrecer garantías de cumplimiento de las personas autorizadas a tratar datos personales, para ello:

8.2.1. El Encargado del Tratamiento implementará las medidas necesarias para que únicamente accedan a los datos personales las personas autorizadas que tengan necesidad de tratarlos para llevar a cabo sus funciones en relación con la prestación de los Servicios y bajo las instrucciones del Responsable del tratamiento.

8.2.2. El Encargado del Tratamiento dará a conocer y exigirá, a las personas autorizadas para tratar datos personales, el cumplimiento de las obligaciones contenidas en este Contrato de encargo y advertirles del carácter confidencial de la información y de su responsabilidad en caso de divulgarla.

8.2.3. El Encargado del Tratamiento garantiza que todas las personas que traten los datos personales se han comprometido de forma expresa y por escrito a guardar la confidencialidad y a cumplir las medidas de seguridad correspondientes. Los documentos acreditativos de esta obligación estarán a disposición del Responsable del tratamiento.

8.2.4. El Encargado del Tratamiento garantiza que llevará a cabo formación necesaria en materia de protección de datos personales a las personas autorizadas para tratar datos personales.

8.2.5. En el caso de que las personas autorizadas presten los Servicios en los locales del Responsable del tratamiento o bien de forma remota accediendo a los sistemas del Responsable, dichas personas se someterán a las normas, procedimientos y demás disposiciones contenidas en las políticas de seguridad, guías, protocolos o manuales que facilite el Responsable del tratamiento.

8.3. Actuar al recibir derechos de los interesados

8.3.1. Cuando las personas afectadas ejerzan los derechos de acceso, rectificación, supresión y oposición, limitación del tratamiento, portabilidad de datos y a no ser objeto de decisiones automatizadas ante el Encargado del tratamiento, éste debe comunicarlo al Responsable del tratamiento enviando un email a la dirección de correo electrónico que se informe como dirección de contacto.

8.3.2. La comunicación debe hacerse de forma inmediata y en ningún caso más allá de los cinco (5) días laborables siguientes a la recepción de la solicitud. La comunicación contendrá la solicitud recibida junto con toda la información y documentación relativa al reclamante y al tratamiento de datos a que se refiere su reclamación, así como todas aquellas que puedan ser relevantes para resolver la solicitud.

8.3.3. El Encargado del tratamiento asistirá al Responsable del tratamiento, teniendo en cuenta la naturaleza del tratamiento, a través de medidas técnicas y organizativas apropiadas, y con cualquier información que pueda ser relevante para atender correctamente la petición recibida de conformidad con el artículo 12 del RGPD.

8.4. Notificar al Responsable las violaciones de seguridad de los datos personales

8.4.1. En caso de producirse una violación de seguridad, el Encargado del tratamiento notificará al Responsable del tratamiento, antes del plazo máximo de setenta y dos (72) horas desde la detección, y a través del correo electrónico de contacto, adjuntando con toda la información relevante para la documentación y comunicación de la incidencia.

8.4.2. La comunicación deberá incluir como mínimo, la información siguiente:

(a) Descripción de la naturaleza de la violación de la seguridad de los datos personales, inclusive, las categorías y el número aproximado de interesados afectados, y las categorías y el número aproximado de registros de datos personales afectados.
(b) Datos del delegado de protección de datos del Encargado del tratamiento o la persona de contacto para obtener más información.
(c) Descripción de las posibles consecuencias de la violación de la seguridad de los datos personales.
(d) Descripción de las medidas adoptadas o propuestas para poner remedio a la violación de la seguridad de los datos personales, incluyendo, si procede, las medidas adoptadas para mitigar los posibles efectos negativos.

8.4.3. Si no es posible facilitar la información simultáneamente, y en la medida en que no lo sea, el Encargado del Tratamiento facilitará al Responsable del Tratamiento la información pendiente sin dilación indebida.

8.4.4. El Encargado asistirá al Responsable del tratamiento, para que este pueda cumplir con sus obligaciones de notificar la brecha de seguridad ante la Autoridad de protección de datos y en su caso a los interesados.

8.5. Implementar medidas de seguridad

8.5.1. El encargado del tratamiento aplicará, como mínimo, las medidas técnicas y organizativas especificadas en el Anexo III para garantizar la seguridad de los datos personales y cualquier cambio sobre las mismas deberá notificarlo al Responsable del tratamiento. Las medidas de seguridad implementadas deberán garantizar un nivel de seguridad adecuado, incluida la confidencialidad, teniendo en cuenta el estado de la técnica, los costes de aplicación, la naturaleza, el alcance, el contexto y los fines del tratamiento, así como los riesgos que plantea el tratamiento

para los interesados.

8.5.2. En cualquier caso, el Encargado del tratamiento, implantará las medidas detalladas en el Anexo III que serán mecanismos apropiados para:

(a) Garantizar la confidencialidad, integridad, disponibilidad y resiliencia permanentes de los sistemas y servicios de tratamiento.
(b) Restaurar la disponibilidad y el acceso a los datos personales de forma rápida, en caso de incidente físico o técnico.
(c) Verificar, evaluar y valorar, de forma regular, la eficacia de las medidas técnicas y organizativas implantadas para garantizar la seguridad del tratamiento.
(d) Seudonimizar y cifrar los datos personales, en su caso.

8.6. Auditorías y garantías de cumplimiento

8.6.1 El Encargado del tratamiento se obliga a poner a disposición del Responsable del tratamiento, a su simple requerimiento, toda la información relativa a las medidas de seguridad efectivamente implementadas, así como indicar estándar, certificación, medidas de seguridad y organizativas que garantizan un nivel de seguridad adaptado al riesgo o certificado de la última auditoría en materia de protección de datos, realizada. Asimismo, el Encargado del tratamiento, permitirá la llevanza de auditorías de control, en lo referente a las medidas de seguridad, por parte del Responsable del tratamiento o de un tercero autorizado por él. Estas auditorías de control se informarán con mínimo un mes de antelación y se ejecutarán de manera que no se vea afectada la actividad del Encargado y limitándose exclusivamente al tratamiento de datos personales objeto de este Contrato de encargo sin acceder a información que pueda pertenecer a otros responsables del tratamiento a los que el Encargado preste Servicios.

8.7. Asistir al Responsable del tratamiento:

8.7.1. El Encargado del Tratamiento dará soporte al Responsable del tratamiento en la realización de las evaluaciones de impacto relativas a la protección de datos y en la realización de las consultas previas a la autoridad de control, cuando proceda. El Encargado podrá solicitar compensación al Responsable cuando estime que el soporte prestado excede de lo razonable.

8.7.2. Cuando sea necesario o lo exija la normativa aplicable el Encargado del tratamiento nombrará un Delegado de Protección de Datos y comunicará al Responsable del tratamiento su identidad y datos de contacto; o, en su defecto, un punto de contacto.

8.8. Destruir o devolver los datos al finalizar el Contrato de encargo

8.8.1. Cumplido el Contrato principal, el Encargado del tratamiento se compromete, a elección del Responsable del tratamiento, a:
(a) Destruir los datos personales.
(b) Devolver al Responsable del tratamiento todos los datos personales.
(c) Enviar los datos personales a otro encargado del tratamiento que designe por escrito el Responsable del tratamiento.

8.8.2. La devolución de los datos comporta la destrucción de todas las copias, cualquier soporte o documento existentes en los sistemas de información del Encargado del tratamiento y adoptar las medidas de seguridad para evitar la sustracción, pérdida o acceso indebido a los datos durante su tránsito. En el caso de supresión, el Encargado del tratamiento garantiza las medidas necesarias para evitar el acceso a la información o recuperación posterior y siempre que lo solicite el Responsable deberá certificar su destrucción por escrito y entregar el certificado correspondiente al Responsable del tratamiento.

8.8.3. Sin perjuicio de lo anteriormente expuesto, el Encargado del tratamiento podrá mantener debidamente bloqueados los datos personales de referencia durante el período en el que se pudieran derivar responsabilidades de su relación con el Responsable del tratamiento, de acuerdo con la normativa de aplicación en vigor.

9. SUBCONTRATACIÓN Y SUBENCARGADOS DEL TRATAMIENTO.

9.1. El Encargado del tratamiento no podrá subcontratar total o parcialmente ninguno de los

Servicios u tratamientos cubiertos por este Contrato de encargo, excepto por aquellos servicios auxiliares que sean necesarios para el funcionamiento normal de los Sistemas del Encargado y los indicados en el Anexo II.

9.2. En caso de requerirse la subcontratación de proveedores, el Encargado del tratamiento deberá comunicarlo por escrito previamente al Responsable, en el plazo de un (1) mes antes de iniciar la prestación de los servicios, indicando los tratamientos que se pretenden subcontratar e identificando de forma clara e inequívoca la empresa subcontratista, junto con una descripción, y sus datos de contacto.

9.3. La subcontratación podrá realizarse si se cuenta con la autorización del Responsable o, en su defecto, si el Responsable no se opone a la contratación en el plazo de 10 días desde que se envió la notificación.

9.4. En todo caso, el tratamiento de los datos por parte del subencargado deberá ajustarse a las instrucciones del Responsable del tratamiento, debiendo ser el Encargado del tratamiento el responsable de regular la nueva relación con el subencargado en los términos previstos en este Contrato de encargo, expresamente y por escrito, cuando el subencargado asuma obligaciones idénticas a las establecidas para el Encargado del en virtud de este Contrato de encargo. En caso de incumplimiento por parte del subencargado, el Encargado seguirá siendo totalmente responsable ante el Responsable con respecto al cumplimiento de sus obligaciones.

9.5. La lista de subencargados autorizados por el Responsable en el momento de la contratación se establece en el Anexo II.

10. RÉGIMEN APLICABLE A LAS TRANSFERENCIAS INTERNACIONALES.

10.1. Con el fin de preservar y mantener el nivel de protección de los datos personales garantizado por el RGPD y la LOPDGDD, solo se podrán realizar transferencias de los Datos Personales a un tercer país u organización internacional si el Responsable del Tratamiento y el Encargado del Tratamiento cumplen con las condiciones y requisitos estipulados en el Capítulo V del RGPD, tal y como establece el artículo 44 del RGPD.

10.2. El Encargado se obliga a realizar transferencias internacionales únicamente cuando el destino cuente con una decisión de adecuación, la organización tenga en vigor normas corporativas vinculantes o se formalicen cláusulas contractuales tipo.

11. RESPONSABILIDAD

11.1. Ambas Partes se comprometen a respetar el cumplimiento de las obligaciones que se deriven del Contrato de encargo y de la legislación aplicable, haciendo frente cada una a la responsabilidad que derive de su propio incumplimiento.

11.2. El Encargado del tratamiento responderá de los daños y perjuicios causados por el tratamiento cuando no haya cumplido con las obligaciones del RGPD dirigidas específicamente a los encargados o haya actuado al margen o en contra de las instrucciones legales del Responsable.

11.3. Siempre que el Encargado infrinja le estipulado en este contrato y determine los fines y los medios del tratamiento, será considerado responsable del tratamiento con respecto a dicho tratamiento.

12. INFORMACIÓN DE CONTACTO.

12.1. A efectos de notificaciones relacionadas con este Contrato de encargo se puede contactar con el Encargado del tratamiento enviando un correo electrónico al Delegado de Protección de Datos a gdpr@flexxible.com.

13. INCUMPLIMIENTO Y RESOLUCIÓN.

13.1. El Responsable del Tratamiento tendrá derecho a resolver el Contrato de encargo en la medida en que se refiera al tratamiento de Datos Personales si:

13.1.2. El Encargado del Tratamiento incumple de forma sustancial o persistente sus obligaciones en virtud del RGPD y la LOPDGDD y lo indicado en el Contrato de encargo;

13.1.3. El Encargado del Tratamiento incumple una decisión vinculante de un tribunal competente o de la autoridad o autoridades de supervisión competentes en relación con sus obligaciones en virtud de este Contrato de encargo, el RGPD o la LOPDGDD.

13.2. El Encargado del tratamiento tendrá derecho a rescindir el Contrato principal con respecto al tratamiento de datos personales, sin perjuicio de

que el resto de servicios o prestaciones del Contrato se mantengan vigentes cuando, después de informar al Responsable del tratamiento que sus instrucciones infringen los requisitos legales establecidos en la cláusula 6.1, letra b), del RGPD, el Responsable del tratamiento insista en que se sigan dichas instrucciones. Esta resolución no podrá suponer ningún tipo de indemnización o pago por daños y perjuicios por parte del Encargado al Responsable.

13.3. Tras la finalización del Acuerdo, el Encargado del tratamiento, a petición del Responsable del tratamiento, se aplicará lo estipulado en el punto 8.8 de este Contrato de encargo. Hasta que los datos sean destruidos o devueltos, el Encargado del Tratamiento seguirá garantizando el cumplimiento del presente Contrato de encargo.

14. LEGISLACIÓN APLICABLE Y TRIBUNALES COMPETENTES.

14.1. En lo previsto en este Contrato de encargo, así como en la interpretación y resolución de los conflictos que pudieran surgir entre las Partes como consecuencia del mismo, será de aplicación la legislación española.

14.2. Para la resolución de cualquier controversia que pudiera derivarse del presente Contrato de encargo, ambas Partes se someterán a la jurisdicción que se indica en el Contrato Principal, con renuncia expresa a cualquier otro fuero que pudiera corresponderles.

DESCRIPCIÓN DEL TRATAMIENTO

<table>
<tr><td>1. Categorías de interesados cuyos datos personales se tratan:</td><td>☒ Empleados
☐ Clientes
☐ Proveedores</td><td>☒ Usuarios web
☐ Candidatos
☐ Otros:</td></tr>
<tr><td>2. Categorías de datos personales tratados:</td><td>☒ Identificativos
☐ Ocupación profesional
☐ Características personales
☐ Circunstancias sociales</td><td>☐ Académicas y profesionales
☐ Transacciones bienes y servicios
☐ Económicos y financieros
☐ Información comercial
☒ Otros: Datos relativos a los dispositivos de los USUARIOS.</td></tr>
<tr><td rowspan="5">3. Datos de categoría especial tratados (si procede) y restricciones o garantías aplicadas:</td><td colspan="2">3.1. ☐ Sí, se tratan datos sensibles:</td></tr>
<tr><td>☐ Opiniones políticas
☐ Datos biométricos
☐ Afiliación sindical
☐ Vida sexual
☐ Condenas/ infracciones penales
☐ Origen racial o étnico
☐ Salud</td><td>☐ Religión
☐ Estado fisiológico
☐ Creencias filosóficas
☐ Necesidades educativas especiales
☐ Discapacidades físicas o intelectuales
☐ Datos genéticos</td></tr>
<tr><td colspan="2">3.1.1. RESTRICCIONES Y GARANTÍAS APLICADAS:
☐ Limitación estricta de la finalidad.
☐ Restricciones de acceso.
☐ Registro de acceso a los datos.
Para más información, consultar Anexo III.</td></tr>
<tr><td colspan="2">3.2. ☒ No se tratan datos sensibles.</td></tr>
<tr><td colspan="2">3.3. ☐ Se tratan datos relativos a condenas e infracciones penales</td></tr>
<tr><td>4. Naturaleza del tratamiento:</td><td>☒ Recogida
☒ Extracción
☐ Confrontación
☒ Conservación
☐ Difusión
☐ Comunicación
☒ Estructuración
☒ Limitación
☐ Otras:</td><td>☒ Supresión
☒ Registro
☒ Consulta
☒ Interconexión
☐ Adaptación o modificación
☒ Utilización
☒ Destrucción</td></tr>
<tr><td>5. Finalidad(es) del tratamiento de los datos personales por cuenta del responsable del tratamiento:</td><td colspan="2">Prestación de los Servicios según consta identificado en el Contrato Principal.</td></tr>
<tr><td>6. Duración del tratamiento:</td><td colspan="2">El tratamiento de datos cesará en el momento en que se resuelva el Contrato Principal, con excepción de aquellos tratamientos que se encuentren en proceso y deban ser finalizados.</td></tr>
</table>

LISTA DE SUBENCARGADOS DEL TRATAMIENTO

El Encargado del tratamiento ha pedido la autorización para subcontratar con los siguientes subencargados, que han sido aprobados por el Responsable del tratamiento:

Nombre del subencargado	Datos de contacto	Descripción del tratamiento y el servicio contratado
Microsoft Ireland Operations, Ltd.	Attn: Data Protection One Microsoft Place South County Business Park Leopardstown Dublín 18, D18 P521, Irlanda	Proveedor de servicios cloud para la plataforma, incluyendo almacenamiento, bases de datos, máquinas virtuales, monitorización, logs y otros servicios Azure necesarios para la operación.

ANEXO II
CIBERSEGURIDAD DE LAS SOLUCIONES FLEXXIBLE

1. OBJETO Y ALCANCE

El presente Anexo tiene por objeto recoger de forma estructurada la información, compromisos y procedimientos que FLEXXIBLE como PROVEEDOR debe poner a disposición del CLIENTE, en cumplimiento de los requisitos establecidos en las normas internacionales ISO/IEC 27001:2022, ISO/IEC 27701:2019, ISO/IEC 27017:2021 e ISO/IEC 27018:2021, así como en la normativa aplicable, incluyendo el Esquema Nacional de Seguridad (ENS), el Reglamento General de Protección de Datos (RGPD) y la Directiva NIS2.

Estas normas y regulaciones establecen que el PROVEEDOR de servicios en la nube debe informar, acordar y documentar con el CLIENTE aspectos relacionados con la seguridad de la información, la protección de datos personales, la gestión de incidentes, la ubicación de datos, la devolución y eliminación de activos, entre otros.

El alcance del presente Anexo se limita a las Soluciones FLEXXIBLE contratadas por el CLIENTE y complementa el Contrato principal sin modificar sus condiciones económicas ni operativas.

2. ROLES Y RESPONSABILIDADES

A continuación se establecen los roles y responsabilidades en materia de seguridad de la información entre el PROVEEDOR del Servicio en la Nube y el CLIENTE del servicio en la nube.

2.1. Proveedor del servicio en la nube

El PROVEEDOR del servicio en la nube es responsable de:

- Seguridad de la Infraestructura: Implementar y mantener la seguridad física, lógica y de red en sus centros de datos y plataformas.
- Aislamiento de CLIENTES: Garantizar el aislamiento seguro de los entornos multi inquilino y la segmentación de datos.
- Gestión de Identidades y Accesos: Implementar autenticación robusta y acceso basado en roles (RBAC) para minimizar riesgos.
- Protección de Datos: Asegurar el cifrado de datos en tránsito y en reposo, así como copias de seguridad seguras.
- Monitoreo y Respuesta a Incidentes: Implementar herramientas de detección y respuesta ante incidentes de seguridad.
- Cumplimiento y Auditoría: Mantener conformidad con normativas aplicables y realizar auditorías periódicas.

El PROVEEDOR del servicio en la nube se compromete a:

- Documentar y comunicar sus capacidades de seguridad de la información, asegurando la transparencia de los controles implementados para la protección de la infraestructura, los datos y el servicio.
- Definir y mantener una matriz de responsabilidades para especificar las tareas de seguridad correspondientes a cada parte.
- Proporcionar mecanismos de configuración y recomendaciones de seguridad para que el CLIENTE pueda gestionar sus propios controles en el entorno de la nube.
- Informar al CLIENTE sobre los requisitos de seguridad que este debe implementar en el uso del servicio en la nube, incluyendo, entre otros:
    - Configuración de accesos y autenticación.
    - Uso de cifrado en datos en reposo y en tránsito.
    - Políticas de gestión de identidades y accesos.
    - Monitoreo y respuesta a incidentes.
- Mantener procedimientos de notificación y comunicación ante incidentes de seguridad que puedan impactar al CLIENTE.
- Documentar y comunicar los procedimientos para la devolución y eliminación de los activos del CLIENTE al finalizar el acuerdo del servicio.
- Definir los plazos y mecanismos para la eliminación segura de los datos y activos del CLIENTE de sus sistemas y plataformas, asegurando la conformidad con regulaciones aplicables.
- Proporcionar al CLIENTE un informe detallado sobre los activos eliminados, incluyendo la fecha de eliminación y la metodología utilizada.
- Garantizar la eliminación irreversible de todas las copias de los activos del CLIENTE en sus sistemas, salvo que existan requisitos legales

o contractuales que exijan su conservación por un periodo determinado.

2.2. CLIENTE del servicio en la nube

El CLIENTE del servicio en la nube es responsable de:

- Configuración Segura: Asegurar que la configuración de los servicios en la nube siga las mejores prácticas de seguridad.
- Gestión de Accesos: Controlar credenciales de usuarios y aplicar principios de menor privilegio.
- Protección de Datos: Implementar cifrado adicional si es necesario y definir estrategias de retención de datos.
- Monitoreo y Respuesta: Detectar actividades sospechosas en sus aplicaciones y reportarlas al proveedor si es necesario.
- Cumplimiento Normativo: Asegurar que su uso del servicio en la nube cumple con las regulaciones aplicables.

El CLIENTE del servicio en la nube se compromete a:

- Definir o ampliar sus políticas y procedimientos internos de seguridad de la información para su uso dentro del servicio en la nube, alineándolos con las recomendaciones del Proveedor.
- Garantizar que sus usuarios conozcan y cumplan con sus roles y responsabilidades en el uso del servicio en la nube, proporcionando capacitación y lineamientos específicos.
- Implementar y gestionar controles de seguridad sobre los datos, aplicaciones y configuraciones bajo su responsabilidad, incluyendo:
    - Definición y aplicación de políticas de acceso.
    - Uso adecuado de los mecanismos de cifrado proporcionados por el Proveedor.
    - Configuración de auditorías y monitoreo de actividades.
    - Planes de respaldo y recuperación ante desastres.
- Notificar al Proveedor sobre incidentes de seguridad relacionados con el servicio en la nube que puedan requerir acción conjunta.
- Respetar los acuerdos de nivel de servicio (SLA) en lo que respecta a la gestión de la seguridad y la privacidad de la información.
- Solicitar al Proveedor una descripción documentada del proceso de terminación del servicio que cubra la devolución y eliminación de sus activos.
- Validar que todos los activos hayan sido eliminados conforme al proceso documentado por el Proveedor.
- Coordinar con el Proveedor cualquier requisito específico para la devolución de activos físicos o digitales antes de la terminación del servicio.
- Confirmar la recepción de los activos devueltos y la conformidad con los procedimientos establecidos.
- Mantener registros de la eliminación y devolución de activos como evidencia de cumplimiento de la seguridad de la información.

2.3. Responsabilidades compartidas

Ambas partes acuerdan establecer mecanismos de comunicación permanentes para la gestión de seguridad del servicio en la nube, incluyendo:

- Reuniones periódicas de seguimiento.
- Canales de notificación de incidentes.
- Informes de cumplimiento y auditorías conjuntas.

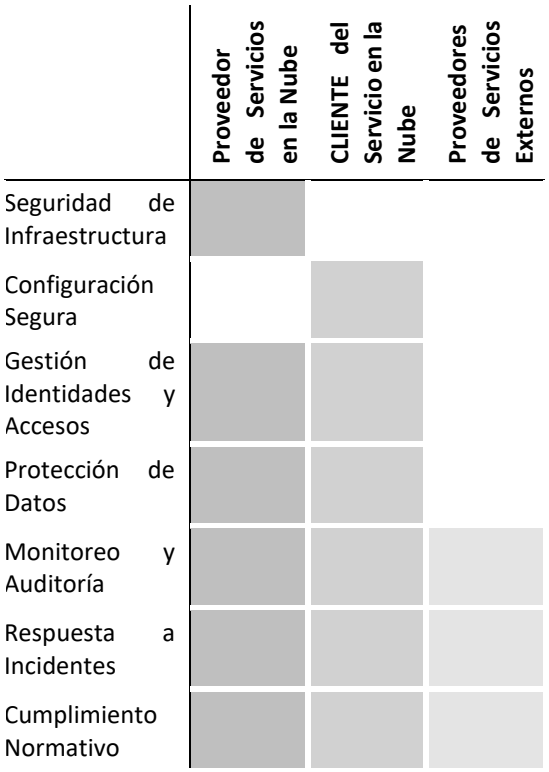
En caso de modificaciones en las responsabilidades o en las políticas de seguridad, ambas partes se comprometen a revisar y actualizar este acuerdo según sea necesario.

2.4. Proveedores de servicios externos

Los terceros que proporcionan servicios adicionales relacionados con la nube tienen la responsabilidad de:

- Cumplimiento de Seguridad: Aplicar medidas de seguridad compatibles con las políticas del proveedor de servicios en la nube.
- Integridad de los Servicios: Garantizar que las soluciones ofrecidas no introducen vulnerabilidades.
- Monitoreo y Auditoría: Proporcionar evidencia de controles de seguridad aplicados.
- Notificación de Incidentes: Informar al proveedor de la nube sobre cualquier incidente de seguridad que pueda impactar a CLIENTES.

2.5. Matriz de responsabilidades



3. UBICACIONES GEOGRÁFICAS Y PAÍSES DE ALMACENAMIENTO

El PROVEEDOR informa al CLIENTE que las Soluciones FLEXXIBLE se ejecutan sobre infraestructura cloud híbrida segura y escalable, basada en Microsoft Azure, Cloudflare y Cloud privado, cumpliendo con la normativa aplicable en materia de protección de datos y seguridad.

Para garantizar el cumplimiento legal, el PROVEEDOR utiliza regiones que ofrecen garantías adecuadas, priorizando centros de datos dentro del Espacio Económico Europeo (EEE). Actualmente, la solución está desplegada en la región West & North Europe de Azure, EU de Cloudflare y en Equinix España.

El PROVEEDOR se compromete a:

- Mantener la transparencia sobre las ubicaciones donde se almacenan y procesan los datos.
- Comunicar al CLIENTE cualquier cambio relevante en dichas ubicaciones.
- Garantizar que cualquier tratamiento de datos se realice conforme a la normativa aplicable.

4. GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN

El PROVEEDOR y el CLIENTE acuerdan establecer responsabilidades y procedimientos claros para la gestión de incidentes de seguridad de la información. Estos procedimientos incluyen la asignación de responsabilidades y la metodología para la detección, notificación y resolución de incidentes.

4.1. Alcance de los incidentes de seguridad

El PROVEEDOR notificará al CLIENTE los incidentes que puedan comprometer la seguridad del servicio, incluyendo:

- Accesos no autorizados a la plataforma.
- Violaciones de la integridad o disponibilidad de los datos procesados.
- Incidentes relacionados con la autenticación y autorización.
- Cualquier evento que afecte la confidencialidad, integridad o disponibilidad del servicio.

4.2. Nivel de divulgación y respuestas a los incidentes

- Divulgación de la Detección: La divulgación se realizará de acuerdo con la gravedad del incidente y el impacto potencial en el CLIENTE. Cada notificación incluirá: descripción del incidente e impacto, servicios afectados, cronología y medidas de contención aplicadas, próximas acciones y recomendaciones.
- Respuestas a los Incidentes: El PROVEEDOR proporcionará una respuesta adecuada a los incidentes, que puede incluir medidas de mitigación inmediatas, análisis forenses, y la implementación de cambios para prevenir incidentes futuros.

4.3. Plazos de notificación

El PROVEEDOR se compromete a notificar al CLIENTE según la gravedad del incidente:

- Incidentes Gaves (interrupción total o parcial de la plataforma): en un plazo máximo de 2 horas.
- Incidentes de Gravedad Media (impacto significativo en la funcionalidad): en un plazo máximo de 4 horas.
- Incidentes de Gravedad Baja: en un plazo máximo de 16 horas hábiles.

En todos los casos, se proporcionará una descripción clara del incidente, sus posibles implicaciones y las medidas correctivas tomadas.

Si el PROVEEDOR no cumple con los compromisos de notificación o respuesta, el CLIENTE podrá solicitar los Créditos de Nivel de Servicio especificados en la sección correspondiente del SLA, o en su caso, una extensión de los días de servicio, conforme a los créditos acumulados por incidentes de seguridad.

4.4. Procedimiento para la notificación de incidentes

El CLIENTE podrá notificar incidentes de seguridad de la información al PROVEEDOR utilizando los canales establecidos, como correo electrónico, portal de tickets o llamadas telefónicas a través del soporte 24x7.
El PROVEEDOR se compromete a confirmar la recepción de la notificación y proporcionar un número de ticket único para el seguimiento del incidente.

4.5. Información de contacto para la gestión de incidentes

Los CLIENTES de disponen de un equipo especializado para la gestión de incidentes de seguridad.

Los canales y horarios son los siguientes:

- **Contacto de Emergencia:**
  E-mail: security@flexxible.com
  Teléfono: +34 937 880 333
- **Soporte L2 (Incidencias relacionadas con seguridad):**
  Disponibilidad: 24x7
- **Soporte L3 (Soporte avanzado):**
  Horario: 09:00 a 18:00 (hora local)

5. SOLICITUDES DE PRUEBAS DIGITALES Y COLABORACIÓN FORENSE

El PROVEEDOR y el CLIENTE acuerdan los procedimientos específicos para responder a cualquier solicitud de pruebas digitales o evidencias relacionadas con incidentes de seguridad de la información en el entorno cloud.

5.1. Alcance de la evidencia

La recolección de evidencias podrá incluir:

- **Registros relevantes**: logs de acceso, registros de actividad de la plataforma y otros datos necesarios para la investigación.
- **Configuraciones del servicio** y parámetros técnicos.
- **Capturas forenses** del entorno, limitadas al alcance acordado.

5.2. Procedimiento y custodia

El PROVEEDOR garantizará la conservación segura de las evidencias, aplicando controles de acceso y trazabilidad para mantener la cadena de custodia.

Se documentará el proceso de recolección, almacenamiento y entrega para asegurar la integridad de la información.

5.3. Solicitud formal

El CLIENTE podrá solicitar evidencias mediante la apertura de un ticket de soporte en los canales habilitados.

El PROVEEDOR proporcionará la documentación necesaria para formalizar la solicitud, incluyendo detalles del proceso y formato de entrega.

5.4. Plazo de entrega

El PROVEEDOR se compromete a entregar la evidencia solicitada en un plazo máximo de 30 días hábiles desde la aceptación de la solicitud, salvo que la naturaleza del incidente requiera un tiempo adicional, que será comunicado al CLIENTE.

5.5. Colaboración forense

En caso de investigaciones forenses, el PROVEEDOR colaborará plenamente con el CLIENTE, brindando acceso a la información necesaria para el análisis del incidente, siempre respetando:

- La protección de secretos comerciales del PROVEEDOR.
- La confidencialidad de datos de otros CLIENTES.

5.6. Limitaciones

Las evidencias se proporcionarán únicamente en la medida en que no vulneren la normativa aplicable ni los derechos de terceros. Cualquier coste adicional derivado de la preparación y entrega será informado previamente al CLIENTE.

6. JURISDICCIÓN Y REQUISITOS LEGALES

6.1. Jurisdicción y ley aplicable

La prestación del servicio se regirá por la legislación española y, en particular, por la normativa europea

aplicable en materia de protección de datos y seguridad de la información. Las partes acuerdan someterse a la jurisdicción exclusiva de los Juzgados y Tribunales de Barcelona, salvo disposición imperativa en contrario.

6.2. Normativa aplicable

El PROVEEDOR declara cumplir con:

- El Reglamento (UE) 2016/679 (RGPD) y normativa nacional complementaria.
- Normativa aplicable en materia de privacidad y seguridad de la información, incluyendo el Esquema Nacional de Seguridad (ENS) y la Directiva NIS2.
- Normas internacionales ISO/IEC 27001, 27701, 27017 y 27018.

6.3. Requisitos legales identificados

El PROVEEDOR garantiza la implementación de:

- Cifrado para proteger la información de identificación personal (PII) conforme a la normativa aplicable.

- Medidas técnicas y organizativas para asegurar la confidencialidad, integridad y disponibilidad de la información.

6.4. Información a solicitud del CLIENTE

El PROVEEDOR pondrá a disposición del CLIENTE, previa solicitud formal:

- Evidencias de cumplimiento con la legislación aplicable y requisitos contractuales.
- Descripción de los controles criptográficos implementados para garantizar el cumplimiento normativo.

7. PROTECCIÓN DE REGISTROS

El PROVEEDOR recopila y almacena registros relacionados con el uso de los servicios en la nube por parte del CLIENTE, garantizando su integridad, confidencialidad y disponibilidad.

Los registros incluyen, pero no se limitan a:

- Logs de acceso y autenticación.
- Actividad del sistema y eventos operativos.
- Modificaciones de configuración.
- Eventos de seguridad relevantes.

7.1. Controles de seguridad aplicados

Todos los registros son protegidos mediante controles técnicos y organizativos adecuados, incluyendo:

- Cifrado en tránsito y en reposo, conforme a estándares internacionales
- Mecanismos de auditoría y monitoreo continuo para detectar accesos no autorizados o alteraciones.
- Políticas de retención alineadas con los requisitos legales, contractuales y normativos aplicables.

7.2. Acceso y confidencialidad

El acceso a los registros está restringido al personal autorizado del PROVEEDOR, bajo el principio de mínimo privilegio y con trazabilidad completa de las operaciones realizadas.

7.3. Disponibilidad y conservación

Los registros se conservarán durante el plazo necesario para cumplir con las obligaciones legales y contractuales, así como para la investigación y resolución de incidentes de seguridad.

7.4. Información de solicitud al CLIENTE

El PROVEEDOR proporcionará al CLIENTE, previa solicitud formal:

- Descripción de los controles implementados para la protección de registros.
- Evidencias de cumplimiento con las políticas de retención y seguridad aplicables.

El acceso a registros por parte del CLIENTE se limitará a aquellos que no vulneren la normativa aplicable ni los derechos de terceros. Cualquier coste adicional derivado de la preparación y entrega será informado previamente al CLIENTE.

8. VIGENCIA Y MODIFICACIONES

8.1. Duración

El presente Anexo permanecerá vigente mientras el CLIENTE utilice los servicios en la nube proporcionados por el PROVEEDOR, directamente o a través del distribuidor, y se considerará parte integrante del contrato principal.

8.2. Modificaciones

El PROVEEDOR se reserva el derecho de modificar el contenido del presente Anexo para:

- Adaptarlo a cambios normativos o nuevas obligaciones legales.
- Incorporar mejores prácticas de seguridad o actualizaciones técnicas que incrementen la protección del servicio.

Cualquier modificación relevante será comunicada al CLIENTE con una antelación mínima de 30 días naturales, salvo que la modificación sea necesaria para dar cumplimiento inmediato a una disposición legal o regulatoria.
La comunicación se realizará por medios electrónicos a los contactos designados por el CLIENTE. La continuidad en el uso del servicio tras la entrada en vigor de las modificaciones se considerará aceptación tácita de las mismas.

9. GESTIÓN DE VULNERABILIDADES TÉCNICAS

El PROVEEDOR se compromete a garantizar la seguridad de los servicios prestados mediante la identificación, evaluación y corrección de vulnerabilidades técnicas que puedan afectar la infraestructura de la nube y la plataforma FLEXXIBLE.

9.1. Detección, evaluación, remediación y plazos

Se realizarán escaneos de seguridad periódicos y pruebas de penetración utilizando herramientas automatizadas y procedimientos especializados, al menos una vez al año.

Las vulnerabilidades detectadas serán evaluadas en función de su criticidad, considerando severidad, posibilidad de explotación e impacto en los servicios.

Las vulnerabilidades críticas serán tratadas con máxima urgencia.

El PROVEEDOR implementará planes de mitigación y remediación en un plazo razonable.

Para vulnerabilidades críticas, se aplicarán medidas correctivas en un plazo máximo de 30 días desde su detección.

Se documentará el plan de acción, incluyendo actualizaciones y parches aplicados.

9.2. Notificación al CLIENTE

El PROVEEDOR notificará al CLIENTE cualquier vulnerabilidad crítica que pueda afectar la seguridad del servicio en un plazo máximo de 96 horas desde su identificación.

La notificación se realizará mediante correo electrónico a los contactos designados por el CLIENTE.

El aviso incluirá: naturaleza de la vulnerabilidad, riesgo asociado y acciones correctivas implementadas o en curso.

9.3. Actualizaciones y parches

El PROVEEDOR llevará a cabo actualizaciones regulares y aplicará parches de seguridad de manera oportuna para proteger la infraestructura contra vulnerabilidades conocidas.

Los plazos de implementación de parches serán acordados con el CLIENTE para minimizar la interrupción de los servicios.

Cuando sea necesario aplicar un parche de emergencia para corregir una vulnerabilidad o fallo crítico, el PROVEEDOR podrá implementarlo sin previo aviso, emitiendo posteriormente una notificación con los detalles del mismo.

El ciclo de actualización será documentado y comunicado al CLIENTE cuando implique impacto en el servicio.

9.4. Responsabilidad del CLIENTE

El CLIENTE colaborará en la identificación y resolución de vulnerabilidades y notificará al PROVEEDOR cualquier incidente de seguridad detectado durante el uso del servicio.

10. COPIAS DE SEGURIDAD

El PROVEEDOR garantizará la disponibilidad, integridad y confidencialidad de la información del CLIENTE mediante políticas y procedimientos rigurosos de copias de seguridad. Estas copias incluirán todos los datos relevantes para el servicio, como configuraciones, bases de datos y componentes críticos de la plataforma FLEXXIBLE. Las copias se realizarán diariamente, preferentemente en horario nocturno para minimizar el impacto en la operativa.

10.1. Seguridad y retención

Todas las copias estarán cifradas en tránsito y en reposo utilizando estándares internacionales como AES-256, y se almacenarán en ubicaciones seguras con medidas físicas y lógicas, incluyendo control de acceso y autenticación multifactor.

Se garantizará la segregación de datos entre CLIENTES y, cuando sea necesario, se aplicará redundancia geográfica para asegurar la disponibilidad ante desastres.

Las copias se conservarán durante un período de 7 días, tras el cual serán eliminadas de forma segura conforme a las políticas de gestión y destrucción de datos.

10.2. Verificación, restauración y comunicación

El PROVEEDOR realizará pruebas de restauración de forma periódica para verificar la integridad y recuperabilidad de los datos, documentando los resultados y el proceso. Estas pruebas incluirán restauraciones parciales y completas, así como la verificación de la consistencia de los datos, y se efectuarán con una frecuencia regular, siendo al menos una vez al año el mínimo exigido.

El PROVEEDOR establecerá procedimientos claros y probados para la restauración de datos desde las copias de seguridad, que se activarán en caso de pérdida de datos o desastre. Los plazos para la restauración serán los siguientes:

- Restauración completa: dentro de un plazo máximo de 24 horas tras el incidente, utilizando el RPO del servicio o superior

El CLIENTE será notificado por correo electrónico tanto al inicio como al finalizar el proceso de restauración, indicando el alcance y estado de los datos recuperados.

10.4. Acceso seguro

El acceso a las copias se realizará de forma segura y segregada, limitado a personal autorizado y aplicando autenticación fuerte. En caso de ofrecer acceso a instantáneas virtuales, se garantizará que solo usuarios autorizados del CLIENTE puedan acceder.

11. SINCRONIZACIÓN DE RELOJ

El PROVEEDOR garantiza que todos los sistemas críticos utilizados para la prestación de los servicios están sincronizados con una fuente de tiempo confiable, utilizando el protocolo estándar Network Time Protocol (NTP). Esta sincronización asegura la coherencia temporal necesaria para la correcta operación de los servicios y el registro de eventos.

Los sistemas de FLEXXIBLE sincronizan sus relojes con el servidor hora.roa.es, alineado con los estándares internacionales para garantizar la precisión del tiempo. Para permitir la sincronización adecuada de los sistemas locales del CLIENTE con los servicios de FLEXXIBLE, se recomienda utilizar el protocolo NTP y configurar los sistemas para sincronizarse con la siguiente fuente:

- Servidor NTP: hora.roa.es

El PROVEEDOR de servicios en la nube se compromete a informar al CLIENTE cualquier cambio relacionado con la fuente de tiempo utilizada y a colaborar para mantener la sincronización entre los sistemas durante la operación de los servicios. Esta comunicación se realizará por medios electrónicos y con antelación suficiente para evitar interrupciones.

12. USO DE PROGRAMAS DE UTILIDAD PRIVILEGIADOS

El PROVEEDOR de servicios en la nube se compromete a identificar, gestionar y auditar el uso de programas de utilidad privilegiados en su infraestructura. El acceso a estos programas está estrictamente limitado al personal autorizado, basado en roles definidos y bajo el principio de mínimo privilegio. Los registros de acceso y uso de estos programas se auditan de manera periódica para garantizar que no se eludan los procedimientos operativos y de seguridad establecidos. Cualquier uso de estos programas será sometido a una revisión regular y los registros de auditoría estarán disponibles para su inspección en caso de ser necesario.

13. USO DE CRIPTOGRAFÍA

El PROVEEDOR informa al CLIENTE sobre el uso de criptografía para proteger la información procesada en la plataforma FLEXXIBLE, aplicando mecanismos robustos conforme a estándares internacionales y normativa aplicable.

13.1. Criptografía en tránsito y en reposo

Los datos transmitidos entre el CLIENTE y la plataforma se protegen mediante TLS 1.2 o superior, garantizando la confidencialidad e integridad durante la transmisión. La información almacenada se cifra con algoritmos avanzados como AES-256, asegurando que los datos sensibles no sean accesibles sin autorización.

13.2. Gestión de claves

La gestión de claves criptográficas se realiza

siguiendo las mejores prácticas de seguridad. Asimismo, el CLIENTE puede aplicar cifrado adicional a archivos y documentos antes de cargarlos, utilizando herramientas propias o las proporcionadas por el PROVEEDOR.

13.3. Capacidades y soporte

El PROVEEDOR pondrá a disposición del CLIENTE documentación técnica detallada, incluyendo guías de implementación, mejores prácticas y soporte especializado para la configuración y gestión de cifrado.

Además, se compromete a mantener la infraestructura actualizada con los últimos algoritmos y protocolos recomendados, notificando cualquier cambio significativo que afecte la protección de datos.

13.4. Protección de PII y transparencia

El PROVEEDOR de servicios en la nube garantiza el cifrado de datos personales identificables (PII) tanto en tránsito como en reposo, aplicando controles criptográficos en bases de datos, copias de seguridad y almacenamiento en la nube.

Se ofrecerá información actualizada sobre los mecanismos de cifrado utilizados, y cualquier modificación en la política de criptografía será comunicada al CLIENTE con antelación. El CLIENTE podrá revisar auditorías y certificaciones relacionadas con la protección criptográfica de la PII.

14. CICLO DE VIDA DE DESARROLLO SEGURO

El PROVEEDOR de servicios en la nube garantiza que el ciclo de vida de desarrollo de sus servicios sigue procedimientos de desarrollo seguro, conforme a estándares internacionales y mejores prácticas. Las principales medidas incluyen:

- Revisión de Código: Se realizan revisiones regulares mediante herramientas automatizadas para identificar vulnerabilidades.
- Pruebas de Seguridad: Se llevan a cabo pruebas de penetración y análisis de vulnerabilidades durante todo el ciclo de desarrollo.
- Gestión de Parcheo: Se implementa un proceso para corregir rápidamente cualquier vulnerabilidad a través de parches y actualizaciones de seguridad.
- Control de Acceso: El acceso a sistemas de desarrollo y código fuente está restringido a usuarios autorizados, aplicando el principio de mínimo privilegio.

El PROVEEDOR de servicios en la nube se compromete a proporcionar al CLIENTE información sobre las prácticas utilizadas para asegurar la plataforma durante el ciclo de vida del desarrollo, en la medida en que sea compatible con su política de divulgación. No obstante, podrán aplicarse restricciones a la divulgación de información técnica específica por motivos de propiedad intelectual y seguridad operacional.

El PROVEEDOR se compromete a mejorar de forma continua las prácticas de desarrollo seguro, adaptándose a nuevas amenazas y actualizando las políticas conforme sea necesario para garantizar la protección de los servicios.

15. GESTIÓN DEL CAMBIO

El PROVEEDOR garantiza la gestión estructurada de cambios en el servicio en la nube, asegurando que cualquier modificación que pueda afectar la seguridad de la información sea evaluada y comunicada oportunamente al CLIENTE. Este proceso incluye la clasificación, planificación y notificación de cambios relevantes que impacten la disponibilidad, integridad o confidencialidad del servicio.

15.1. Información y comunicación de cambios

El PROVEEDOR informará al CLIENTE sobre los cambios relevantes, proporcionando como mínimo:

- Categoría del cambio: clasificado como menor, crítico o de emergencia según su impacto potencial.
- Fecha y hora previstas: con antelación suficiente para permitir la planificación del CLIENTE.
- Descripción técnica: detallando la modificación realizada en el servicio o en los sistemas subyacentes.
- Notificación de inicio y finalización: confirmando su correcta aplicación.

La comunicación se realizará mediante portal de CLIENTES, correo electrónico y, cuando aplique, a través de API de gestión de cambios para consulta en tiempo real.

15.2. Cambios de emergencia y dependencias de terceros

Cuando sea necesario aplicar un cambio de

emergencia para corregir una vulnerabilidad o fallo crítico, el PROVEEDOR podrá implementarlo sin previo aviso, emitiendo posteriormente una notificación con los detalles del cambio realizado. Asimismo, cuando la plataforma FLEXXIBLE dependa de servicios proporcionados por terceros, el PROVEEDOR informará al CLIENTE sobre cualquier modificación significativa derivada de dichos proveedores.

El PROVEEDOR mantiene un proceso de mejora continua en la gestión del cambio, asegurando que el CLIENTE disponga de la información necesaria para evaluar el impacto de las modificaciones en la seguridad del servicio.

16. DEVOLUCIÓN, TRANSFERENCIA Y/O ELIMINACIÓN DE PII (INFORMACIÓN DE IDENTIFICACIÓN PERSONAL)

El PROVEEDOR garantiza la protección de los derechos del CLIENTE en relación con la información personal identificable (PII) procesada en la plataforma. Para ello, mantiene una política específica sobre la devolución, transferencia y/o eliminación de PII, que se pondrá a disposición del CLIENTE cuando sea requerida.

En caso de terminación del servicio, el PROVEEDOR se compromete a devolver los datos del CLIENTE en un formato seguro y estándar, y posteriormente proceder a su eliminación definitiva mediante técnicas de borrado seguro que impidan su recuperación, conforme a la normativa aplicable. Si existieran obligaciones legales que requieran la conservación temporal de determinados datos, el PROVEEDOR informará al CLIENTE y garantizará su protección hasta su eliminación definitiva.

17. CONTACTO

El CLIENTE dispondrá de canales oficiales para comunicarse con el PROVEEDOR en relación con la prestación del servicio, incluyendo:

- Soporte técnico y apertura de incidentes.
- Consultas sobre seguridad, cumplimiento normativo y protección de datos.
- Solicitudes relacionadas con la gestión de registros y evidencias.

El PROVEEDOR pondrá a disposición del CLIENTE los medios de contacto habilitados y garantizará su disponibilidad durante la vigencia del servicio. Toda comunicación se realizará a través de los canales designados para asegurar trazabilidad y confidencialidad.

18. VIGENCIA

Este Anexo entrará en vigor en la fecha de su firma por ambas Partes y tendrá la misma vigencia que los Términos y Condiciones Generales de Contratación.

ANEXO III
ACUERDO DE NIVEL DE SERVICIO (SLA) – Flexxible Portal

El presente Anexo regula los niveles de servicio aplicables a la prestación del servicio Flexxible Portal. En caso de contradicción entre este Anexo y el cuerpo del contrato, prevalecerá lo dispuesto en el contrato salvo en lo expresamente referido a niveles de servicio, materia en la que prevalece este Anexo.

1. OBJETO Y ALCANCE DEL SERVICIO

Este Acuerdo define los compromisos de disponibilidad y los tiempos de atención de incidencias, consultas y peticiones relativos al "Servicio", entendido como los siguientes componentes operados por Flexxible:

- **Flexxible Portal** — el portal SaaS (acceso, autenticación y funcionalidades de la interfaz de usuario).

- **Flexxible Portal API** — la API que sustenta la ingesta y el procesamiento de la telemetría recibida desde los dispositivos.

Estos componentes son los publicados y monitorizados de forma continua en la página pública de estado del servicio, **https://status.portal.flexxible.com**, que constituye la fuente oficial del estado del Servicio.

Aclaración sobre el FlexxAgent. El agente DEX (FlexxAgent) se ejecuta en los dispositivos del Cliente. Su capacidad de reportar depende de que el dispositivo esté encendido y conectado a la red, circunstancia ajena al control de Flexxible. Por ello, la disponibilidad del FlexxAgent en el endpoint queda excluida del compromiso de disponibilidad de la Sección 5; el compromiso aplica al procesamiento de la telemetría una vez recibida por la Plataforma.

2. DEFINICIONES

- **Petición:** Evaluación, planificación y entrega de una necesidad nueva (alta, cambio o ampliación). Las peticiones quedan fuera del SLA de resolución: solo se comprometen el tiempo de primera respuesta y la planificación por mutuo acuerdo.

- **Consulta:** Resolución de dudas sobre el uso, configuración o funcionamiento del producto, sin que exista una avería del Servicio.

- **Incidencia:** Degradación o interrupción no planificada del Servicio respecto a su funcionamiento normal. Se clasifica en grave, media o leve según la Sección 3.

- **Incidencia grave:** Problema crítico que interrumpe totalmente el Servicio o afecta de forma generalizada, sin solución temporal disponible, y que requiere atención inmediata.

- **Incidencia media:** Problema que afecta parcialmente al Servicio o a un subconjunto de usuarios/dispositivos, con impacto moderado y existiendo o no solución temporal.

- **Incidencia leve:** Problema de bajo impacto que no impide el funcionamiento del Servicio y puede resolverse sin urgencia.

- **Tiempo de respuesta:** Intervalo entre la apertura de la incidencia por un canal válido y el acuse de recepción con asignación y diagnóstico inicial por parte de Flexxible. Es un compromiso.

- **Tiempo de mitigación (solución temporal o "workaround"):** Intervalo hasta restablecer el funcionamiento del Servicio mediante una solución temporal, aunque la causa raíz siga abierta. Es un compromiso.

- **Tiempo de resolución:** Intervalo hasta el cierre de la causa raíz, con el Servicio plenamente restablecido y sin solución temporal pendiente. Es un objetivo, no un compromiso, y está sujeto a la parada de reloj de la Sección 6 (por depender frecuentemente de terceros o de la infraestructura del Cliente).

- **Parada de reloj ("clock-stop"):** Suspensión del cómputo de los tiempos mientras la resolución dependa del Cliente o de un tercero ajeno a Flexxible (ver Sección 6).

- **Disponibilidad:** Porcentaje de tiempo, dentro de la ventana mensual de medición, durante el cual el Servicio está operativo y accesible, calculado según la Sección 5.

- **Horario natural / horario hábil:** El cómputo "natural" corre de forma continua (horas/días corridos). El cómputo "hábil" corre solo dentro del horario laboral acordado (8x5). La base de reloj de cada nivel se indica en las tablas de la Sección 4.

- **8x5 / 24x7:** 8x5 = horario laboral, lunes a viernes en jornada laboral (excluidos festivos). 24x7 = veinticuatro horas, todos los días del año.

3. CLASIFICACIÓN DE INCIDENCIAS

Clasificación. El Cliente indica la severidad propuesta al abrir la incidencia. Flexxible confirma o ajusta la clasificación en el momento del acuse de recepción, conforme a los criterios de esta Sección. Tanto el Cliente como Flexxible pueden solicitar la reclasificación si la evolución de la incidencia lo justifica.

Discrepancias. En caso de desacuerdo sobre la severidad, se aplica de forma provisional la clasificación más alta de las dos propuestas mientras se resuelve la discrepancia mediante la matriz de escalado (Sección 9). La resolución de la discrepancia se documenta en el ticket.

Criterios y ejemplos orientativos

Severidad	Ejemplos orientativos (Flexxible Experience)
Grave	Portal SaaS totalmente inaccesible para todos los usuarios; interrupción total de la ingesta de telemetría de toda la flota; pérdida de una funcionalidad crítica que impide operar y afecta de forma generalizada, sin solución temporal.
Media	Lentitud o degradación parcial del portal; retraso significativo en la ingesta; un módulo no crítico no disponible; afectación limitada a un subconjunto de usuarios o dispositivos.
Leve	Error cosmético o de presentación; incidencia en un único dispositivo o usuario sin impacto en el Servicio; incidencia con solución temporal aplicable de inmediato.

Los ejemplos son orientativos; la clasificación final atiende al impacto y alcance reales de cada caso.

4. NIVELES DE SERVICIO

4.1 Gestión de peticiones y consultas

Tipología	Primera respuesta	Resolución	Horario	Base de reloj
Petición	16 h	Por mutuo acuerdo (fuera de SLA)	8x5	Hábil
Consulta	16 h	16 h (objetivo)	8x5	Hábil

Las peticiones no tienen tiempo de resolución comprometido: su alcance y plazo se acuerdan caso por caso.

4.2 Gestión de incidencias

Los tiempos de respuesta y de mitigación son compromisos. El tiempo de resolución es un objetivo, sujeto a la parada de reloj (Sección 6). *Todos los tiempos de esta tabla se computan en horario natural salvo la incidencia leve, que se computa en horario hábil*

Severidad	Respuesta	Mitigación	Resolución (objetivo)	Horario	Base de reloj
Grave	2 h	8 h	24 h	24x7	Natural
Media	4 h	24 h	72 h	24x7	Natural
Leve	16 h	—	5 días hábiles	8x5	Hábil

5. DISPONIBILIDAD

Servicio medido	Disponibilidad	Ventana de medición	Horario
Flexxible Portal	99 %	Mensual (mes natural)	24x7
Flexxible Portal API	99 %	Mensual (mes natural)	24x7

Fórmula. Disponibilidad (%) = (Minutos totales del mes − Minutos de indisponibilidad) / Minutos totales del mes × 100. Los minutos de mantenimiento planificado y los excluidos por la Sección 7 no se contabilizan como indisponibilidad.

Indisponibilidad. Se considera indisponible el componente medido cuando no es accesible o no procesa telemetría por causa imputable a Flexxible, confirmado por la monitorización de Flexxible. No constituye indisponibilidad la degradación parcial de rendimiento, que se gestiona como incidencia.

Medición y fuente oficial. La disponibilidad y los incidentes de cada componente se monitorizan de forma continua mediante un proveedor independiente y se publican, en tiempo real e históricamente, en la página pública de estado https://status.portal.flexxible.com.

6. PARADA DE RELOJ (“CLOCK-STOP”)

El cómputo de los tiempos de mitigación y de resolución

queda suspendido mientras concurra cualquiera de las siguientes circunstancias, reanudándose al cesar la causa:

- Espera de información, acceso, accesos remotos o confirmación por parte del Cliente.
- Dependencia de un tercero ajeno a Flexxible (proveedor cloud, autoridad de certificación/PKI, operador de red, fabricante de hardware o software).
- Causa raíz situada fuera del perímetro del Servicio: infraestructura del Cliente (controladores de dominio, red, almacenamiento, ITSM, dispositivos).
- Ventana de mantenimiento planificado conforme a la Sección 7.
- Solicitud de cambio que exceda el alcance de la incidencia abierta.

La activación de una parada de reloj se documenta en el ticket con su causa y momento.

7. EXCLUSIONES

Quedan excluidos de los compromisos de este Acuerdo, y no computan como indisponibilidad ni como incumplimiento de tiempos:

- Mantenimiento planificado, notificado con al menos 48 h de antelación y publicado en la página de mantenimiento del estado del servicio (**https://status.portal.flexxible.com/maintenance**) o pactado de mutuo acuerdo mediante canal establecido, preferentemente en ventana de bajo impacto.
- Fuerza mayor y causas ajenas al control razonable de Flexxible.
- Fallos de la infraestructura, redes, servicios o aplicaciones de terceros del Cliente.
- Indisponibilidad del FlexxAgent derivada de que el dispositivo esté apagado, suspendido o sin conexión.
- Uso del Servicio fuera de las condiciones soportadas, configuraciones no autorizadas o modificaciones realizadas por el Cliente o terceros.
- Versiones del software fuera del ciclo de soporte vigente.
- Incidencias cuya causa raíz se localice en sistemas del Cliente o de terceros (PKI, identidad, ITSM, etc.).

8. APERTURA Y GESTIÓN DE SOLICITUDES

- **Canales.** Portal de soporte de Flexxible (canal preferente) y correo electrónico de soporte. Para incidencias graves se habilita además un canal telefónico de guardia
- **Personas autorizadas.** Solo los contactos designados por el Cliente en el alta del servicio pueden abrir y escalar solicitudes. El Cliente mantiene actualizada esta lista y debe notificar cualquier cambio a Flexxible.
- **Horario de apertura.** Las incidencias graves y medias pueden abrirse 24x7; las leves, peticiones y consultas, en horario 8x5.
- **Inicio del cómputo.** Los tiempos comienzan a contar desde la recepción de la solicitud por un canal válido y con la información mínima necesaria para su gestión.
- **Datos de contacto.** Para incidencias se deberá indicar un teléfono de contacto con el fin de acelerar la solución de la misma.

9. MATRIZ DE ESCALADO

Nivel	Responsable	Activación
N1	Soporte de Flexxible	Recepción y gestión inicial de toda solicitud.
N2	Ingeniería de Flexxible	Incidencia sin mitigar dentro del plazo, o discrepancia de severidad no resuelta en N1.
N3	Responsable de Servicio / Dirección	Incidencia grave sin mitigar, incumplimiento de SLA o conflicto no resuelto en N2.

El Cliente puede solicitar el escalado a través de los canales de la Sección 8 indicando el identificador del ticket.

10. DISPONIBILIDAD

Flexxible facilita una plataforma que incluye:

- Detalle de mantenimientos planificados
- Estado en tiempo real

El Cliente puede suscribirse a las notificaciones de estado (correo, Slack, webhook o RSS), por componente, en **https://status.portal.flexxible.com**, recibiendo aviso de la apertura, actualización y cierre de cada incidente.

11. CRÉDITOS DE SERVICIO

Cuando la disponibilidad mensual real de la Plataforma SaaS quede por debajo del objetivo por causa imputable a Flexxible, el Cliente tendrá derecho, previa solicitud, a los siguientes créditos sobre la cuota mensual del servicio afectado:

Disponibilidad mensual real	Crédito (sobre cuota mensual)
≥ 99,5 %	Sin crédito (objetivo cumplido)
99,0 % – 99,49 %	5 %
98,0 % – 98,99 %	10 %
< 98,0 %	15 %

Los créditos son el único remedio por incumplimiento de disponibilidad, no son acumulables entre meses, tienen como límite máximo el 15 % de la cuota mensual del servicio afectado y deben solicitarse en los 30 días naturales siguientes a la entrega del informe mensual. Esta sección es opcional y puede suprimirse si las partes no acuerdan créditos.