TÉRMINOS Y CONDICIONES

Perfecto. Para un ERP de facturación/contabilidad (SaaS) que trata datos sensibles "de negocio" y datos personales, lo más **blindado** suele ser un **"Master" de Términos y Condiciones / Términos del Servicio** + **anexos** (DPA, SLA, etc.). Te dejo una **estructura completa** (solo índice + qué cubre cada punto), pensada para España/UE y contratación online (LSSI-CE) + RGPD/LOPDGDD.

---

0) Documentos que componen el "pack legal"

- 0.1 **Términos del Servicio (TyC / ToS)** (documento principal)
- 0.2 **Política de Privacidad** (web/marketing y usuarios)
- 0.3 **Política de Cookies** (si aplica)
- 0.4 **Acuerdo de Tratamiento de Datos (DPA / Encargo de Tratamiento)** (Anexo A, art. 28 RGPD)
- 0.5 **Anexo de Medidas de Seguridad** (TOMs, art. 32 RGPD)
- 0.6 **SLA / Soporte / Mantenimiento** (Anexo B)
- 0.7 **Política de Uso Aceptable (AUP)** (Anexo C)
- 0.8 **Listado de Subencargados** (Anexo D) + mecanismo de actualización
- 0.9 **Condiciones Comerciales** (planes, precios, límites, add-ons) (Anexo E)
- 0.10 **Acuerdo de nivel de servicio de incidentes de seguridad** (Anexo F) (opcional, pero muy recomendable)

---

1) Identificación del prestador y alcance legal del sitio

- 1.1 Datos identificativos del prestador (empresa, domicilio, NIF, contacto, registro, etc.) (LSSI-CE)
- 1.2 Objeto del documento y a qué productos/URLs aplica
- 1.3 Aceptación expresa y capacidad para contratar (empresa/autónomo/representante)

---

2) Definiciones

Glosario fuerte: “Servicio”, “Cliente”, “Usuario”, “Cuenta”, “Contenido/Datos del Cliente”, “Datos Personales”, “Responsable/Encargado”, “Subencargado”, “Pedido/Order Form”, “Plan”, “SLA”, “Incidente de Seguridad”, etc. (evita ambigüedades).

---

3) Descripción del servicio

- 3.1 Funcionalidades principales (facturación, contabilidad, informes, integraciones, etc.)
- 3.2 Alcance: qué **incluye** y qué **no incluye** (p. ej., asesoramiento fiscal/contable)
- 3.3 Requisitos técnicos mínimos / navegador / disponibilidad

---

4) Elegibilidad, tipo de cliente y rol del usuario

- 4.1 Servicio **B2B** (si es tu enfoque) y qué pasa si contrata un consumidor (cláusula “si aplica normativa de consumo…”)
- 4.2 Roles internos (admin de empresa, contable, empleado, auditor…)
- 4.3 Responsabilidad del Cliente por credenciales, accesos y permisos

---

5) Registro, cuentas y seguridad de acceso

- 5.1 Alta, verificación, usuarios autorizados
- 5.2 Gestión de contraseñas/2FA (si existe), políticas de seguridad
- 5.3 Actividad sospechosa, deber de notificación por parte del Cliente
- 5.4 Prohibición de compartir cuentas / reventa sin autorización

---

6) Contratación electrónica y formación del contrato

Bloque “LSSI-CE blindado”:

- 6.1 Pasos para contratar (checkout/aceptación)
- 6.2 Archivo del contrato y accesibilidad para el usuario
- 6.3 Idioma(s) disponibles

- 6.4 Medios para corregir errores antes de finalizar
- 6.5 Confirmación de contratación / emails / prueba de aceptación

---

7) Planes, precios, impuestos y condiciones económicas

- 7.1 Planes, límites (usuarios, empresas, facturas, almacenamiento, API)
- 7.2 Precios, moneda, impuestos (IVA)
- 7.3 Cambios de precio: preaviso, entrada en vigor, derecho a no renovar
- 7.4 Gastos de terceros (pasarelas, firma electrónica, SMS, etc.)
- 7.5 Promociones/cupones y condiciones

---

8) Facturación, pagos y morosidad

- 8.1 Métodos de pago, ciclo de facturación
- 8.2 Impagos: reintentos, intereses (si aplica), suspensión del servicio, recuperación
- 8.3 Reembolsos (si ofreces) / "no refunds" (siempre con matices legales)
- 8.4 Disputas de facturación: plazos y procedimiento

---

9) Prueba gratuita, beta y funcionalidades experimentales

- 9.1 Duración, límites, conversión a pago
- 9.2 "Beta features": sin SLA, posibles errores, feedback, limitación de responsabilidad

---

10) Soporte, mantenimiento y SLA

- 10.1 Canales de soporte, horarios, niveles (Standard/Premium)
- 10.2 Ventanas de mantenimiento planificado
- 10.3 Disponibilidad objetivo (uptime), créditos de servicio (si aplica)
- 10.4 Copias de seguridad, RPO/RTO (si vas a comprometerlos)

---

11) Cambios del servicio

- 11.1 Evolución del producto (mejoras, cambios UI)
- 11.2 Cambios “materiales” que afecten al Cliente: aviso y opciones
- 11.3 Deprecación de API/integraciones: calendario y soporte de versiones

---

12) Datos del Cliente: titularidad, uso y gestión

- 12.1 Titularidad: “los datos son del Cliente”
- 12.2 Licencia limitada para operar el servicio (procesamiento)
- 12.3 Calidad/licitud de los datos: responsabilidad del Cliente
- 12.4 Logs y metadatos (telemetría mínima) y su finalidad (operación/seguridad)

---

13) Confidencialidad

- 13.1 Obligación mutua de confidencialidad
- 13.2 Excepciones (dominio público, requerimiento legal)
- 13.3 Personal autorizado y deber de secreto
- 13.4 Duración (que sobreviva a la terminación)

---

14) Protección de datos personales (bloque RGPD “duro”)

Aquí conviene separar **cláusula resumen** en TyC + **DPA** como anexo:

- 14.1 Roles: normalmente Cliente = Responsable, MAGOS = Encargado (y aclaraciones)
- 14.2 Objeto, naturaleza, finalidades, categorías de datos e interesados (referencia al Anexo DPA)
- 14.3 Instrucciones documentadas y limitación de uso
- 14.4 Medidas técnicas y organizativas (TOMs) + enfoque de riesgo
- 14.5 Subencargados: autorización (general/específica), lista, “flow-down”
- 14.6 Transferencias internacionales (si las hay): mecanismo (SCC, etc.) y transparencia
- 14.7 Asistencia al Cliente: derechos de interesados, DPIA, consultas AEPD

- 14.8 Brechas: notificación, plazos internos, cooperación
- 14.9 Retención y supresión al terminar (borrado/anonimización)
- 14.10 Auditorías / evidencias / certificaciones (si aplica)

(Esto está directamente alineado con el art. 28 RGPD y guías del EDPB).

---

15) Seguridad y uso seguro del servicio

- 15.1 Controles de acceso, cifrado (si lo declaras), segregación de entornos
- 15.2 Gestión de vulnerabilidades y "responsible disclosure"
- 15.3 Registro de actividad (audit logs) y conservación
- 15.4 Obligaciones del Cliente (dispositivos, contraseñas, roles)

---

16) Integraciones, terceros y marketplace (si existe)

- 16.1 Servicios de terceros (p. ej., email/SMS, banca, firma, storage)
- 16.2 "Third-party terms": tu responsabilidad vs la de ellos
- 16.3 APIs: límites de uso, rate limits, claves, revocación
- 16.4 Importación/exportación: responsabilidad por el origen de datos

---

17) Firma electrónica y evidencias digitales (si MAGOS firma algo)

- 17.1 Tipo de firma (simple/avanzada/cualificada) y límites
- 17.2 Evidencias: sellado temporal, logs, conservación
- 17.3 Validez y reconocimiento (eIDAS)

---

18) Propiedad intelectual y licencia de uso

- 18.1 Titularidad del software, marca, documentación
- 18.2 Licencia al Cliente: no exclusiva, revocable, limitada
- 18.3 Restricciones: ingeniería inversa, scraping, redistribución
- 18.4 Feedback del Cliente (cesión/licencia del feedback)
- 18.5 Componentes open-source (si procede) y sus licencias

---

19) Uso aceptable y prohibiciones

- 19.1 Prohibición de uso ilícito, fraude, suplantación, malware
- 19.2 Abuso de recursos, minería, stress testing sin permiso
- 19.3 Contenido prohibido (p. ej., categorías de datos especiales sin base legal, etc.)
- 19.4 Medidas ante incumplimiento (suspensión, bloqueo, reporte)

---

20) Suspensión y terminación por incumplimiento

- 20.1 Suspensión temporal (seguridad, impago, abuso)
- 20.2 Terminación por causa
- 20.3 Efectos: acceso, exportación, borrado, continuidad mínima

---

21) Duración, renovación, cancelación y "exit plan"

- 21.1 Duración (mensual/anual), renovación automática o no
- 21.2 Cancelación y fechas de efecto
- 21.3 **Portabilidad**: exportación de datos (formatos), plazo de disponibilidad tras baja
- 21.4 Borrado definitivo: plazos y excepciones (obligación legal/defensa jurídica)

---

22) Garantías, "as-is", y disclaimers específicos del sector

- 22.1 No garantía de adecuación a una finalidad (salvo lo pactado)
- 22.2 Disclaimer "no asesoramiento fiscal/contable/legal"
- 22.3 Responsabilidad del Cliente de revisar y validar resultados
- 22.4 Compatibilidad con normativa contable/fiscal: alcance real de MAGOS

---

23) Limitación de responsabilidad

- 23.1 Exclusión de daños indirectos (lucro cesante, pérdida de negocio)
- 23.2 Límite/cap (p. ej., cuotas pagadas últimos X meses)
- 23.3 Excepciones (dolo, etc.) según lo permita la ley
- 23.4 Responsabilidad por terceros/integraciones

---

24) Indemnización (“hold harmless”)

- 24.1 Indemnización del Cliente por uso ilícito, infracción de derechos, datos aportados
- 24.2 Indemnización del proveedor por infracción IP (si te ves capaz de asumirla)
- 24.3 Procedimiento: notificación, control de defensa, cooperación

---

25) Cumplimiento normativo y cooperación con autoridades

- 25.1 Requerimientos legales: cómo se gestiona una orden/mandato
- 25.2 Trazabilidad y evidencias (logs)
- 25.3 Prevención de fraude/abuso (sin prometer de más)

---

26) Fuerza mayor

Eventos fuera de control (cloud providers, cortes, desastres, etc.) y efectos.

---

27) Notificaciones y comunicaciones

- 27.1 Medios válidos (email, panel, etc.)
- 27.2 Efectos de la notificación (plazos)
- 27.3 Preferencias de comunicaciones comerciales (si aplica)

---

28) Cesión del contrato y subcontratación

- 28.1 Cesión por parte del Cliente
- 28.2 Cesión por parte del proveedor (M&A)
- 28.3 Subcontratación técnica vs subencargados (conexión con DPA)

---

29) Resolución de conflictos, ley aplicable y jurisdicción

- 29.1 Ley aplicable (España)
- 29.2 Juzgados competentes (normalmente Madrid)
- 29.3 Mecanismos alternativos (mediación/arbitraje) si quieres
- 29.4 Si hay consumidores: cláusula de adaptación obligatoria

---

30) Miscelánea contractual

- 30.1 Integridad del acuerdo y prevalencia de anexos / order forms
- 30.2 Modificación de TyC (preaviso, aceptación)
- 30.3 Nulidad parcial (severability)
- 30.4 No renuncia
- 30.5 Idioma y versión prevalente
- 30.6 Prueba de aceptación (logs) — sin pasarse, pero útil

Nota práctica

Para “blindarlo” de verdad, el **DPA (art. 28 RGPD)** y el **Anexo de Seguridad (art. 32)** deberían estar **muy desarrollados**, aunque el “cuerpo” de TyC solo los referencie.

0.

---

1. Identificación del prestador y alcance legal del sitio

1.1 Titularidad del sitio y condición de prestador

1.1.1 Titularidad y responsable del servicio

El presente sitio web y el servicio/software **MAGOS** (en adelante, el "Servicio") son titularidad de **Servimac Informarica S.L.** (en adelante, el "Prestador" o "Servimac"), que actúa como proveedor del Servicio ofrecido a través de Internet.

1.1.2 Condición de prestador de servicios de la sociedad de la información

Servimac tiene la condición de **prestador de servicios de la sociedad de la información** y desarrolla su actividad conforme al marco aplicable en España y la Unión Europea, incluyendo las obligaciones de información y transparencia exigibles a este tipo de prestadores.

1.1.3 Acceso a la información legal

Servimac pone a disposición de los usuarios/destinatarios del Servicio la información identificativa y de contacto exigible **por medios electrónicos**, de forma **permanente, fácil, directa y gratuita**, mediante su publicación en el apartado/ubicación correspondiente (p. ej., "Aviso legal", "Términos y condiciones" o equivalente) dentro del Sitio.

1.2 Datos identificativos del Prestador

De conformidad con las obligaciones de información general, los datos identificativos del Prestador son:

- **Razón social:** Servimac Informarica S.L.
- **CIF:** B86575552
- **Domicilio:** C/ Francisco Lozano 3, Primero Derecha
- **Código postal:** 28008
- **Ciudad / País:** Madrid, España

Asimismo, a efectos de contacto directo y efectivo, el Prestador facilitará y mantendrá operativo, al menos, un **correo electrónico** y un medio adicional de contacto (por ejemplo, teléfono), que se indicarán en el Sitio/Servicio:

- **Correo electrónico:** POR COMPLETAR
- **Teléfono u otro medio adicional:** POR COMPLETAR

Datos registrales (si aplica): POR COMPLETAR — Registro Mercantil u otro registro público, tomo/folio/hoja, inscripción.

1.3 Canales de contacto por tipo de asunto

Con el fin de facilitar una comunicación directa y efectiva, y de canalizar adecuadamente las solicitudes, Servimac habilita (o habilitará) los siguientes canales, que podrán figurar en el Sitio y/o en el panel del Servicio:

- **Soporte técnico (incidencias, funcionamiento, errores):** EMAIL SOPORTE / FORMULARIO
- **Consultas comerciales y facturación (planes, cobros, facturas):** EMAIL COMERCIAL/FACTURACIÓN
- **Comunicaciones legales (notificaciones formales):** EMAIL LEGAL / DIRECCIÓN POSTAL
- **Privacidad y protección de datos (derechos, cuestiones RGPD):** EMAIL PRIVACIDAD / DPO SI EXISTE
- **Seguridad (reporte responsable de vulnerabilidades):** EMAIL SECURITY / PROCEDIMIENTO

En todo caso, los canales anteriores se entienden sin perjuicio de las comunicaciones que puedan realizarse mediante los mecanismos internos del Servicio (por ejemplo, centro de ayuda, tickets o avisos en el panel).

1.4 Delimitación del Sitio y del Servicio

1.4.1 Dominio y espacios incluidos

El Sitio y el Servicio se prestan, principalmente, a través del dominio **magos-sif.com** (en adelante, el "Dominio"), incluyendo (si se habilitan) sus **subdominios** y rutas asociadas a:

- la **web pública** (información general),
- el **acceso/área privada** para clientes y usuarios autorizados,
- y cualquier entorno funcional relacionado (p. ej., documentación, estado del servicio, portal de soporte), cuando esté bajo control del Prestador.

1.4.2 Componentes del Servicio

El Servicio puede comprender, entre otros componentes:

- aplicación web (SaaS),
- funcionalidades de administración/cuentas,
- APIs y/o integraciones (si se ofrecen),
- y herramientas auxiliares necesarias para la prestación del Servicio.

1.4.3 Exclusiones

Quedan excluidos del ámbito del "Sitio/Servicio" (salvo que se indique expresamente lo contrario):

- páginas o servicios de **terceros** enlazados desde el Sitio,
- herramientas externas no controladas por Servimac,
- y condiciones/servicios contratados directamente por el usuario con terceros.

1.4.4 Proveedor de infraestructura (información técnica)

A efectos informativos, el Dominio/infraestructura se apoya en un proveedor de servicios de hosting:

- **Proveedor:** IONOS
- **Servidor (SO):** Ubuntu

La información técnica anterior tiene carácter descriptivo y podrá variar por necesidades operativas, de seguridad, mantenimiento o evolución del Servicio, sin alterar la titularidad del Servicio ni las obligaciones asumidas por el Prestador frente al Cliente/Usuario en los presentes términos.

Si quieres, el siguiente paso natural es que me pases **(1)** el **email de contacto legal** que usaréis sí o sí y **(2)** los **datos registrales** (si la SL está inscrita, que casi seguro), y te dejo el **1.2** completamente cerrado sin placeholders.

Claro — aquí tienes el **desarrollo redactado** de los puntos **1.5 a 1.9**, con el mismo estilo contractual que el 1.1–1.4 y manteniendo un enfoque **B2B/SaaS** "blindado" (sin entrar todavía en jurisdicción/foro, que irá más adelante).

1.5 Delimitación de destinatarios (alcance subjetivo)

1.5.1 Destinatarios del Servicio y uso en nombre de una entidad

El Servicio MAGOS está dirigido, con carácter general, a **empresas, profesionales y autónomos** que requieran herramientas de facturación, gestión y contabilidad, así como a las personas físicas que actúen **por cuenta y/o en representación** de dichas entidades (en adelante, el "Cliente").

Cuando un usuario utilice el Servicio **en nombre de una entidad**, se entenderá que dicha entidad es el Cliente y titular de la relación contractual, y que el usuario actúa como persona autorizada por el Cliente.

1.5.2 Declaración de capacidad y facultades de representación

La persona que acepta los presentes Términos y/o contrata el Servicio declara y garantiza que:

a) tiene **capacidad legal suficiente** para obligarse; y/o

b) si actúa en representación de una empresa o tercero, dispone de las **facultades necesarias** para vincular al Cliente, así como para gestionar usuarios y permisos dentro del Servicio.

El Prestador podrá requerir, en caso de duda razonable o por motivos de seguridad y cumplimiento, evidencia de dichas facultades.

1.5.3 Roles de cuenta (definiciones)

A efectos meramente definitorios, dentro de MAGOS podrán existir los siguientes perfiles o roles (sin perjuicio de otros que pudieran habilitarse):

- **Administrador del Cliente / Administrador de Empresa:** usuario con capacidad de alta, gestión y baja de usuarios, configuración básica de la cuenta del Cliente y asignación de permisos.
- **Usuario Autorizado:** usuario creado o autorizado por el Cliente (o su Administrador) para acceder y utilizar el Servicio dentro del alcance de permisos concedidos.
- **Colaborador / Invitado (si se habilita):** usuario con acceso limitado a determinadas áreas o funciones concretas, conforme a lo establecido por el Cliente.

  En todo caso, el Cliente será responsable de que los accesos y permisos asignados se correspondan con su organización y necesidades, y de que se limiten a personal debidamente autorizado.

1.6 Naturaleza jurídica de la información del sitio

1.6.1 Documentos legales y alcance de cada uno

La información y documentación publicada en el Sitio/Servicio puede estructurarse en distintos documentos con finalidad y alcance propio:

- **Aviso Legal:** identifica al Prestador, el Sitio y la información general exigible; regula aspectos básicos de uso del sitio web (p. ej., enlaces, responsabilidad por contenidos externos, etc.).
- **Términos y Condiciones / Términos del Servicio (TyC):** regulan la relación contractual de acceso y uso del Servicio (alta, planes, uso permitido, responsabilidad, suspensión/terminación, etc.).
- **Política de Privacidad:** describe el tratamiento de datos personales para finalidades propias del Prestador (p. ej., web, atención de solicitudes, usuarios, comunicaciones, etc.), así como derechos y canales de ejercicio.

- **Política de Cookies (si aplica):** informa sobre el uso de cookies o tecnologías similares y sus finalidades, configuraciones y opciones.
- **Acuerdo de Tratamiento de Datos (DPA / Encargo de Tratamiento):** regula, cuando proceda, el tratamiento de datos personales por cuenta del Cliente, con el contenido mínimo exigible para la relación Responsable–Encargado.
- **SLA / Condiciones de Soporte y Mantenimiento:** fija, cuando aplique, niveles de servicio, soporte, disponibilidad objetivo, ventanas de mantenimiento y compromisos operativos.

1.6.2 Regla básica de jerarquía y prevalencia documental

Salvo que se indique expresamente lo contrario, y a efectos de interpretación, la documentación aplicable se ordenará conforme al siguiente criterio general de prevalencia:

1. **Condiciones particulares**, pedidos, propuestas aceptadas u "order forms" (si existen) y sus anexos específicos;
2. **Anexos operativos y de cumplimiento** (incluyendo, en su caso, DPA y SLA);
3. **Términos y Condiciones del Servicio (TyC)**;
4. **Políticas informativas** (Privacidad, Cookies) y otros avisos del Sitio, en lo que resulte aplicable.

   En caso de contradicción, prevalecerá el documento de rango superior para la materia concreta afectada.

1.7 Alcance territorial y marco normativo aplicable

1.7.1 Territorio de oferta del Servicio

El Servicio se ofrece principalmente a Clientes **establecidos en España y, en general, en el Espacio Económico Europeo (EEE)**. No obstante, el Sitio/Servicio puede ser accesible desde otros países; en tal caso, el acceso se realizará por iniciativa del usuario/Cliente y bajo su responsabilidad respecto del cumplimiento de la normativa local que, en su caso, resulte aplicable.

1.7.2 Marco general aplicable (sin perjuicio de lo que se indique en otros apartados)

Sin entrar todavía en determinaciones de jurisdicción o fuero, el Prestador opera desde España y, con carácter general, el Servicio se enmarca en la normativa española y europea aplicable a los servicios de la sociedad de la información y a la contratación electrónica, así como en la normativa de protección de datos cuando corresponda.

1.7.3 Restricciones geográficas y cumplimiento (opcional/precautorio)

El Prestador se reserva el derecho a **limitar, suspender o denegar** el acceso al Sitio/Servicio en aquellos territorios o a aquellos usuarios para los que:

a) existan restricciones legales aplicables (incluidas, en su caso, medidas restrictivas/sanciones); o

b) no sea posible garantizar el cumplimiento normativo o la prestación segura del Servicio.

Cualquier limitación de este tipo se aplicará con criterios razonables de seguridad, cumplimiento y gestión de riesgos.

1.8 Idioma, versiones y vigencia del documento

1.8.1 Idioma(s) disponible(s)

Los presentes TyC se publican en **español**. El Prestador podrá ofrecer versiones en otros idiomas (por ejemplo, inglés) con fines informativos o de conveniencia comercial.

1.8.2 Versión vigente, última actualización y entrada en vigor

En el encabezado o pie del documento se indicará:

- **Versión:** vX.Y
- **Fecha de última actualización:** DD/MM/AAAA
- **Fecha de entrada en vigor:** DD/MM/AAAA

  La versión vigente será la publicada en el Sitio/Servicio en cada momento, sin perjuicio de lo establecido para comunicaciones de cambios en apartados posteriores.

1.8.3 Prevalencia entre idiomas

En caso de discrepancia entre distintas versiones lingüísticas, **prevalecerá la versión en español**, salvo que una normativa imperativa aplicable establezca lo contrario o se acuerde expresamente con el Cliente.

1.9 Reserva de exactitud y actualización de datos identificativos

1.9.1 Mantenimiento y actualización de datos

El Prestador manifiesta su compromiso de mantener actualizados los datos identificativos y de contacto publicados en el Sitio/Servicio, realizando las correcciones necesarias cuando se produzcan cambios relevantes.

1.9.2 Comunicación de cambios no materiales

Los cambios **no materiales** (por ejemplo, ajustes menores de datos de contacto o actualización de información administrativa) podrán comunicarse mediante su **actualización en el propio Sitio/Servicio** y/o en los apartados legales correspondientes.

Cuando proceda, el Prestador podrá además informar de cambios mediante avisos en el panel del Servicio o comunicaciones electrónicas, especialmente si afectan a la forma de contacto o al soporte.

Si quieres, el siguiente bloque que suele "atar" todo muy bien es **1.6.2** + el **2 (Definiciones)** para fijar desde ya términos como *"Cliente", "Usuario Autorizado", "Datos del Cliente", "Contenido", "Cuenta", "Subencargado"*; eso reduce muchísimo la ambigüedad y luego hace más fácil blindar limitaciones de responsabilidad y DPA.

2.

Perfecto. Con las apps que me indicas, aquí tienes el **desarrollo redactado** de los puntos **3.1 a 3.6** (en estilo contractual, "blindado" y con **referencias normativas solo donde aportan valor**).

3.1 Objeto y naturaleza del Servicio

3.1.1 Objeto

MAGOS es un software de gestión empresarial en modalidad **servicio digital** (SaaS), accesible por vía electrónica, destinado a facilitar —entre otras— tareas de **facturación, registro y control de ingresos y gastos, gestión de terceros, gestión interna, elaboración/consulta de información contable, fiscal y de tesorería**, así como la visualización de paneles de control (en adelante, el "Servicio").

3.1.2 Naturaleza y forma de prestación

El Servicio se presta **a distancia, por vía electrónica y a petición individual del usuario**, mediante acceso a una aplicación web (y, en su caso, otros componentes técnicos asociados), encajando en el marco general de los **servicios de la sociedad de la información** y la contratación por medios electrónicos.

3.1.3 Finalidad funcional

El Servicio proporciona herramientas para **registrar, organizar, consultar y exportar** información y documentación de gestión (incluida la económica/administrativa), con el fin de apoyar los procesos internos del Cliente y su toma de decisiones.

3.2 Componentes, apps existentes y alcance funcional

3.2.1 Estructura por aplicaciones/módulos

El Servicio se articula en aplicaciones o módulos, que podrán activarse o estar disponibles según el plan, configuración o evolución del producto. A la fecha, el Servicio incluye (o contempla incluir) aplicaciones como las siguientes:

- **Ingresos**
- **Gastos**
- **Clientes**
- **Proveedores**
- **Productos**
- **Empleados**
- **Fiscalidad**
- **Libro contable**
- **Paneles de control**
- **Caja**
- **Usuarios**
- **Diseño**

3.2.2 Funcionalidades “núcleo” (alto nivel)

Sin perjuicio del detalle funcional que figure en la documentación, el Servicio puede incluir, a nivel general: (i) creación/gestión/consulta de registros; (ii) parametrización y organización de información; (iii) generación de documentos y reportes; (iv) exportación/importación en formatos soportados; (v) herramientas de control interno y visualización de métricas mediante paneles.

3.2.3 Evolución del catálogo funcional

El Prestador podrá **modificar, ampliar o reorganizar** módulos, pantallas o flujos de uso como parte del ciclo de vida del software, conforme a lo previsto en los apartados de cambios y actualizaciones del Servicio (y, en su caso, el SLA), manteniendo el carácter de herramienta digital de gestión descrito en esta cláusula.

3.3 Qué incluye y qué no incluye el Servicio

3.3.1 Incluye

El Servicio incluye, con carácter general:

a) el **acceso** a la plataforma y a las funcionalidades disponibles en el plan contratado;

b) la **puesta a disposición** de herramientas de gestión vinculadas a las apps descritas;

c) la **documentación** o recursos de ayuda que el Prestador publique para el uso ordinario del Servicio.

3.3.2 Exclusiones: ausencia de asesoramiento profesional

Salvo pacto expreso en condiciones particulares, el Servicio:

a) **no constituye** un servicio de asesoramiento **legal, fiscal, contable o laboral**;

b) **no sustituye** la intervención de profesionales cualificados ni la obligación del Cliente de revisar y validar su operativa y obligaciones;

c) **no garantiza** por sí mismo la adecuación del Cliente a requisitos concretos que dependan de su actividad, jurisdicción, régimen fiscal, organización o casuística.

En particular, las áreas o apps denominadas "**Fiscalidad**", "**Libro contable**" o equivalentes se entienden como **herramientas de soporte y organización de información**, sin que ello implique que el Prestador asuma la posición de asesor del Cliente ni emita dictámenes.

3.3.3 Dependencias y responsabilidades del Cliente

El Cliente es responsable de: (i) la **licitud, exactitud y actualización** de los datos que introduzca; (ii) la correcta **configuración** de parámetros conforme a su operativa; (iii) la adecuada **custodia** de credenciales y la gestión de usuarios/permisos; y (iv) el cumplimiento de obligaciones que le resulten aplicables en su actividad (incluidas las de naturaleza fiscal/contable/laboral cuando proceda).

3.4 Características esenciales y parámetros del Servicio

3.4.1 Acceso y disponibilidad general

El Servicio se ofrece mediante acceso electrónico. La disponibilidad podrá estar sujeta a:

a) operaciones de mantenimiento planificado;

b) incidencias técnicas;

c) actuaciones necesarias por razones de seguridad; o

d) causas fuera del control razonable del Prestador (p. ej., fallos de red o de terceros).

3.4.2 Límites funcionales/técnicos

El Servicio puede incluir límites asociados al plan contratado o al uso razonable de recursos (por ejemplo, número de usuarios, empresas, volumen de registros/documentos, almacenamiento, etc.), que se detallarán en las condiciones comerciales o en la documentación aplicable.

3.4.3 Interoperabilidad y compatibilidad (principio general)

Cuando el Servicio ofrezca importaciones/exportaciones o integraciones, estas se limitarán a los **formatos y métodos** soportados en cada momento. El Prestador podrá actualizar dichos formatos/métodos por motivos técnicos, de seguridad o de evolución del producto.

3.4.4 Nota de conformidad en caso de contratación con consumidores (si aplicara en el futuro)

Si en algún supuesto el Servicio fuese comercializado a **consumidores**, podrían resultar aplicables reglas específicas de **conformidad y actualizaciones** previstas para servicios digitales en el marco de la UE; en tal caso, se incorporarán o adaptarán las condiciones necesarias.

3.5 Prestación técnica e infraestructura

3.5.1 Prestación técnica

El Prestador proporciona el entorno técnico necesario para el acceso y uso del Servicio, incluyendo los componentes de aplicación y los recursos de infraestructura necesarios para su operación.

3.5.2 Terceros de infraestructura y cambios operativos

El Servicio puede apoyarse en proveedores de infraestructura (hosting, conectividad, etc.). El Prestador podrá **cambiar** proveedores, arquitecturas o configuraciones por razones de mantenimiento, rendimiento, continuidad del negocio o seguridad, sin que ello afecte a la titularidad del Servicio ni a las obligaciones asumidas frente al Cliente, siempre que se mantenga una prestación funcional equivalente.

3.5.3 Mantenimiento

El Prestador podrá realizar **mantenimientos correctivos y evolutivos**. Las ventanas de mantenimiento, si se formalizan, se describirán en el **SLA/Anexo** o en comunicaciones operativas.

3.6 Requisitos técnicos del Cliente/Usuario

3.6.1 Requisitos mínimos

Para utilizar el Servicio, el Usuario deberá disponer, al menos, de:

a) un dispositivo compatible (ordenador o equivalente);

b) un navegador actualizado y configurado conforme a estándares habituales;

c) conectividad a Internet suficiente para operar con normalidad.

3.6.2 Responsabilidad del Cliente sobre su entorno

El Cliente/Usuario es responsable de su propio entorno técnico (dispositivos, red, seguridad del endpoint, antivirus, políticas internas, configuración de firewall/proxy, etc.). El Prestador no será responsable de interrupciones o limitaciones derivadas del entorno del Cliente o de terceros ajenos al Prestador.

3.6.3 Uso conforme a seguridad y cumplimiento

El Cliente se compromete a utilizar el Servicio de forma diligente y conforme a prácticas razonables de seguridad, incluyendo el uso de credenciales robustas y la gestión adecuada de usuarios y permisos, sin perjuicio de lo previsto en las cláusulas de seguridad y uso aceptable.

Si quieres, el siguiente paso es que yo redacte **3.7 (onboarding/importación)** y **3.8 (actualizaciones/cambios)**, que son los dos apartados que más "protegen" frente a reclamaciones por migraciones fallidas y por cambios de producto.

3. Descripción del Servicio (continuación)

3.7 Alta, puesta en marcha y configuración inicial

3.7.1 Onboarding estándar (alta y configuración básica)

El acceso al Servicio se realiza, con carácter general, mediante un proceso de **alta/registro** y creación de cuenta (o cuentas) que habilita el uso del Servicio por parte del Cliente y sus Usuarios Autorizados. Dicho onboarding estándar puede incluir, según el plan o la configuración disponible en cada momento:

a) creación de la **cuenta del Cliente** y definición de parámetros básicos (p. ej., datos de la entidad, preferencias generales);

b) habilitación de **usuarios** y asignación de roles/permisos conforme al modelo de control de accesos del Servicio; y

c) aceptación de los presentes TyC y, cuando proceda, de anexos aplicables (por ejemplo, el **DPA/Encargo de Tratamiento**).

3.7.2 Importación de datos (condiciones, límites y responsabilidad)

Cuando el Servicio permita importar información (por ejemplo, listados de clientes/proveedores, productos, empleados, registros de ingresos/gastos, asientos o datos equivalentes), se aplicarán las siguientes reglas generales:

a) **Formatos y canales**: las importaciones estarán limitadas a los **formatos**, plantillas y métodos habilitados en cada momento (p. ej., CSV/Excel u otros), conforme a la documentación vigente.

b) **Validaciones**: el Servicio podrá aplicar **validaciones automáticas** (estructura, campos obligatorios, coherencia mínima) y rechazar parcial o totalmente importaciones que no cumplan los requisitos publicados o que puedan comprometer la integridad del sistema.

c) **Límites**: podrán existir límites técnicos o de plan (volumen, tamaño de archivo, número de registros, tasa de importación, etc.).

d) **Responsabilidad del Cliente**: el Cliente es responsable de (i) la **licitud** del origen de los datos; (ii) la **exactitud, integridad y actualización** del contenido importado; (iii) la configuración previa necesaria; y (iv) la revisión posterior de resultados.

e) **No garantía de migración "perfecta"**: salvo pacto expreso en condiciones particulares, la importación se proporciona como herramienta de soporte y no constituye un servicio profesional de migración con resultado garantizado.

Cuando las importaciones incluyan **datos personales**, el Cliente declara disponer de base jurídica y legitimación suficiente para tratarlos e introducirlos en el Servicio, quedando el tratamiento por cuenta del Cliente regulado, cuando proceda, por el **DPA** conforme al art. 28 del RGPD.

3.7.3 Servicios profesionales (si se ofrecen)

Si el Prestador ofreciera servicios profesionales (p. ej., consultoría, parametrización avanzada, migración asistida, formación personalizada, desarrollo a medida o acompañamiento de implantación), dichos servicios:

a) tendrán **alcance, plazos y precio** definidos en condiciones particulares, propuesta u orden de pedido;

b) podrán incluir **exclusiones** y supuestos no cubiertos (p. ej., limpieza de datos, corrección de inconsistencias del origen, adaptaciones específicas del modelo contable/fiscal del Cliente); y

c) se prestarán de forma **independiente** del acceso estándar al Servicio, sin alterar la naturaleza SaaS del mismo, salvo pacto expreso.

3.8 Actualizaciones, cambios y evolución del Servicio

3.8.1 Mejoras y actualizaciones (funcionales y de seguridad)

El Cliente reconoce que el Servicio es un producto software en evolución y que el Prestador podrá desplegar **actualizaciones** (incluyendo parches, mejoras de rendimiento, correcciones de errores y actualizaciones de seguridad) como parte del ciclo de vida normal del SaaS. Estas actualizaciones pueden afectar a módulos existentes (p. ej., Ingresos, Gastos, Fiscalidad, Libro contable, Paneles de control, Caja, Usuarios, Diseño) o introducir nuevas capacidades.

3.8.2 Cambios no materiales vs cambios materiales (definición y tratamiento)

A efectos interpretativos:

a) se considerarán **cambios no materiales** aquellos que no alteren de forma sustancial la esencia del Servicio contratado ni reduzcan significativamente sus funcionalidades principales para el uso ordinario (p. ej., ajustes de interfaz, reorganización de menús, mejoras de rendimiento, refuerzos de seguridad).

b) se considerarán **cambios materiales** aquellos que, razonablemente, puedan (i) suprimir o degradar de forma significativa una funcionalidad esencial del plan contratado; (ii) modificar de forma sustancial flujos críticos del Servicio; o (iii) afectar de forma relevante a integraciones/API esenciales para el Cliente.

El régimen de **comunicación, plazos y medidas** asociado a cambios materiales podrá desarrollarse en la cláusula específica de “Cambios del Servicio” y/o en el SLA, si existiera.

3.8.3 Deprecación de funcionalidades, API e integraciones

El Prestador podrá **deprecar** (marcar para retirada) funcionalidades, endpoints de API o integraciones por motivos técnicos, de seguridad, obsolescencia, sustitución por alternativas o decisiones de producto. Con carácter general:

a) se procurará ofrecer, cuando sea razonable, **alternativas funcionales** o rutas de migración;

b) la retirada definitiva podrá ir precedida de avisos en documentación, changelog, panel del Servicio u otros canales operativos; y

c) la continuidad de integraciones de terceros dependerá, en parte, de la disponibilidad y estabilidad de dichos terceros.

3.8.4 Nota para supuestos B2C (servicios digitales)

Si el Servicio fuese comercializado en algún supuesto a **consumidores**, podrían resultar aplicables obligaciones específicas sobre **conformidad y suministro de actualizaciones**, en el marco de la Directiva (UE) 2019/770 y su transposición nacional. En tal caso, el Prestador ajustará las condiciones aplicables a dichos contratos para reflejar los derechos y obligaciones imperativos correspondientes.

3.9 Documentación, guías y recursos

3.9.1 Documentación técnica/funcional (base de conocimiento)

El Prestador podrá poner a disposición del Cliente documentación técnica y/o funcional (manuales, guías, FAQs, artículos de soporte, notas de versión, etc.) para facilitar el uso del Servicio. Salvo que se indique expresamente lo contrario, dicha documentación tiene carácter **informativo** y puede actualizarse conforme evolucione el Servicio.

3.9.2 Materiales de ayuda y comunicaciones operativas

El Prestador podrá publicar o facilitar, por medios electrónicos, comunicaciones operativas tales como:

a) changelog/notas de versión;

b) avisos de mantenimiento;

c) estado del servicio (status page) y comunicaciones de incidentes; y/o

d) recomendaciones de seguridad o buenas prácticas.

Estas comunicaciones podrán formar parte de la operativa ordinaria del Servicio y servir como canal de transparencia y soporte.

3.9.3 Idioma de la documentación y prevalencia

La documentación podrá publicarse en uno o varios idiomas. En caso de discrepancia entre versiones lingüísticas, prevalecerá la versión que el Prestador indique como principal para el Servicio (habitualmente, español), salvo pacto expreso o exigencia normativa imperativa aplicable.

3.10 Integraciones y servicios de terceros

3.10.1 Integraciones disponibles (categorías)

El Servicio podrá incorporar integraciones con servicios de terceros, tales como (a título enunciativo): **banca/fintech**, **facturación electrónica**, **correo y mensajería**, **firma electrónica**, **almacenamiento**, **analítica**, u otros conectores que el Prestador habilite en cada momento.

3.10.2 Responsabilidad por terceros y condiciones aplicables

Las integraciones con terceros pueden requerir que el Cliente mantenga una relación contractual directa con el tercero (cuenta, licencias, claves, pagos, etc.). El Cliente reconoce que:

a) el tercero presta su servicio **bajo sus propios términos y políticas**, y puede modificarlo o interrumpirlo;

b) el Prestador no controla el rendimiento, disponibilidad, seguridad o legalidad del servicio de terceros, más allá de la integración técnica que facilite; y

c) los fallos o cambios del tercero pueden afectar al funcionamiento de la integración, sin que ello suponga incumplimiento del Prestador, salvo que se pacte expresamente lo contrario en condiciones particulares.

3.10.3 Reglas básicas de API (si existe)

Si el Servicio ofrece API u otros mecanismos de integración, el uso de los mismos podrá quedar sujeto a:

a) autenticación mediante credenciales/tokens y obligación de custodia por parte del Cliente;

b) límites de uso (rate limits), cuotas y políticas antiabuso;

c) medidas de seguridad (rotación/revocación de credenciales, restricciones por IP u otras); y

d) posibilidad de **suspensión o revocación** del acceso a la API por razones de seguridad, abuso, riesgo o incumplimiento de los TyC/AUP, sin perjuicio de las obligaciones legales aplicables.

3.11 Datos tratados por el Servicio (mención estructural)

3.11.1 Tipos generales de datos

En el curso de la prestación del Servicio, el Cliente podrá introducir y gestionar información que típicamente puede incluir:

a) datos identificativos y de contacto de **clientes** y **proveedores**;

b) datos de **empleados** (según uso del Cliente);

c) datos económicos y administrativos asociados a **ingresos**, **gastos**, **productos**, **tesorería/caja**, **libros/registros contables**, y documentación relacionada;

d) datos de acceso y uso del Servicio (usuarios, roles, registros de actividad), en la medida necesaria para la operación, soporte y seguridad.

3.11.2 Remisión al DPA / Encargo de Tratamiento (art. 28 RGPD)

Cuando el Servicio implique el tratamiento de **datos personales por cuenta del Cliente**, las partes formalizarán (o se entenderá formalizado mediante aceptación) el

correspondiente **Acuerdo de Tratamiento de Datos (DPA/Encargo de Tratamiento)**, con el contenido mínimo exigible y conforme a lo previsto en el **artículo 28 del Reglamento (UE) 2016/679 (RGPD)**, incluyendo (entre otros) objeto, duración, naturaleza y finalidad del tratamiento, categorías de datos e interesados, instrucciones del Cliente, subencargados, medidas de seguridad y asistencia.

3.12 Versiones, pruebas, beta y funcionalidades experimentales

3.12.1 Versiones beta/preview (si existen)

El Prestador podrá ofrecer, de forma opcional, funcionalidades en estado **beta**, "preview" o experimental, con el fin de probar capacidades nuevas o recopilar feedback. Estas funcionalidades podrán estar sujetas a condiciones específicas (p. ej., acceso limitado, invitación, activación manual) y podrán no estar disponibles en todos los planes.

3.12.2 Inestabilidad, cambios o retirada (sin SLA)

Las funcionalidades beta/experimentales:

a) pueden presentar errores, inestabilidad o limitaciones;

b) pueden modificarse sustancialmente, renombrarse o retirarse; y

c) podrán quedar excluidas de compromisos de disponibilidad/soporte (SLA) salvo pacto expreso.

3.12.3 Feedback y trazabilidad de incidencias

El Cliente podrá remitir feedback, incidencias o sugerencias por los canales habilitados. El Prestador podrá utilizar dicho feedback para mejorar el Servicio y gestionar la evolución del producto. La trazabilidad de incidencias, tiempos de respuesta y niveles de soporte —cuando se formalicen— se desarrollarán en el SLA o en el anexo de soporte aplicable.

Si quieres, el siguiente bloque que conviene atacar (por impacto "defensivo") es el **4 (Elegibilidad/roles/responsabilidades)** o directamente el **10 (SLA/soporte)**, porque es donde se atan expectativas de disponibilidad y respuesta.

4. Elegibilidad, tipo de cliente y rol del usuario

4.1 Naturaleza del cliente objetivo y modalidad de contratación

4.1.1 Contratación profesional (B2B) por defecto

El Servicio MAGOS está concebido y ofertado, con carácter general, para su utilización por **empresas, profesionales y autónomos** en el marco de su actividad económica o profesional (en adelante, el "Cliente"). En consecuencia, salvo que se indique expresamente lo contrario en condiciones particulares, la contratación y el uso del Servicio se entienden realizados en un **contexto B2B**, con las implicaciones propias de dicha naturaleza contractual.

4.1.2 Uso "en nombre de una entidad"

Cuando una persona física (usuario) acceda, utilice o contrate el Servicio **en nombre de una entidad** (sociedad, autónomo, comunidad, asociación u otra organización), se entenderá que:

a) la entidad es el **Cliente** y titular de la relación contractual;

b) el usuario actúa como **persona autorizada** por el Cliente; y

c) los actos realizados mediante su cuenta (incluida la aceptación de condiciones, alta de usuarios, configuración de permisos, cargas de datos y operaciones) se imputarán al Cliente, sin perjuicio de lo previsto sobre suplantación o acceso no autorizado.

4.1.3 Supuesto excepcional de consumidor (carve-out)

Si, de manera excepcional, el Servicio fuese contratado o utilizado por una persona física **ajena a cualquier actividad empresarial o profesional** (consumidor/usuario), se

aplicarán las **normas imperativas de protección de consumidores** que resulten de obligado cumplimiento y, en su caso, las condiciones específicas B2C que el Prestador pudiera habilitar para dicho canal. En particular, en contratos con consumidores podrían ser aplicables reglas especiales en materia de información precontractual, conformidad/garantías de servicios digitales y actualizaciones.

4.2 Capacidad legal, edad mínima y restricciones de acceso

(Se desarrollará en su subcláusula específica del punto 4; no se incluye aquí por petición del Cliente.)

4.3 Representación, autoridad interna y garantías del usuario representante

4.3.1 Declaración de autoridad y capacidad para vincular al Cliente

La persona que acepte los presentes TyC y/o complete el proceso de contratación del Servicio declara y garantiza que dispone de **capacidad legal suficiente** y, cuando actúe por cuenta de una entidad, de las **facultades necesarias** para representar y obligar al Cliente, incluyendo la aceptación de condiciones por vía electrónica.

4.3.2 Responsabilidad del Cliente por usuarios y actuaciones autorizadas

El Cliente será responsable de:

a) la designación de las personas que actuarán como usuarios autorizados;

b) las actuaciones realizadas por dichos usuarios dentro del alcance de sus permisos; y

c) la adecuación de la estructura interna de roles/permisos a su organización (principio de control interno).

4.3.3 Facultades de verificación por parte del Prestador

Por motivos de seguridad, prevención del fraude, cumplimiento o gestión de riesgos contractuales, el Prestador podrá solicitar, de forma **razonable y proporcionada**, evidencia de las facultades de representación o autorización del usuario (por ejemplo, cuando se soliciten cambios críticos de titularidad, administración, facturación, accesos o configuraciones sensibles), sin que ello implique una obligación general de verificación previa en todos los casos.

4.4 Identidad, credenciales y control de acceso

4.4.1 Cuenta nominativa y custodia de credenciales

El acceso al Servicio se realizará mediante **cuentas de usuario** y credenciales asociadas. El Cliente y cada usuario se obligan a:

a) mantener la **confidencialidad** de sus credenciales;

b) no compartirlas con terceros ni permitir su uso por personas no autorizadas;

c) utilizar contraseñas robustas y, si el Servicio lo habilita, mecanismos adicionales de seguridad (p. ej., 2FA); y

d) notificar sin dilación cualquier sospecha de acceso indebido o compromiso de credenciales.

El Cliente reconoce que la contratación y la prestación del Servicio se realizan por vía electrónica y que las actuaciones efectuadas desde una cuenta autenticada podrán considerarse realizadas por el Cliente o por su usuario autorizado, salvo prueba de suplantación o fallo imputable al Prestador.

4.4.2 Control de acceso basado en roles y “mínimo privilegio”

El Servicio puede estructurar permisos y accesos mediante un sistema de **roles**. Sin perjuicio del desarrollo completo de roles en su cláusula específica, el Cliente reconoce que MAGOS podrá contemplar perfiles como:

- **Propietario**, **Administrador**, **Contable**, **CRM**, **RRHH**, **Tesorero**, **Auditor** y **Gestoría**.

El Cliente es responsable de asignar roles/permisos conforme al principio de **necesidad de acceso** (mínimo privilegio), evitando conceder privilegios superiores a los necesarios para la función concreta de cada usuario.

4.4.3 Accesos de terceros (p. ej., Gestoría/Auditoría) bajo control del Cliente

Cuando el Cliente habilite accesos a terceros (por ejemplo, **gestorías**, asesores externos o auditores), dichos accesos:

a) deberán ser autorizados expresamente por el Cliente;

b) quedarán sometidos a los presentes TyC y a las políticas aplicables; y

c) se entenderán concedidos bajo la responsabilidad del Cliente en cuanto a su necesidad, alcance y revocación cuando ya no procedan.

4.4.4 Medidas de limitación por seguridad o indicios de abuso

El Prestador podrá aplicar medidas técnicas razonables para proteger la integridad del Servicio (p. ej., bloqueo temporal, limitación de intentos de acceso, revocación de sesiones, restricciones por riesgo) cuando detecte indicios razonables de suplantación, acceso no autorizado, abuso o amenaza de seguridad, sin perjuicio de lo establecido en las cláusulas de suspensión/terminación.

Cuando quieras, sigo con **4.5 (Roles de usuario dentro del Servicio)** y **4.6 (Obligaciones mínimas por tipo de uso)**, ya aterrizando cada rol (Propietario/Administrador/Contable/…/Gestoría) con definiciones contractuales claras.

4.5 Roles de usuario dentro del Servicio

(Definiciones contractuales, sin operativa detallada)

4.5.1 Propietario / Administrador de cuenta / Administrador del Cliente

A efectos de estos TyC, el **Propietario** y/o **Administrador** (según la nomenclatura concreta del Servicio) es el usuario designado por el Cliente con facultades, normalmente, para:

a) gestionar la **configuración general** de la cuenta/entidad (datos básicos, parámetros globales);

b) **dar de alta, modificar o dar de baja** usuarios y accesos;

c) **asignar y revocar** roles/permisos; y

d) ejecutar acciones de administración relevantes (p. ej., habilitación de integraciones, configuración de controles internos, o acciones equivalentes).

El Cliente reconoce que el Propietario/Administrador actúa como **persona de confianza** y que las actuaciones realizadas por dicho rol se imputan al Cliente, salvo acceso no autorizado o suplantación no imputable al Cliente.

4.5.2 Usuario autorizado (roles funcionales)

Se considera **Usuario Autorizado** toda persona física que, bajo autorización del Cliente (normalmente conferida por el Propietario/Administrador), accede al Servicio y opera dentro del alcance de permisos asignados. A título enunciativo, podrán existir roles funcionales como:

- **Contable**, **Tesorero**, **RRHH**, **CRM**, **Auditor**, **Gestoría**, u otros que el Servicio habilite.

  Cada rol funcional se entiende limitado a la finalidad propia de su función interna o profesional, y siempre sujeto a las restricciones y obligaciones de estos TyC.

4.5.3 Colaborador / Invitado (si existe)

Cuando el Servicio lo permita, un **Colaborador** o **Invitado** será un usuario con acceso limitado a áreas o funcionalidades concretas, según autorización del Cliente. Este tipo de usuario podrá estar sujeto a restricciones adicionales (por ejemplo, acceso de solo lectura, acceso temporal, o acceso a un subconjunto de módulos).

4.5.4 Usuario “técnico” (API) (si existe)

Si el Servicio habilita integraciones mediante API, podrá existir un **Usuario Técnico** (identidad no necesariamente asociada a una persona física concreta) para autenticar integraciones o procesos automatizados. En ese caso:

a) el Cliente será responsable de la **custodia** y uso de credenciales/tokens;

b) el uso del Usuario Técnico se limitará a los fines autorizados (integraciones legítimas del Cliente); y

c) el Prestador podrá aplicar límites (rate limits, cuotas, restricciones) y revocar credenciales por razones de seguridad, abuso o riesgo operativo, conforme a estos TyC y a la política de uso aceptable.

4.6 Obligaciones mínimas del usuario/cliente por tipo de uso

4.6.1 Uso profesional diligente

El Cliente y los Usuarios Autorizados se obligan a utilizar el Servicio:

a) de forma **diligente**, conforme a su finalidad y a la documentación aplicable;

b) respetando los roles y permisos asignados; y

c) con sujeción a estos TyC, al SLA (si lo hubiera), y a las políticas aplicables (incluida la Política de Uso Aceptable, si se incorpora como anexo).

4.6.2 Prohibición de usos ilícitos o de riesgo

Queda prohibido utilizar el Servicio para:

a) fines ilícitos, fraudulentos o que vulneren derechos de terceros;

b) introducir, transmitir o almacenar código malicioso, realizar pruebas de intrusión no autorizadas o acciones que comprometan la seguridad;

c) eludir controles técnicos, límites de uso, autenticación o medidas antiabuso;

d) acceder o intentar acceder a datos o cuentas de terceros sin autorización; o

e) cualquier conducta que pueda causar daño, indisponibilidad o degradación significativa del Servicio.

Este apartado "marca perímetro" y se desarrolla con mayor detalle en la cláusula/política de **Uso Aceptable (AUP)**.

4.6.3 Integridad, licitud y legitimación de la información

El Cliente es responsable de que los datos y contenidos que introduzca o gestione en el Servicio:

a) sean **veraces, exactos, completos y estén actualizados** en la medida razonablemente exigible;

b) procedan de fuentes lícitas y no infrinjan derechos de terceros; y

c) cuando incluyan **datos personales**, el Cliente cuente con la **base jurídica** y legitimación necesaria para su tratamiento e incorporación al Servicio, así como para permitir el tratamiento por parte del Prestador cuando actúe como encargado, conforme al DPA y al RGPD.

4.7 Encaje de roles en protección de datos

(Anclaje mínimo; desarrollo completo en el bloque RGPD y en el DPA)

4.7.1 Regla general de roles (Cliente/Prestador)

Con carácter general, cuando el Cliente utilice el Servicio para tratar datos personales en el marco de su actividad, el **Cliente** actuará como **Responsable del tratamiento** y el **Prestador** actuará como **Encargado del tratamiento**, en la medida en que trate datos personales **por cuenta** del Cliente y conforme a sus instrucciones documentadas.

4.7.2 Tratamiento bajo instrucciones y DPA (art. 28 RGPD)

En los supuestos indicados, el tratamiento por parte del Prestador se regirá por el correspondiente **Acuerdo de Tratamiento de Datos (DPA/Encargo de Tratamiento)**,

incorporando el contenido mínimo exigido por el **artículo 28 del RGPD**, incluyendo, entre otros extremos: instrucciones, confidencialidad, medidas técnicas y organizativas, régimen de subencargados, asistencia al Responsable y devolución/supresión al finalizar.

4.8 Medidas ante incumplimiento de elegibilidad o rol

4.8.1 Facultad de suspensión, limitación o denegación de acceso

Si el Prestador detecta indicios razonables de:

a) falta de autoridad del usuario que contrata/acepta;

b) suplantación de identidad o acceso no autorizado;

c) uso del Servicio por personas no autorizadas por el Cliente; o

d) incumplimientos graves del esquema de roles/permisos o de las obligaciones mínimas de uso,

podrá adoptar medidas proporcionadas de **limitación, suspensión o denegación** del acceso (por ejemplo, bloqueo temporal, revocación de sesiones, reseteo de credenciales, o congelación de integraciones), con la finalidad de proteger la seguridad del Servicio, la continuidad operativa y/o la posición contractual de las partes.

4.8.2 Efectos sobre datos y continuidad (remisión)

Los efectos sobre:

a) la disponibilidad de la cuenta;

b) la conservación, exportación y/o supresión de datos; y

c) la continuidad del Servicio o la terminación contractual,

se regirán por las cláusulas específicas de **suspensión/terminación** y por el "**exit plan**" o apartado equivalente, evitando duplicidades interpretativas.

4.8.3 Notificación y canal

Salvo que existan motivos de seguridad que aconsejen una actuación inmediata o discreta (p. ej., suplantación en curso), el Prestador procurará notificar al Cliente la medida adoptada y su motivo general, mediante los canales habituales (panel del Servicio, correo electrónico u otros canales operativos definidos), sin perjuicio de comunicaciones adicionales que resulten necesarias para restablecer accesos o mitigar riesgos.

Cuando quieras, continúo con **4.2** (capacidad/edad mínima/restricciones) y **4.7/4.8** ya enlazándolo con los apartados futuros de **Uso Aceptable**, **Seguridad**, y **Suspensión/Terminación** para que todo quede perfectamente "cosido" sin contradicciones.

5. Registro, cuentas y seguridad de acceso

5.1 Alta, verificación y usuarios autorizados

5.1.1 Registro/alta de cuenta, aceptación de TyC y trazabilidad

El acceso al Servicio requiere, con carácter general, la creación de una **cuenta de Cliente** (y, en su caso, de usuarios asociados) mediante el procedimiento habilitado en el Sitio/Servicio. En el marco de dicho proceso:

a) el Cliente deberá facilitar los **datos mínimos necesarios** para el alta y la correcta prestación del Servicio;

b) deberá **aceptar** los Términos y Condiciones (y, cuando proceda, los anexos aplicables, como el DPA); y

c) el Prestador podrá mantener **evidencias razonables** de la aceptación y del proceso de contratación (p. ej., fecha/hora, versión de los TyC, identificadores técnicos de sesión), a efectos de **prueba** y cumplimiento de obligaciones de contratación por vía electrónica conforme a la Ley 34/2002 (LSSI-CE), en particular en lo relativo a información previa y posterior a la contratación.

5.1.2 Verificación de identidad/cuenta

Con el fin de prevenir altas fraudulentas, accesos no autorizados o suplantaciones, el Prestador podrá aplicar medidas de **verificación** como:

a) **verificación de correo electrónico** (confirmación de dirección mediante enlace/código);

b) verificación adicional de titularidad o vinculación con la entidad (p. ej., verificación de dominio corporativo, comprobaciones de consistencia o mecanismos equivalentes); y/o

c) **verificación reforzada** para acciones consideradas críticas o de alto impacto (por ejemplo, recuperación de cuenta, cambios de Propietario/Administrador, configuración de integraciones, o acciones que afecten significativamente a la seguridad o a la titularidad).

Estas medidas se aplicarán con criterios de proporcionalidad y gestión del riesgo, sin perjuicio de los mecanismos de suspensión preventiva por seguridad previstos en otros apartados.

5.1.3 Alta de usuarios por el Cliente (usuarios autorizados)

El alta de usuarios dentro de la cuenta del Cliente se realizará, por regla general, por el **Propietario/Administrador** u otro rol con privilegios suficientes, quien podrá:

a) invitar o crear **Usuarios Autorizados** y asignarles roles/permisos;

b) revocar accesos o modificar permisos cuando sea necesario (p. ej., cambios organizativos, bajas laborales o cambio de proveedor externo); y

c) establecer la configuración interna de acceso de acuerdo con la estructura del Cliente.

El número de usuarios, roles habilitados o capacidades de gestión podrán estar **limitados por el plan** contratado o por políticas técnicas/operativas del Servicio.

5.1.4 Gestión de accesos de terceros (gestoría/auditor/asesor) bajo control del Cliente

Cuando el Cliente habilite acceso a terceros (por ejemplo, **Gestoría** o **Auditor**), dicho acceso:

a) se otorgará **bajo autorización expresa** del Cliente y dentro del alcance de permisos definido por éste;

b) podrá estar sujeto a restricciones adicionales (p. ej., acceso limitado, solo lectura, acceso temporal); y

c) será responsabilidad del Cliente en lo relativo a (i) la **necesidad** del acceso, (ii) su adecuación a su organización, (iii) la **revocación** cuando deje de ser procedente y (iv) las instrucciones internas y contractuales que el Cliente mantenga con dicho tercero.

Sin perjuicio de lo anterior, el uso de MAGOS por parte de terceros autorizados queda sujeto a los presentes TyC y a las políticas aplicables (incluida la AUP, cuando exista).

5.1.5 Cuenta única y titularidad

La **cuenta** del Servicio se entiende asociada al **Cliente** (la entidad o profesional que contrata) y no a un usuario individual. Los usuarios (incluidos Propietario/Administrador, Contable, Tesorero, RRHH, CRM, Auditor, Gestoría, etc.) actúan como **Usuarios Autorizados** del Cliente, sin adquirir por ello titularidad sobre la cuenta ni sobre los datos del Cliente.

Cualquier actuación realizada desde una cuenta autenticada se entenderá realizada por el Cliente o por su Usuario Autorizado, salvo prueba de suplantación o acceso indebido no imputable al Cliente.

5.2 Gestión de contraseñas, 2FA y políticas de seguridad

5.2.1 Política de contraseñas

El Cliente y los Usuarios Autorizados deberán mantener contraseñas **robustas** y confidenciales. Sin perjuicio de lo que establezca la configuración concreta del Servicio, podrán aplicarse medidas tales como:

a) requisitos mínimos de longitud/complexidad;

b) bloqueo temporal o escalonado tras **intentos fallidos** repetidos;

c) prohibición o limitación de contraseñas débiles o de uso común; y

d) recomendaciones de **no reutilización** de contraseñas y uso de gestores de contraseñas.

Estas prácticas se alinean con recomendaciones públicas de la AEPD sobre creación de contraseñas robustas.

5.2.2 2FA/MFA (si existe): habilitación, obligatoriedad por rol y recuperación

Cuando el Servicio ofrezca autenticación en dos factores o multifactor (**2FA/MFA**), el Prestador podrá:

a) permitir su activación opcional por el Cliente; y/o

b) exigirla para roles privilegiados (por ejemplo, **Propietario/Administrador** o accesos equivalentes) o para acciones de alto riesgo (p. ej., cambios críticos de seguridad, integraciones, recuperación de cuenta).

En caso de pérdida del segundo factor, se aplicará un procedimiento de **recuperación** que podrá incluir verificaciones reforzadas para reducir el riesgo de suplantación.

Estas medidas se adoptan conforme a un enfoque de seguridad **adecuado al riesgo**, coherente con la obligación de aplicar medidas técnicas y organizativas apropiadas (art. 32 RGPD) cuando el Servicio trate datos personales por cuenta del Cliente.

5.2.3 Recuperación/restablecimiento de credenciales

El Servicio podrá incorporar mecanismos de restablecimiento de credenciales (p. ej., "olvidé mi contraseña"). El Prestador podrá imponer salvaguardas como:

a) verificación mediante correo electrónico u otros factores;

b) periodos de enfriamiento ("cooldown") y limitación de intentos;

c) invalidación de sesiones activas tras el reseteo; y

d) verificaciones adicionales cuando exista riesgo razonable (p. ej., cambios de Propietario/Administrador, indicios de fraude o acceso desde ubicaciones anómalas).

El Cliente es responsable de mantener actualizados los datos de contacto necesarios para completar estos procesos.

5.2.4 Sesiones y dispositivos

El Servicio podrá aplicar controles de sesión orientados a la seguridad, tales como:

a) expiración de sesión tras inactividad;

b) limitación de sesiones concurrentes o por dispositivo (si se habilita);

c) cierre de sesión remoto o invalidación de tokens; y/o

d) mecanismos de "recordarme" sujetos a controles de seguridad razonables.

El Prestador podrá ajustar estas políticas por motivos de seguridad o evolución del Servicio.

5.2.5 Seguridad por diseño y por defecto (autenticación y control de acceso)

El Prestador procurará aplicar principios de **seguridad y privacidad desde el diseño y por defecto** en los mecanismos de autenticación y control de acceso, adoptando medidas proporcionadas al riesgo (por ejemplo, controles de acceso, minimización de privilegios, y mecanismos antiabuso), sin necesidad de comprometerse a tecnologías concretas en el texto contractual.

Lo anterior se entiende sin perjuicio del desarrollo detallado en el **Anexo de Seguridad** y del marco de "protección de datos desde el diseño y por defecto" del art. 25 RGPD, cuando proceda.

5.3 Actividad sospechosa y deberes de notificación

5.3.1 Definición de actividad sospechosa

Se considerará "actividad sospechosa", a título enunciativo:

a) accesos desde ubicaciones/dispositivos inusuales o patrones anómalos;

b) múltiples intentos fallidos de autenticación;

c) indicios de credenciales comprometidas (filtraciones, phishing, reutilización detectada);

d) uso atípico o abusivo de integraciones/API (si existe);

e) modificaciones inesperadas en roles/permisos o acciones administrativas críticas; o

f) cualquier otro indicador razonable de suplantación, fraude o riesgo de seguridad.

5.3.2 Obligación del Cliente de notificar diligentemente

El Cliente se obliga a notificar **sin dilación** al Prestador, por los canales habilitados, cualquier:

a) sospecha de compromiso de credenciales (contraseñas, 2FA, tokens);

b) acceso no autorizado real o presunto;

c) error material en la asignación de roles/permisos que pueda exponer información; o

d) actividad anómala detectada en su organización relacionada con el uso del Servicio.

Esta obligación es especialmente relevante cuando el Servicio contenga o trate **datos personales**, por su impacto potencial en la seguridad y en el cumplimiento normativo.

5.3.3 Cooperación y medidas inmediatas

Ante una notificación o detección de actividad sospechosa, el Prestador podrá adoptar medidas proporcionadas como:

a) bloqueo temporal de acceso o de determinadas acciones;

b) reseteo de credenciales y cierre de sesiones activas;

c) revocación/rotación de tokens y credenciales técnicas (si existen); y/o

d) limitación temporal de integraciones o funcionalidades especialmente sensibles.

El Cliente cooperará razonablemente para restaurar la seguridad (p. ej., confirmación de usuarios autorizados, revisión de permisos, adopción de 2FA, etc.).

5.3.4 Incidentes de seguridad y datos personales (notificación al Cliente)

Cuando el Prestador actúe como **Encargado del tratamiento** respecto de datos personales tratados por cuenta del Cliente, y tenga conocimiento de una **violación de seguridad de datos personales**, notificará al Cliente **sin dilación indebida**, conforme al art. 33.2 RGPD, para permitir al Cliente valorar y, en su caso, cumplir sus obligaciones de notificación ante la autoridad de control y/o comunicación a interesados. El procedimiento detallado (canales, contenido mínimo y cooperación) se desarrollará en el **DPA** y/o en el Anexo de Seguridad/Incidentes.

5.4 Prohibición de compartir cuentas y reventa sin autorización

5.4.1 Cuentas nominativas y no compartibles

Las cuentas de usuario son **personales e intransferibles** dentro del marco de la cuenta del Cliente. Queda prohibido:

a) compartir credenciales entre varias personas;

b) permitir el acceso a usuarios no autorizados; o

c) eludir la creación de usuarios individuales mediante el uso de una cuenta “genérica”, salvo que el Servicio lo permita expresamente bajo condiciones específicas.

El Cliente es responsable de implementar una gestión adecuada de altas/bajas y permisos.

5.4.2 Prohibición de reventa, sublicencia o “service bureau” sin autorización

Salvo autorización expresa y por escrito del Prestador, queda prohibido:

a) revender o sublicenciar el Servicio a terceros;

b) ofrecer el Servicio como parte de una solución “marca blanca” sin acuerdo; o

c) utilizar MAGOS como “service bureau” para prestar servicios a múltiples terceros de forma que, en la práctica, el tercero sea el destinatario real del Servicio sin ser Cliente autorizado.

Lo anterior no impide que una **gestoría** o asesor externo use el Servicio **como Usuario Autorizado** del Cliente, si el Cliente le concede acceso conforme a estos TyC.

5.4.3 Consecuencias (remisión)

Las consecuencias del incumplimiento de este apartado (incluida la suspensión, limitación de acceso o terminación) se regirán por las cláusulas específicas de **Uso Aceptable**, **Suspensión/Terminación** y, en su caso, por el régimen de planes y licencias, evitando duplicidades.

5.5 Registro de actividad y trazabilidad

5.5.1 Logs / audit trail (qué se registra)

El Prestador podrá mantener registros de actividad (“logs”) y, cuando el Servicio lo habilite, un rastro de auditoría (“audit trail”) que recoja, a nivel general, eventos tales como:

a) accesos e intentos de acceso;

b) acciones administrativas relevantes (altas/bajas de usuarios, cambios de roles/permisos);

c) configuración de integraciones/credenciales técnicas (si existe); y

d) otros eventos necesarios para la seguridad, operación, soporte y prevención de fraude.

5.5.2 Finalidades

Los registros anteriores podrán utilizarse para:

a) reforzar la **seguridad** del Servicio (detección y respuesta ante incidentes);

b) prestar **soporte** y resolución de incidencias;

c) asegurar la continuidad operativa y prevenir abuso; y

d) cumplir obligaciones de diligencia y medidas de seguridad cuando corresponda, en coherencia con el art. 32 RGPD (medidas técnicas y organizativas apropiadas) en los tratamientos en que el Prestador actúe como encargado.

5.5.3 Retención

Los logs y registros de trazabilidad se conservarán durante el **tiempo estrictamente necesario** para las finalidades anteriores y/o durante los plazos que resulten necesarios para la atención de incidencias, seguridad y defensa frente a reclamaciones, de acuerdo con criterios de minimización y proporcionalidad. Los plazos o criterios concretos de retención (si se fijan) se detallarán en el **Anexo de Seguridad** y/o en la documentación de privacidad aplicable.

Si quieres, en el siguiente paso enlazo esto con un **Anexo de Seguridad** (no técnico en exceso, pero sí "contractual") donde fijemos: 2FA obligatorio para Propietario/Administrador, retención de logs por ventanas (p. ej., 90/180 días), y un mini **procedimiento de respuesta a incidentes** alineado con AEPD/RGPD.

5.6 Gestión de accesos privilegiados

5.6.1 Usuarios privilegiados (Propietario/Administrador): medidas reforzadas y 2FA obligatorio

A efectos de seguridad, se consideran **usuarios privilegiados** aquellos con capacidad para administrar la cuenta del Cliente, gestionar usuarios/roles, configurar integraciones o ejecutar acciones de alto impacto (incluyendo, en particular, los roles de **Propietario** y **Administrador**).

a) **2FA/MFA obligatorio (cuando esté disponible)**: el Cliente acepta que, **en cuanto el Servicio lo habilite**, el uso de **2FA/MFA será obligatorio** para los roles de Propietario y Administrador (y, en su caso, roles equivalentes). El Cliente deberá asegurar que dichos usuarios activen y mantengan operativo el 2FA/MFA; en caso contrario, el

Prestador podrá limitar el acceso a funcionalidades privilegiadas o al propio acceso privilegiado, por razones de seguridad. Esta medida se adopta conforme a un enfoque de seguridad adecuado al riesgo, coherente con la exigencia de medidas técnicas y organizativas apropiadas del **art. 32 RGPD** en los tratamientos en que el Prestador actúe como encargado.

b) **Medidas reforzadas**: el Prestador podrá imponer verificaciones adicionales para acciones privilegiadas (p. ej., reautenticación, confirmación por canal secundario, limitaciones temporales), especialmente ante señales de riesgo (accesos anómalos, cambios masivos de permisos, etc.).

c) **Revisión periódica**: el Cliente se compromete a revisar periódicamente (por ejemplo, con carácter trimestral o cuando existan cambios organizativos) qué personas mantienen roles privilegiados, reduciendo privilegios a lo estrictamente necesario (principio de mínimo privilegio).

5.6.2 Segregación de funciones (SoD) y configuración interna

Cuando el Servicio lo permita, el Cliente deberá configurar roles y permisos de forma que exista **segregación de funciones** razonable entre tareas incompatibles (por ejemplo, separación entre funciones de **Contable**, **Tesorero** y **Auditor**), con el fin de reducir riesgo de error, fraude o accesos indebidos.

El Cliente reconoce que la efectividad de esta segregación depende de su configuración y gobierno interno, y que el Prestador no puede garantizar el control interno del Cliente más allá de las herramientas de permisos que el Servicio ponga a su disposición.

5.6.3 Procedimiento para cambios críticos (cambio de Propietario, recuperación de cuenta, etc.)

Se consideran **cambios críticos**, entre otros: cambio del Propietario, sustitución del Administrador principal, recuperación de una cuenta corporativa, cambios de email principal, rotación de credenciales técnicas, o reconfiguraciones que afecten significativamente a la seguridad.

Para estos supuestos, el Prestador podrá exigir un procedimiento reforzado que incluya:

a) verificación reforzada de identidad/autorización;

b) confirmación mediante canales previamente establecidos (email corporativo, verificación adicional u otros);

c) periodos de enfriamiento o limitación temporal de acciones posteriores; y/o

d) bloqueo preventivo si existen indicios de fraude o suplantación.

Estas medidas se aplicarán de forma proporcionada al riesgo y sin perjuicio de los apartados de suspensión preventiva y restablecimiento.

5.7 Accesos técnicos e integraciones (si hay API)

5.7.1 Emisión y custodia de tokens/keys

Si el Servicio ofrece API, webhooks o integraciones técnicas, el acceso podrá realizarse mediante **tokens/keys** u otros mecanismos de autenticación. El Cliente se obliga a:

a) custodiar dichas credenciales como **confidenciales**;

b) limitar su acceso a personal/servicios estrictamente necesarios;

c) no publicar ni incorporar credenciales en repositorios, código compartido o entornos inseguros; y

d) informar sin dilación de cualquier indicio de compromiso.

5.7.2 Límites, rotación y revocación

El Prestador podrá establecer:

a) **límites de uso** (rate limits, cuotas, límites por plan);

b) requisitos de **rotación** periódica o rotación obligatoria tras incidentes;

c) revocación de tokens por motivos de seguridad, abuso, incumplimiento o riesgo operativo; y

d) expiración automática y necesidad de reemisión.

Estas medidas podrán ajustarse por evolución técnica, seguridad o continuidad del Servicio, y se entenderán complementarias a la política de uso aceptable.

5.7.3 Responsabilidad por automatizaciones del Cliente

El Cliente es responsable de las automatizaciones, integraciones y procesos que ejecute contra la API o mediante credenciales técnicas, incluyendo:

a) que su uso sea conforme a estos TyC y a la finalidad del Servicio;

b) que no genere cargas abusivas, comportamientos anómalos o accesos indebidos; y

c) que adopte medidas razonables de control (monitorización, límites internos, revocación de credenciales al finalizar relaciones con terceros).

El Prestador podrá aplicar medidas antiabuso y, si fuera necesario, limitar o suspender accesos técnicos conforme a los apartados 5.8 y a las cláusulas de uso aceptable.

5.8 Suspensión preventiva por seguridad

5.8.1 Derecho a suspender/limitar accesos ante riesgo razonable

El Prestador podrá **suspender o limitar** de forma preventiva el acceso a la cuenta (total o parcial), a determinados usuarios, o a integraciones técnicas, cuando existan indicios razonables de:

a) suplantación, fraude o acceso no autorizado;

b) compromiso de credenciales (incluyendo credenciales técnicas);

c) abuso de recursos o ataques al Servicio; o

d) cualquier situación que pueda comprometer la seguridad, integridad o disponibilidad del Servicio o de los datos.

Estas medidas se adoptarán con criterios de proporcionalidad y gestión del riesgo, y se entienden sin perjuicio del régimen de terminación (que se regula en cláusulas específicas).

5.8.2 Restablecimiento del acceso

El restablecimiento podrá condicionarse, según el caso, a:

a) verificación de identidad/autorización del Cliente o del usuario privilegiado;

b) reseteo de contraseñas y cierre de sesiones;

c) activación de 2FA/MFA (en especial para Propietario/Administrador cuando esté disponible);

d) rotación/reemisión de tokens/keys; y/o

e) revisión de roles/permisos y de accesos de terceros.

El Prestador podrá mantener restricciones temporales hasta que el riesgo se considere mitigado.

5.8.3 Comunicación (canales y criterios)

Salvo que existan motivos de seguridad que aconsejen discreción o inmediatez (p. ej., ataque en curso), el Prestador procurará informar al Cliente de la suspensión/limitación y su motivo general mediante los canales operativos definidos (panel del Servicio, correo electrónico u otros). La comunicación no incluirá información que pudiera comprometer la seguridad del Servicio o facilitar abusos.

5.9 Responsabilidades del Cliente en su entorno

5.9.1 Seguridad del endpoint

El Cliente es responsable de asegurar los dispositivos y entornos desde los que se accede al Servicio (equipos, móviles, redes), incluyendo medidas razonables como:

a) sistemas actualizados;

b) protección frente a malware;

c) uso de gestores de contraseñas;

d) control de accesos físicos y lógicos; y

e) políticas internas de seguridad (especialmente para usuarios privilegiados).

5.9.2 Gestión interna de usuarios

El Cliente se compromete a mantener una gestión diligente del ciclo de vida de usuarios, incluyendo:

a) alta únicamente de usuarios necesarios;

b) revocación inmediata de accesos ante bajas/cambios de puesto o finalización de relación con terceros (p. ej., gestorías);

c) revisión periódica de roles/permisos; y

d) evitar cuentas genéricas compartidas.

5.9.3 Buenas prácticas (alineación con recomendaciones AEPD)

El Cliente procurará adoptar buenas prácticas de seguridad coherentes con recomendaciones públicas habituales (por ejemplo, contraseñas robustas, doble factor, prevención de phishing, mínimo privilegio), especialmente cuando el Servicio trate datos personales o información sensible del negocio, contribuyendo al principio de **integridad y confidencialidad** y al enfoque de medidas apropiadas al riesgo previsto por el **RGPD** (arts. 5.1.f y 32, cuando aplique).

5.10 Evidencia de aceptación y comunicaciones de cuenta

5.10.1 Evidencia de aceptación/contratación electrónica

A efectos de prueba de contratación y aceptación de condiciones, el Prestador podrá conservar registros razonables que acrediten:

a) la aceptación de los TyC (y anexos aplicables) por vía electrónica;

b) la versión concreta aceptada;

c) la fecha/hora y eventos relevantes del proceso; y

d) confirmaciones o comunicaciones emitidas durante el alta/contratación.

Lo anterior se realiza en el marco de la contratación por medios electrónicos y obligaciones asociadas, conforme a la **Ley 34/2002 (LSSI-CE)**, sin perjuicio de que el detalle del proceso precontractual y confirmaciones se desarrolle en el apartado específico de contratación electrónica del contrato.

5.10.2 Comunicaciones operativas de seguridad

El Prestador podrá remitir comunicaciones operativas relacionadas con la seguridad y la cuenta, tales como:

a) avisos de inicio de sesión o accesos anómalos (si se habilita);

b) confirmaciones de cambios de credenciales, activación/desactivación de 2FA, cambios de roles/permisos;

c) alertas sobre integraciones/tokens (creación, rotación, revocación); y/o

d) avisos de mantenimiento o medidas preventivas de seguridad.

Estas comunicaciones podrán realizarse por email, panel del Servicio u otros canales definidos, y tendrán carácter operativo y de seguridad.

Si quieres, el siguiente paso lógico es redactar el **punto 6 (Contratación electrónica y formación del contrato)**, porque encaja perfectamente con 5.10 y deja cerrada la parte LSSI-CE de forma muy sólida.

6. Contratación electrónica y formación del contrato

6.0 Alcance del proceso de contratación

6.0.1 Canales de contratación incluidos

La contratación del Servicio podrá realizarse, según la modalidad habilitada en cada momento, a través de:

a) **contratación "self-serve"** mediante formulario de registro/alta disponible en la web/app;

b) **contratación por propuesta/orden de pedido ("Order Form")** o condiciones particulares, cuando el Prestador la habilite; y/o

c) contratación por canal **asistido** (por ejemplo, alta gestionada con soporte/comercial), cuando proceda.

6.0.2 Definición de "procedimiento de contratación"

A los efectos de la **Ley 34/2002 (LSSI-CE)**, el "procedimiento de contratación" comprende el conjunto de pasos electrónicos que van, con carácter general, desde la **selección del plan** y la **introducción de datos** del Cliente, hasta la **aceptación expresa** de los TyC y la **confirmación** del alta/contratación.

6.0.3 Exclusiones: soporte o consultas que no constituyen oferta contractual

Las comunicaciones informativas, demostraciones, consultas a soporte, o intercambios previos (por correo, teléfono o similares) **no constituyen** por sí mismos una oferta contractual vinculante, salvo que se formalicen mediante los mecanismos de contratación habilitados (formulario/aceptación o, en su caso, Order Form aceptado).

6.1 Pasos para contratar (checkout/aceptación)

(Conforme al deber de informar de "los distintos trámites" previos a la contratación del art. 27 LSSI-CE.)

6.1.1 Selección del plan/servicio

El Cliente seleccionará el **plan** del Servicio (y, en su caso, opciones o módulos disponibles conforme a la oferta vigente). La disponibilidad de funcionalidades podrá depender del plan contratado y de la configuración habilitada.

6.1.2 Identificación del Cliente (datos de empresa y facturación)

El Cliente completará el formulario de alta facilitando los datos necesarios para:

a) identificar a la **entidad** que contrata (razón social/identificación fiscal y demás datos requeridos); y

b) habilitar la **facturación y el cobro** conforme a la modalidad vigente.

Cuando el usuario actúe en nombre de una entidad, declara hacerlo con facultades suficientes para vincularla (conforme a lo indicado en el punto 4).

6.1.3 Revisión previa del pedido (resumen)

Antes de finalizar el alta, el Cliente dispondrá de un **resumen** del servicio/plan seleccionado y de las condiciones económicas esenciales (precio, periodicidad e impuestos, si aplica), así como, en su caso, de información relativa a la mecánica del primer cobro.

6.1.4 Aceptación expresa de TyC y anexos aplicables (clickwrap)

Como parte del proceso, el Cliente debe manifestar una **aceptación expresa** de los presentes **Términos y Condiciones** mediante un mecanismo de checkbox ("clickwrap") y acceso a su lectura. Cuando resulte aplicable, el Cliente aceptará también los anexos que procedan (por ejemplo, DPA o SLA, cuando se incorporen).

Esta aceptación forma parte del procedimiento de contratación electrónica y su trazabilidad podrá conservarse conforme a lo indicado en el punto 5.10.

6.1.5 Finalización del alta y momento de emisión de la aceptación (formación del contrato)

El procedimiento finaliza cuando el Cliente envía el formulario de alta mediante el botón o acción equivalente ("Confirmar", "Crear cuenta", "Contratar" o similar). En ese momento:

a) se entiende emitida la **aceptación** del Cliente; y

b) el contrato se considera **formalizado** y el Cliente obtiene acceso al Servicio (alta efectiva), sin perjuicio de verificaciones posteriores (p. ej., verificación de email) y de las medidas de seguridad previstas en estos TyC.

6.1.6 Pago y cobro (domiciliación; primer mes gratuito)

En el modelo vigente, el Servicio se activa tras la finalización del alta, y el **cobro** se gestiona **por fuera del formulario** mediante **domiciliación**. En particular:

a) el **primer mes** desde la contratación es **gratuito**; y

b) la **primera cuota** se cargará el **primer día hábil del mes siguiente** al mes de contratación (p. ej., alta el 15 de enero → primer cargo el primer día hábil de febrero).

El Prestador podrá introducir en el futuro modalidades de cobro integradas en el proceso de contratación (p. ej., pasarela de pago), así como validaciones razonables de antifraude y seguridad. El detalle económico completo se regula en los puntos de planes/precios y pagos (puntos 7 y 8).

6.2 Archivo del contrato y accesibilidad para el usuario

(Art. 27 LSSI-CE: informar si se archiva el documento electrónico y si será accesible.)

6.2.1 Archivo del contrato

El Prestador **archivará** evidencia del contrato electrónico y de la aceptación de los TyC (incluyendo, razonablemente, la versión vigente aceptada y la fecha/hora), de acuerdo con lo indicado en el punto 5.10.

6.2.2 Acceso del Cliente

El Cliente podrá acceder a la información contractual y a los TyC vigentes, con carácter general, a través de:

a) el **panel/área privada** del Servicio o el área legal correspondiente; y/o

b) las secciones legales del Sitio.

El email de confirmación de alta tendrá carácter **meramente confirmativo** y no sustituye a la disponibilidad de los TyC en el Sitio/Servicio.

6.2.3 Duración de disponibilidad

La información contractual se mantendrá accesible, al menos, mientras la cuenta del Cliente permanezca activa y, tras la baja, durante el tiempo que resulte razonablemente necesario conforme a la política de retención y/o a necesidades de soporte, seguridad o defensa frente a reclamaciones.

6.2.4 Evidencia de versión

El Prestador conservará evidencia de la **versión** de TyC aceptada y de la fecha de aceptación, pudiendo emplear registros razonables (p. ej., identificadores de sesión y marca temporal), en coherencia con la prueba de contratación por vía electrónica prevista en el Título IV de la LSSI-CE.

6.3 Idioma(s) disponibles

(Art. 27 LSSI-CE: indicar lengua(s) en que podrá formalizarse el contrato.)

6.3.1 Idioma contractual

El contrato se formaliza, por defecto, en **español**.

6.3.2 Idiomas adicionales

El Prestador podrá ofrecer en el futuro versiones en otros idiomas (p. ej., catalán, gallego, euskera, inglés, portugués, francés). Salvo indicación expresa, dichas versiones podrán tener carácter informativo hasta que se habiliten como idioma contractual.

6.3.3 Regla de prevalencia

En caso de discrepancia entre versiones lingüísticas, prevalecerá la versión **en español**, salvo pacto expreso o norma imperativa aplicable en sentido distinto.

6.4 Medios para corregir errores antes de finalizar

(Art. 27 LSSI-CE: "medios técnicos para identificar y corregir errores" antes de confirmar.)

6.4.1 Identificación de errores (validaciones y mensajes)

Durante el registro/alta, el sistema podrá realizar **validaciones automáticas** para ayudar a identificar errores en los datos introducidos (p. ej., campos obligatorios incompletos, formatos inválidos, incoherencias evidentes), mostrando mensajes para su corrección.

6.4.2 Corrección previa (edición de datos antes de confirmar)

Antes de finalizar el alta, el Cliente dispondrá de medios para **editar** y corregir los datos facilitados (por ejemplo, volver a campos anteriores y modificar información).

6.4.3 Resumen final (pantalla de revisión)

Con carácter general, el procedimiento incluirá una instancia de **revisión** o resumen previo a la confirmación final (plan, datos esenciales y aceptación de TyC), que actúa como salvaguarda adicional para detectar y corregir errores.

6.4.4 Errores detectados tras contratar (subsanación)

Si, tras finalizar el alta, el Cliente detecta errores en datos administrativos o de facturación, podrá solicitar su **subsanación** por los canales habilitados (p. ej., soporte o panel), sin que ello implique un derecho de desistimiento propio de consumo en un contexto B2B. La corrección de datos podrá afectar a la emisión de documentos o a la operativa de cobro, conforme a lo previsto en los apartados económicos y de facturación.

Cuando quieras, continúo con **6.5** (confirmación/acuse de recibo del art. 28 LSSI-CE) y lo conectamos con vuestro email confirmativo y la evidencia de aceptación.