



PO.GMI

Grupos de Mensajería Instantánea

Política de Protección de Datos

Versión: **v1.0** | Fecha: **01/08/25** | Clasificación: **Confidencial / Interno**

La **Política de Protección de Datos en Grupos de Mensajería Instantánea** establece las normas y responsabilidades para la creación, gestión y cierre de grupos corporativos en aplicaciones de mensajería, con el fin de garantizar un uso responsable y seguro de estos canales, proteger la confidencialidad de la información y asegurar el cumplimiento del RGPD, la LOPDGDD y la normativa interna de la organización.

Tabla de contenido

1. Identificación y Control Documental.....	2
2. Objeto, Finalidad y Alcance	4
3. Marco Normativo y Referencias.....	7
4. Definiciones y Conceptos Clave	9
5. Principios de Tratamiento de Datos Personales	11
6. Bases Jurídicas y Evaluación de Licitud	14
7. Roles y Responsabilidades	17
8. Reglas de Creación, Uso y Administración.....	19
9. Transparencia e Información a los Interesados.....	21
10. Seguridad y Confidencialidad	22
11. Derechos de los Interesados.....	24
11. Evaluación de Impacto y Análisis de Riesgos	26
12. Brechas de Seguridad y Notificación de Incidentes	28
13. Conservación y Supresión de Grupos y Mensajes.....	30
14. Difusión y Concienciación	32
15. Supervisión, Auditoría y Actualización	33
16. Anexos	35

1. Identificación y Control Documental

Este apartado garantiza la **trazabilidad, autenticidad y control de versiones** de la presente Política, conforme a los principios de **gobernanza documental** y de **responsabilidad proactiva** (art. 24 RGPD).

1.1. Identificación del documento

- **Título:** Política de Protección de Datos para Grupos de Comunicación mediante Mensajería Instantánea
- **Código interno:** PO.GMI
- **Versión:** v1.0
- **Fecha de emisión:** 01/08/2025
- **Fecha de revisión:** 01/08/2026
- **Propietario/Custodia:** [Área de Cumplimiento / Administración]
- **Responsables de aprobación:** Alta Dirección
- **Distribución (quién tiene acceso):** Distribución controlada (Empleados, administradores de grupos, colaboradores autorizados, auditores internos/externos).
- **Nivel de Confidencialidad:** Confidencial / Interno
- **Estado del documento:** Vigente

1.2. Propietario del documento y custodia

El propietario del documento es el Representante Legal de la entidad, quien se encarga de:

- Mantener la versión actualizada y accesible.
- Asegurar la custodia en el repositorio corporativo autorizado (intranet, gestor documental).
- Garantizar la correcta clasificación de la información (Interna / Confidencial).

1.3. Aprobaciones

La presente Política ha sido aprobada por:

- **Órgano de gobierno competente:** Dirección de la entidad
- **Fecha de aprobación:** 19/08/2025

1.4. Historial de cambios (control de versiones)

VERSIÓN	FECHA	DESCRIPCIÓN DEL CAMBIO	AUTOR	APROBADO POR
v1.0	01/08/2025	Emisión inicial	S. Cabello	J.J. Puchol

1.5. Distribución y acceso

- **Acceso autorizado:**
 - Personal interno de la entidad (empleados, directivos).
 - Administradores de grupos de mensajería.
 - Colaboradores externos bajo NDA o contrato con cláusula de confidencialidad.
- **Repositorios de acceso:**
 - Intranet corporativa / Gestor documental / Carpeta de políticas de seguridad.
- **Clasificación de seguridad:** Documento **Confidencial Interno**.

1.6. Calendario de revisión y vigencia

- **Periodicidad de revisión:** Anual, o antes si concurren cambios normativos, tecnológicos u organizativos relevantes.
- **Fecha de próxima revisión:** 01/08/2025
- El área de Cumplimiento será responsable de proponer modificaciones.
- El Comité/Alta Dirección aprobará la nueva versión.

2. Objeto, Finalidad y Alcance

Esta sección define con precisión **qué regula la presente Política**, sus objetivos en materia de cumplimiento normativo, a quién y a qué aplica, y qué situaciones quedan expresamente excluidas.

2.1. Objeto de la política

El objeto de la presente **Política de Protección de Datos para Grupos de Comunicación mediante Mensajería Instantánea (en adelante, la “Política”)** es:

- Establecer las **normas, controles y responsabilidades** que rigen la creación, uso administración y cierre de grupos de mensajería instantánea utilizados por **MAQUICER SL** para fines corporativos (incluyendo, a título enunciativo, WhatsApp, Telegram, Signal, Microsoft Teams, Slack, Google Chat u otras plataformas autorizadas).
- Garantizar que el tratamiento de datos personales en dichos grupos se realiza de manera **lícita, leal, transparente, segura y conforme al RGPD, LOPDGDD y normativa sectorial aplicable**.
- Prevenir riesgos legales, reputacionales y de seguridad derivados del uso inadecuado de canales de mensajería en la organización (ejemplo: fuga de datos por mensajería no controlada).

2.2. Finalidad y objetivos de cumplimiento

La finalidad de esta política es **proteger los datos personales** tratados en grupos de mensajería, asegurando un uso controlado y responsable de estos canales. Sus objetivos específicos son:

- **Cumplimiento normativo:** asegurar la conformidad con el RGPD, LOPDGDD y normativa sectorial.
- **Confidencialidad:** preservar la privacidad de empleados, clientes, proveedores y terceros.
- **Seguridad:** minimizar riesgos de fuga, pérdida o acceso indebido a la información compartida.
- **Transparencia:** garantizar que los interesados reciben información clara sobre el tratamiento de sus datos.
- **Eficiencia organizativa:** unificar criterios en la creación, uso, administración y cierre de grupos.

- **Responsabilidad proactiva:** demostrar ante auditorías y autoridades que la entidad aplica controles efectivos.

2.3. Alcance (Organizativo y Geográfico)

Alcance organizativo:

- **Personal interno:** empleados, directivos y becarios de **MAQUICER SL**.
- **Colaboradores externos:** proveedores, encargados del tratamiento, consultores y terceros que participen en grupos corporativos por encargo de **MAQUICER SL**.
- **Unidades y proyectos:** todas las áreas, filiales y proyectos, con independencia de su localización geográfica.

Alcance geográfico:

- Aplica a todos los tratamientos realizados con independencia del lugar donde se encuentren los miembros del grupo o los servidores de la aplicación utilizada. Es decir, aplica a todas las sedes, filiales y teletrabajo de la entidad y fuera de ella.
- Incluye los supuestos en los que la plataforma de mensajería realice **transferencias internacionales de datos** fuera del EEE.

2.4. Procesos, Sistemas y Datos cubiertos

Procesos cubiertos:

- Comunicación interna entre equipos y departamentos.
- Coordinación de proyectos y turnos.
- Gestión de emergencias o incidencias.
- Atención a clientes, proveedores o usuarios mediante grupos autorizados.

Sistemas cubiertos:

- Únicamente las plataformas de mensajería **aprobadas por el Responsable del Tratamiento**.
- Aplicaciones integradas con sistemas corporativos bajo contrato de encargo de tratamiento (cuando aplique).

Datos cubiertos:

- Datos identificativos (nombre, teléfono, alias, correo electrónico).
- Datos de comunicación (mensajes, audios, archivos compartidos).
- Metadatos (hora, fecha, remitente, estado de entrega).

2.5. Exclusiones justificadas

Quedan fuera del alcance de esta política:

- Grupos de mensajería creados por iniciativa personal de empleados sin autorización de la organización.
- Grupos estrictamente privados de carácter personal, familiar o social.
- Plataformas de mensajería no aprobadas por la organización.
- Conversaciones bilaterales privadas entre empleados en plataformas personales (salvo que se utilicen indebidamente para tratar información corporativa).
- Tratamientos de datos que, por su naturaleza, estén regulados por otras políticas internas específicas (ej. política de videovigilancia, política de control de accesos, política de gestión de incidentes).

2.6. Prohibiciones

- Queda prohibida la creación de grupos con **menores de edad** salvo autorización expresa y cumplimiento de requisitos legales reforzados.
- Queda prohibido tratar en grupos **categorías especiales/sensibles** de datos (art. 9 RGPD) o **datos penales** (art. 10 RGPD), salvo supuestos **estrictamente justificados**, documentados y **autorizados por** el Responsable del Tratamiento (y, en su caso, por el Área de Cumplimiento), con **medidas reforzadas**.
- Cualquier uso no autorizado de grupos o aplicaciones de mensajería para tratar datos personales de la entidad será considerado **incumplimiento grave** de esta política y podrá conllevar responsabilidades disciplinarias, contractuales o legales.
- Se prohíbe expresamente la sincronización con nubes personales.

3. Marco Normativo y Referencias

3.1. Reglamento General Protección de Datos (RGPD – UE 2016/679)

El RGPD constituye la **norma principal** que regula el tratamiento de datos personales en el contexto de grupos de mensajería instantánea. Los artículos más relevantes son:

- **Artículo 5:** Principios del tratamiento (licitud, transparencia, minimización, limitación del plazo, integridad/confidencialidad y responsabilidad proactiva).
- **Artículo 6:** Bases de licitud (contrato, obligación legal, interés legítimo, consentimiento, etc.).
- **Artículo 9:** Prohibición general y excepciones al tratamiento de categorías especiales de datos.
- **Artículo 10:** Tratamiento de datos relativos a condenas e infracciones penales.
- **Artículos 12 a 14:** Transparencia e información a los interesados.
- **Artículos 15 a 22:** Derechos de los interesados (acceso, rectificación, supresión, limitación, oposición, portabilidad, decisiones automatizadas).
- **Artículo 25:** Privacidad desde el diseño y por defecto.
- **Artículo 32:** Seguridad del tratamiento.
- **Artículos 33 y 34:** Notificación de brechas de seguridad.
- **Artículo 35:** Evaluación de impacto relativa a la protección de datos.
- **Artículos 44 a 49:** Transferencias internacionales de datos (aplicable en servicios de mensajería con servidores fuera del EEE).

3.2. Ley Orgánica 3/2018 de Protección de Datos Personales y Garantía de Derechos Digitales (LOPDGDD)

Complementa el RGPD en España y contiene disposiciones específicas aplicables al uso de mensajería instantánea en entornos corporativos:

- **Título I:** Principios de protección de datos.
- **Título II:** Derechos de los interesados (ejercicio en entornos laborales y digitales).
- **Artículo 87 y ss.:** Derechos digitales en el ámbito laboral (uso de dispositivos digitales, desconexión digital, protección frente a videovigilancia y geolocalización).
- **Artículo 91:** Regulación de sistemas de información en la relación laboral.

- **Artículos 70-72:** Régimen sancionador y tipificación de infracciones.

3.3. Legislación laboral y sectorial aplicable

Dependiendo de la actividad de **MAQUICER SL**, pueden resultar de aplicación:

- **Estatuto de los Trabajadores** (art. 20 y 21 sobre facultades de control empresarial; art. 64 sobre derechos de información de representantes).
- **Ley de Prevención de Riesgos Laborales**, en relación con la desconexión digital y la salud laboral.
- **Normativa sectorial específica:**
 - No aplica, pues no existen normativas sectoriales que afecten a la protección de los datos personales.

3.4. Normas y políticas internas relacionadas

Esta Política **complementa** (no sustituye) y debe leerse conjuntamente con otras normas corporativas:

- Política de Seguridad de la Información.
- Política de Control de Accesos y Uso de Dispositivos.
- Política de Confidencialidad y Secreto Profesional.
- Política de Gestión de Incidentes de Seguridad.
- Política de Conservación y Eliminación de Información.
- Código Ético / Código de Conducta.
- Manual de Cumplimiento Normativo.
- Contratos y Acuerdos con proveedores tecnológicos.
- Cualquier otra Política o Procedimiento establecido por la organización

En caso de conflicto, prevalecerá la normativa legal aplicable y la Política de Seguridad de la Información.

4. Definiciones y Conceptos Clave

La presente Política emplea las siguientes definiciones, que deben entenderse conforme al **RGPD** y la **LOPDGDD**.

4.1. Grupo de mensajería instantánea

Conjunto de usuarios reunidos en un canal o espacio digital dentro de una plataforma de mensajería instantánea (p. ej., WhatsApp, Telegram, Signal, Teams, Slack), creado con fines **profesionales, organizativos o corporativos** y vinculado a la actividad de **MAQUICER SL**.

- Puede ser **interno** (empleados, colaboradores, directivos) o **externo** (clientes, proveedores, socios).
- El grupo no constituye un medio oficial de archivo ni un sistema de registro administrativo, salvo que se indique expresamente en esta Política o normativa aplicable.

4.2. Administrador del grupo

Persona (empleado o colaborador) designada por **MAQUICER SL** para gestionar un grupo de mensajería corporativo.

4.3. Miembro/Usuario del grupo

Persona física que participa en un grupo de mensajería corporativo.

4.4. Datos personales tratados en los grupos

Cualquier información que identifique o pueda identificar a una persona física y que pueda ser comunicada, compartida o gestionada dentro de los grupos, entre otros:

- **Datos identificativos:** nombre, apellidos, alias, cargo, número de teléfono, dirección de correo electrónico.
- **Datos de comunicación:** mensajes escritos, notas de voz, archivos compartidos, documentos adjuntos, imágenes, vídeos.
- **Metadatos:** fecha/hora de envío, dispositivo emisor, estado de lectura.
- **Otros datos sensibles:** queda prohibido compartir categorías especiales (salud, religión, afiliación sindical, orientación sexual, etc.) salvo autorización expresa y justificada conforme al art. 9 RGPD.

4.5. Comunicación electrónica corporativa vs. personal

- **Comunicación corporativa:** Aquella que se produce en grupos creados o gestionados por **MAQUICER SL**, vinculada a fines laborales, operativos o de negocio.
- **Comunicación personal:** Aquella que se produce en grupos privados creados por empleados o terceros fuera del control de la organización.

⚠ Queda expresamente prohibido usar comunicaciones personales para tratar datos corporativos o compartir información sujeta a protección de datos de la organización.

5. Principios de Tratamiento de Datos Personales

Todo tratamiento de datos personales realizado en grupos de mensajería instantánea deberá ajustarse estrictamente a los principios recogidos en el **artículo 5 del RGPD**, desarrollados a continuación con aplicación práctica:

5.1. Licitud, lealtad y transparencia

- **Licitud:** Solo se crearán y utilizarán grupos cuando exista una **base jurídica válida** (ej. cumplimiento de un contrato laboral, prestación de un servicio, interés legítimo documentado, consentimiento informado en casos justificados).
- **Lealtad:** No se utilizarán los grupos para fines ocultos, engañosos o distintos a los comunicados.
- **Transparencia:** Cada grupo deberá contar con una **cláusula informativa** accesible para sus miembros, explicando finalidad, base jurídica, responsable del tratamiento y derechos.

5.2. Limitación de la finalidad

Los grupos se crearán únicamente para fines **específicos y legítimos**, previamente definidos y aprobados.

- **Ejemplos de finalidades legítimas:**
 - Comunicación de incidencias operativas.
 - Coordinación de proyectos y trabajos internos.
 - Comunicación entre personal de guardia/emergencias.
 - Comunicación de turnos de trabajo.
- **Queda prohibido:**
 - Uso para fines personales no relacionados con la organización.
 - Difusión de publicidad no autorizada.
 - Intercambio de datos sensibles sin autorización expresa.

5.3. Minimización de datos

Solo se compartirán los **datos estrictamente necesarios** para cumplir la finalidad del grupo.

- Ejemplos de aplicación:

- En lugar de compartir datos de clientes completos, solo se compartirá un identificador interno.
- Evitar reenviar cadenas de mensajes o adjuntar documentos innecesarios.
- Se desaconseja el uso de fotos, audios o documentos que contengan **información excesiva o irrelevante**.

5.4. Exactitud y actualización

- Los administradores deberán procurar que los miembros sean siempre los adecuados y actualizados (ejemplo: baja inmediata del grupo de un trabajador que finaliza contrato).
- Los datos compartidos deberán ser exactos, verificables y actualizados.
- Se prohíbe reenviar información obsoleta o no contrastada que pueda generar riesgos de seguridad o de derechos para los interesados.

5.5. Limitación del plazo de conservación

- Los mensajes y archivos en grupos **no constituyen un repositorio permanente**.
- Una vez cumplida la finalidad, los grupos deberán:
 - Ser eliminados de forma segura, o
 - Procederse al borrado de mensajes/documentos irrelevantes.
- El **plazo máximo de conservación** será el necesario para la finalidad declarada, salvo que exista obligación legal de conservar ciertas comunicaciones como evidencia.

5.6. Integridad y confidencialidad

Se implementarán medidas técnicas y organizativas que eviten accesos no autorizados, difusión indebida o pérdida de la información.

Medidas mínimas:

- Uso de plataformas de mensajería con **cifrado de extremo a extremo**.
- Configuración de privacidad adecuada (no mostrar teléfonos a desconocidos, evitar inclusión masiva no consentida).
- Bloqueo de pantalla en dispositivos y control de acceso.
- Prohibición de reenvío, difusión externa o capturas de pantalla sin autorización.

5.7. Responsabilidad proactiva (accountability)

El Responsable del Tratamiento y el Área de Cumplimiento deben documentar las decisiones relacionadas con el uso de mensajería instantánea.

Ejemplos de responsabilidad proactiva:

- Justificar documentalmente la creación de cada grupo (finalidad, base jurídica, responsables).
- Mantener un registro de grupos activos con sus administradores designados.
- Revisar periódicamente los grupos para comprobar cumplimiento de esta Política.

6. Bases Jurídicas y Evaluación de Licitud

El tratamiento de datos personales en grupos de mensajería instantánea deberá apoyarse en una **base de licitud válida** conforme al artículo 6 del RGPD, documentada y justificada en cada caso.

6.1. Contrato, obligación legal, interés vital, interés público, interés legítimo

- **Contrato (art. 6.1.b RGPD):** Procede cuando el uso de grupos sea necesario para la ejecución de un contrato con empleados, clientes o proveedores.
 - Ejemplo: grupo de soporte técnico creado para cumplir un contrato de mantenimiento.
- **Obligación legal (art. 6.1.c RGPD):** Procede cuando una norma exija mantener un canal de comunicación específico.
 - Ejemplo: grupo para coordinación en emergencias exigido por normativa sectorial o de prevención de riesgos.
- **Interés vital (art. 6.1.d RGPD):** Procede en casos excepcionales para proteger la vida o integridad física de una persona.
 - Ejemplo: compartir ubicación en grupo de emergencias médicas.
- **Interés público (art. 6.1.e RGPD):** Procede en organismos públicos o privados que actúen en funciones de interés público.
 - Ejemplo: comunicación entre sanitarios en un plan de salud pública.
- **Interés legítimo (art. 6.1.f RGPD):** Procede cuando la organización necesita usar mensajería instantánea para fines operativos, siempre que no prevalezcan los derechos del interesado.
 - Ejemplo: grupo de coordinación de guardias en una clínica.
 - Requiere documentar un **Juicio de Interés Legítimo (LIA)** con:
 1. Identificación del interés perseguido.
 2. Necesidad del tratamiento.
 3. Equilibrio frente a los derechos de los interesados.

6.2. Consentimiento (requisitos, obtención y retirada)

Se utilizará **solo cuando no sea posible aplicar otra base jurídica**.

Requisitos del consentimiento:

- **Libre:** el interesado no debe sentirse obligado.
- **Específico:** para una finalidad concreta (ej. comunicaciones comerciales vía WhatsApp).
- **Informado:** debe conocer el responsable, finalidad, base legal y derechos.
- **Inequívoco:** debe manifestarse con una acción clara (ej. marcar casilla, aceptar cláusula).
- **Retirada:** debe poder retirarse en cualquier momento, sin consecuencias negativas.

6.3. Categorías especiales (art. 9) y penales (art. 10)

- **Datos especiales (art. 9 RGPD):** salud, religión, afiliación sindical, orientación sexual, etc.
 - **Prohibido** su tratamiento en grupos salvo que concurra una excepción (consentimiento explícito, obligación legal en salud pública, etc.).
 - Ejemplo prohibido: compartir partes o pruebas de accidentes de un trabajador en un grupo de WhatsApp de trabajo.
- **Datos penales (art. 10 RGPD):** relativos a condenas e infracciones.
 - Solo pueden tratarse por **autoridad competente** o con **base legal expresa**.
 - Ejemplo prohibido: comentar antecedentes penales de un candidato en un grupo de RRHH.

6.4. Juicio de interés legítimo (LIA) y documentación

Cuando se base en interés legítimo, la organización deberá realizar un **Legitimate Interest Assessment (LIA)** documentado, con las siguientes fases:

1. **Identificación del interés legítimo:** finalidad empresarial u organizativa concreta.
2. **Necesidad:** analizar si existen medios menos intrusivos que la mensajería instantánea.
3. **Equilibrio:** valorar el impacto en la privacidad de los interesados y si existen salvaguardas suficientes (información clara, posibilidad de oponerse, configuración de privacidad).

4. **Documentación:** conservar un registro de la evaluación como prueba de cumplimiento.
5. **Revisión periódica:** actualizar la LIA en función de cambios en tecnología, normativa o finalidad del grupo.

7. Roles y Responsabilidades

La correcta gestión de grupos de mensajería instantánea requiere definir de forma clara los **roles involucrados en el tratamiento de datos** y sus **responsabilidades específicas**.

7.1. Responsable del Tratamiento

Es **MAQUICER SL**, representada por su órgano de dirección competente.

Funciones:

- Determinar las finalidades y medios del tratamiento.
- Aprobar esta Política y garantizar su aplicación.
- Designar a los **administradores de grupo** y supervisar su actividad.
- Adoptar las medidas técnicas y organizativas adecuadas (art. 24 y 32 RGPD).
- Velar por que los grupos no se usen para fines distintos a los autorizados.

7.2. Encargados del Tratamiento

Son los **proveedores tecnológicos** que prestan servicios de mensajería a la organización (p. ej. Microsoft Teams, Slack, Google Chat) o terceros que gestionen operativamente los grupos por encargo de la entidad.

Obligaciones:

- Estar vinculados mediante un **Contrato de Encargo del Tratamiento** conforme al art. 28 RGPD.
- Garantizar seguridad, confidencialidad y cumplimiento de la normativa.
- No subcontratar sin autorización del Responsable.
- Notificar incidentes de seguridad sin dilación indebida.

⚠ Nota: cuando se usen plataformas de mensajería que actúan como **corresponsables** (ej. WhatsApp, Telegram), deberán valorarse las condiciones contractuales y políticas de privacidad de dichos servicios.

7.3. Administradores de Grupo

Empleados o colaboradores internos designados expresamente para gestionar grupos de mensajería.

Responsabilidades específicas:

- Crear y configurar los grupos previa autorización.
- Incorporar y eliminar miembros según los criterios establecidos.
- Garantizar que todos los miembros reciben la cláusula informativa.
- Velar por el cumplimiento de las normas de uso y seguridad.
- Escalar incidencias al de Cumplimiento y Seguridad de la Información.
- Proceder a la **supresión del grupo** una vez alcanzada la finalidad.

Los administradores actúan bajo instrucciones del Responsable del Tratamiento.

7.4. Miembros del Grupo

Todo usuario que participe en un grupo de mensajería creado por la entidad.

Obligaciones:

- Usar el grupo exclusivamente para la finalidad prevista.
- Respetar la confidencialidad de la información compartida.
- Abstenerse de difundir datos personales sin autorización o innecesarios.
- No reenviar información a terceros no autorizados ni realizar capturas o difusiones externas.
- Notificar inmediatamente cualquier incidencia de seguridad o vulneración de la política.

8. Reglas de Creación, Uso y Administración

Los grupos de mensajería instantánea creados bajo el marco de esta Política deben cumplir con las siguientes reglas organizativas y técnicas.

8.1. Criterios para la creación de grupos (finalidad y autorización)

Todo grupo debe tener una **finalidad concreta, legítima y documentada** (ej. coordinación de un proyecto, gestión de incidencias, comunicación de emergencias).

- **La creación de un grupo debe ser aprobada por:**
 - El **Responsable del Área** (por motivos operativos).
 - El **Área de Cumplimiento**, cuando se trate de grupos con datos sensibles o externos.
- El nombre del grupo debe reflejar claramente su finalidad (ejemplo: “*Soporte Técnico – Turno Noche*”).
- Está prohibido crear grupos para fines personales, difusos o que no tengan relación con la actividad de **MAQUICER SL**.

8.2. Procedimiento de alta y baja de miembros

La inclusión de un miembro debe estar **justificada** y vinculada a la finalidad del grupo.

- **Los nuevos miembros deben recibir:**
 - La **cláusula informativa de privacidad** (o consentimiento, en su caso).
 - Un **resumen de las normas de uso (Manual de Uso)**.
- **La baja de miembros debe realizarse de inmediato cuando:**
 - Finalice su relación laboral o contractual.
 - Cambien sus funciones y dejen de necesitar acceso al grupo.
- El administrador debe actualizar periódicamente la lista de miembros.

8.3. Normas de comportamiento y contenido permitido

Los grupos deben usarse **únicamente** para fines relacionados con la finalidad declarada.

- **Está permitido compartir:**
 - Comunicaciones de trabajo relevantes.

- Documentos estrictamente necesarios.
- Avisos internos y mensajes de coordinación.
- **Está prohibido compartir:**
 - Información irrelevante o personal no vinculada al trabajo.
 - Imágenes, vídeos o audios de carácter privado o sensible.
 - Contenidos ofensivos, discriminatorios o no profesionales.
- El lenguaje debe ser **profesional, respetuoso y no ambiguo**.

8.4. Prohibiciones específicas

- Difundir **datos sensibles (art. 9 RGPD)** o **datos penales (art. 10 RGPD)** salvo autorización expresa y documentada.
- Utilizar grupos para enviar **publicidad o comunicaciones comerciales** sin base jurídica adecuada (consentimiento, interés legítimo ponderado).
- Compartir credenciales, contraseñas o información de seguridad.
- Grabar, capturar o reenviar conversaciones sin autorización.
- Usar el grupo como **sustituto** de los sistemas oficiales de archivo, CRM, ERP o gestor documental.

8.5. Mensajería instantánea como canal complementario

- Los grupos se consideran un **canal de comunicación complementario**.
- La **información oficial y vinculante** debe registrarse en los sistemas corporativos habilitados (correo corporativo, intranet, ERP, gestor documental).
- La mensajería instantánea no sustituye:
 - El sistema de gestión documental.
 - Los registros de entradas/salidas oficiales.
 - Los procedimientos formales de notificación.

9. Transparencia e Información a los Interesados

El uso de grupos de mensajería instantánea requiere que todos los miembros sean informados de forma clara, concisa y accesible sobre el tratamiento de sus datos personales.

9.1. Capas informativas y avisos de privacidad

Se aplicará el principio de **información por capas**:

- **Primera capa (información básica, al acceder al grupo):**
 - Responsable del tratamiento.
 - Finalidad principal del grupo.
 - Base jurídica.
 - Enlaces a la política completa de privacidad.
- **Segunda capa (información detallada, disponible mediante enlace o documento adjunto):**
 - Datos tratados.
 - Destinatarios (incluyendo transferencias internacionales si la plataforma las implica).
 - Plazos de conservación.
 - Derechos de los interesados y cómo ejercerlos.
 - Datos de contacto de la entidad

9.2. Registro y evidencia de la información proporcionada

- El Responsable del Tratamiento deberá poder **acreditar** que los interesados fueron informados:
 - Guardando copia del mensaje de invitación/bienvenida con la cláusula.
 - Archivando consentimientos obtenidos cuando proceda.
 - Conservando evidencias de entrega de documentos o accesos web.
- Se recomienda que el **administrador de grupo** registre la confirmación de que se ha comunicado la información de privacidad a todos los miembros.

10. Seguridad y Confidencialidad

La seguridad y la confidencialidad constituyen pilares esenciales en la gestión de grupos de mensajería instantánea. Se aplicarán las siguientes medidas:

10.1. Configuración de privacidad

- Se priorizará el uso de plataformas que permitan **ocultar números de teléfono** o limitar la visibilidad a miembros autorizados.
- En caso de que la plataforma exponga el número de teléfono de los miembros (ej. WhatsApp), deberá:
 - Informarse previamente a los interesados.
 - Usarse únicamente cuando la base jurídica lo legitime y no existan alternativas menos intrusivas.
- Se fomentará el uso de **alias o identificadores corporativos** en lugar de números personales.

10.2. Cifrado de extremo a extremo y medidas técnicas

- Solo se podrán utilizar plataformas que garanticen un nivel de **cifrado de extremo a extremo** o cifrado robusto en tránsito y reposo.
- El Responsable del Tratamiento debe verificar periódicamente la **política de seguridad del proveedor**.
- En dispositivos:
 - Activar bloqueo de pantalla con PIN o biometría.
 - Usar cifrado del dispositivo.
 - Deshabilitar copias de seguridad no cifradas en la nube.

10.3. Gestión de dispositivos y accesos

- Se priorizará el uso de **dispositivos corporativos gestionados** (MDM).
- En casos de BYOD (Bring Your Own Device: Dispositivos personales), será obligatorio:
 - Separar perfiles personales y corporativos.
 - Instalar software de gestión corporativa (si procede).
 - Configurar políticas de borrado remoto.

- Los accesos estarán limitados a los miembros autorizados, con incorporación y baja inmediata según cambios de rol.

10.4. Prevención de fugas de información

- Queda prohibido realizar capturas de pantalla, grabaciones, reenvíos o descargas no autorizadas de mensajes y archivos compartidos.
- Se sensibilizará a los miembros sobre los riesgos de compartir información fuera del grupo.
- Cuando la plataforma lo permita, se configurarán restricciones de reenvío y descarga.

10.5. Conservación y eliminación de mensajes/documentos

- Los grupos no constituyen un repositorio oficial de almacenamiento.
- La información relevante deberá trasladarse a los **sistemas corporativos oficiales** (ERP, CRM, gestor documental, intranet).
- Procedimientos:
 - Borrado periódico de mensajes y archivos obsoletos.
 - Eliminación segura de grupos finalizados.
 - Supresión inmediata de mensajes enviados por error con datos personales, siempre que la plataforma lo permita.

11. Derechos de los Interesados

El Responsable del Tratamiento garantizará en todo momento el ejercicio de los **derechos de los interesados** en el contexto de los grupos de mensajería instantánea, de acuerdo con los arts. 15 a 22 del RGPD y el Título II de la LOPDGDD.

10.1. Procedimiento para ejercer derechos

Los interesados podrán ejercer los siguientes derechos:

- **Acceso:** conocer qué datos personales suyos se tratan en el grupo.
- **Rectificación:** corregir información inexacta o desactualizada.
- **Supresión (“derecho al olvido”):** solicitar la eliminación de sus datos cuando no sean necesarios o se hayan tratado indebidamente.
- **Limitación del tratamiento:** restringir el uso de sus datos en determinadas circunstancias.
- **Oposición:** negarse al tratamiento de sus datos basado en interés legítimo.
- **Portabilidad:** recibir sus datos en un formato estructurado y transmitirlos a otro responsable, en los casos legalmente aplicables.

Canales habilitados:

- Dirección de correo electrónico de la entidad: **info@maquicer.com**
- Dirección postal de la entidad: **Apartado de correos, 36. 12110, Alcora (Castellón)**
- Mensaje privado al Administrador del Grupo

El procedimiento deberá ser **gratuito, sencillo y documentado**, con resolución en un plazo máximo de **un mes**, ampliable a dos en casos complejos, notificando siempre al interesado.

10.2. Gestión de solicitudes dentro de los grupos

- Las solicitudes de ejercicio de derechos **no deben resolverse dentro del grupo**, sino a través de los canales oficiales de la entidad.
- El administrador de grupo que reciba una petición deberá:
 1. Redirigir inmediatamente al interesado al canal oficial.
 2. Informar al Área de Cumplimiento de la solicitud recibida (en su caso)

- En caso de que la solicitud implique la **eliminación de mensajes o salida del grupo**, el administrador actuará siguiendo instrucciones del Área de Cumplimiento y del Responsable del Tratamiento.

10.3. Limitaciones y excepciones

El ejercicio de los derechos podrá ser limitado cuando:

- Exista una **obligación legal** de conservar los datos.
- Sea necesario para el ejercicio o defensa de **reclamaciones legales**.
- La supresión afecte a derechos de terceros o a la integridad de evidencias en procedimientos internos o judiciales.

En todo caso, estas limitaciones deberán ser **debidamente justificadas y documentadas**.

11. Evaluación de Impacto y Análisis de Riesgos

El uso de grupos de mensajería instantánea puede conllevar **riesgos elevados para los derechos y libertades de los interesados**. El Responsable del Tratamiento deberá realizar un análisis sistemático de dichos riesgos y, cuando proceda, una **Evaluación de Impacto en Protección de Datos (EIPD)** conforme al artículo 35 RGPD.

11.1. Identificación de riesgos asociados a la mensajería instantánea

Principales riesgos que deben considerarse:

- **Exposición de datos de contacto** (ej. números de teléfono visibles entre miembros).
- **Incorporación indebida** de miembros no autorizados.
- **Difusión no controlada** de mensajes o documentos (reenvíos, capturas).
- **Falta de control de dispositivos personales** (BYOD sin cifrado o medidas de seguridad).
- **Transferencias internacionales** de datos (cuando los servidores estén fuera del EEE sin garantías adecuadas).
- **Uso indebido de datos sensibles o penales** en grupos no autorizados.
- **Conservación excesiva** de mensajes o ficheros.
- **Brechas de seguridad** derivadas de pérdida o robo de dispositivos.

11.2. Valoración de probabilidad e impacto

El análisis de riesgos deberá contemplar:

- **Probabilidad de ocurrencia:** alta, media, baja.
- **Impacto en los derechos y libertades:** leve, significativo, grave.
- **Nivel de riesgo resultante:** combinación de probabilidad + impacto.

Ejemplo:

- *Exposición de números de teléfono entre miembros externos:* probabilidad alta / impacto medio → riesgo alto.
- *Reenvío no autorizado de mensajes internos:* probabilidad media / impacto significativo → riesgo alto.

11.3. Medidas de mitigación y controles aplicados

Para cada riesgo identificado deberán aplicarse medidas específicas:

- **Exposición de datos de contacto:** usar plataformas con alias corporativos, informar previamente.
- **Incorporación indebida:** procedimiento de altas y bajas controlado por administradores.
- **Difusión no controlada:** formación a usuarios, prohibición expresa de reenvíos.
- **BYOD inseguro:** exigir cifrado, PIN y borrado remoto.
- **Transferencias internacionales:** verificar cláusulas contractuales tipo o decisiones de adecuación.
- **Datos sensibles:** prohibición expresa salvo autorización documentada.
- **Conservación excesiva:** borrado periódico de mensajes y cierre de grupos.

11.4. Supuestos que requieren una EIPD

Será obligatorio realizar una **EIPD** en los siguientes casos:

- Uso de mensajería instantánea para tratar **datos sensibles** (salud, religión, etc.).
- Inclusión de **menores de edad** en los grupos.
- Comunicación de datos de **gran número de interesados**.
- Transferencias internacionales de datos sin garantías adecuadas.
- Uso de mensajería como **canal principal de relación con clientes o usuarios**.

La EIPD deberá:

1. Describir detalladamente las operaciones de tratamiento.
2. Evaluar necesidad y proporcionalidad del uso de mensajería.
3. Analizar riesgos para los derechos y libertades.
4. Establecer medidas de mitigación.
5. Consultar a la AEPD cuando el riesgo residual siga siendo alto.

12. Brechas de Seguridad y Notificación de Incidentes

La gestión de incidentes de seguridad es esencial para garantizar la resiliencia organizativa y el cumplimiento del RGPD (arts. 33 y 34). En el contexto de grupos de mensajería, se aplicarán las siguientes directrices.

12.1. Tipos de incidentes en mensajería instantánea

Algunos ejemplos de incidentes relevantes:

- **Accesos no autorizados:** inclusión de personas no autorizadas en un grupo.
- **Pérdida o robo de dispositivos** con acceso a los grupos.
- **Difusión indebida:** reenvío de mensajes, capturas de pantalla o archivos a terceros.
- **Exposición de datos sensibles:** publicación de información de salud, afiliación sindical u otros datos especiales sin autorización.
- **Errores humanos:** envío de mensajes a un grupo equivocado.
- **Fugas por terceros proveedores:** fallos de seguridad en la propia plataforma de mensajería.

12.2. Protocolo de detección, comunicación y respuesta

1. **Detección del incidente:** cualquier miembro o administrador debe reportar de inmediato la sospecha de una brecha.
2. **Comunicación interna:**
 - Aviso inmediato al **Administrador del grupo** y al **Área de Seguridad / Área de Cumplimiento**.
 - Canal de reporte: info@maquicer.com – 964 328 338
3. **Contención inmediata:**
 - Retirar al miembro no autorizado.
 - Eliminar mensajes o archivos erróneos (cuando la plataforma lo permita).
 - Bloquear accesos en caso de pérdida de dispositivo (borrado remoto).
4. **Análisis y evaluación:** el Área de Cumplimiento y Seguridad determinarán el alcance, impacto y riesgo para los derechos de los interesados.
5. **Registro del incidente:** se documentará en el **Registro de Incidentes de Seguridad**, incluyendo causa, impacto, medidas adoptadas y responsable.

12.3. Notificación a la AEPD y a los interesados

- Si el incidente supone un **riesgo para los derechos y libertades de las personas**, el Responsable del Tratamiento deberá notificar a la AEPD en un plazo máximo de **72 horas** desde que tenga conocimiento.
- Cuando la brecha suponga un **alto riesgo** para los interesados, se deberá comunicar también directamente a los afectados de forma clara y sencilla.
- El Área de Cumplimiento evaluará si concurren las condiciones para notificar y coordinará la comunicación.

13. Conservación y Supresión de Grupos y Mensajes

El tratamiento de datos personales en grupos de mensajería debe respetar el **principio de limitación del plazo de conservación** (art. 5.1.e RGPD). Los mensajes, archivos y grupos no deben mantenerse más allá del tiempo estrictamente necesario para cumplir la finalidad prevista.

13.1. Plazos de conservación de mensajes y ficheros

- Los **mensajes y documentos compartidos en grupos** no constituyen un archivo oficial de la organización.
- La información con valor probatorio o contractual debe trasladarse a los **sistemas corporativos oficiales** (ERP, CRM, gestor documental).
- Los plazos de conservación se ajustarán a:
 - **Duración del proyecto o servicio** vinculado al grupo.
 - **Obligaciones legales específicas** (ejemplo: normativa fiscal, laboral o sanitaria).
 - En ausencia de obligación legal, los mensajes deberán ser eliminados en un **plazo máximo de 24 horas, 7 o 90 días** tras la finalización de la finalidad del grupo (según establezca el administrador del grupo).

13.2. Supresión segura de grupos

- Una vez cumplida la finalidad, el **administrador** procederá a:
 - Notificar a los miembros el cierre del grupo.
 - Eliminar de manera segura los mensajes y archivos (cuando la plataforma lo permita).
 - Proceder a la **eliminación total del grupo**.
- Queda prohibido mantener grupos “inactivos” con datos personales almacenados sin finalidad actual.
- La supresión debe registrarse en el **Registro de Grupos de Mensajería**, indicando fecha y responsable del cierre.

13.3. Evidencias y registros de eliminación

- El Responsable del Tratamiento mantendrá **evidencias documentales** de la eliminación:
 - Captura o exportación del aviso de cierre.
 - Registro del administrador que ejecutó la supresión.
 - Fecha y motivo de cierre.
- Cuando la plataforma no permita eliminar mensajes antiguos (ejemplo: WhatsApp), se documentará la limitación técnica y se aplicarán medidas compensatorias (ej. borrado periódico de chats en dispositivos).

14. Difusión y Concienciación

El éxito en la protección de datos en grupos de mensajería instantánea depende no solo de las medidas técnicas, sino también del **comportamiento responsable de los usuarios**. Por ello, la organización adopta las siguientes medidas:

14.1. Guías prácticas de uso seguro de mensajería

La entidad elaborará **guías rápidas** o **manuales prácticos** para los usuarios, que incluirán:

- Buenas prácticas (ej. no compartir datos sensibles, usar alias corporativos).
- Prohibiciones (ej. reenvíos a terceros, uso personal de grupos corporativos).
- Recomendaciones técnicas (ej. bloqueo de pantalla, uso de cifrado, desactivación de copias en la nube no seguras).
- Ejemplos de situaciones correctas e incorrectas de uso.

14.2. Comunicación interna de la política

- La presente Política será publicada en la **intranet corporativa** o medio equivalente.
- La invitación para unirse al grupo incluirá un **enlace a la Política de Privacidad, a la Política de Protección de Datos y al Manual de Uso para Miembros**.
- Periódicamente (al menos una vez al año) se realizarán **campañas de recordatorio** mediante correo electrónico, cartelería interna o webinars.
- Se fomentará la **cultura de responsabilidad compartida**, sensibilizando a los miembros de que la seguridad depende del comportamiento de cada usuario.

15. Supervisión, Auditoría y Actualización

El cumplimiento de esta Política requiere un sistema estructurado de **seguimiento, verificación y revisión periódica**, alineado con el principio de **responsabilidad proactiva** (art. 24 RGPD).

15.1. Mecanismos de seguimiento y control

- El **Responsable del Tratamiento**, con apoyo del área de Cumplimiento y del área de Seguridad de la Información, deberá implantar mecanismos de control, tales como:
 - Registro actualizado de grupos creados, administradores y finalidades.
 - Verificación periódica de la correcta aplicación de altas y bajas.
 - Monitorización de configuraciones de seguridad en las plataformas utilizadas.
 - Supervisión de incidentes y reclamaciones relacionadas con grupos de mensajería.

15.2. Auditorías periódicas

- La entidad realizará **auditorías internas o externas** para verificar la adecuación y eficacia de esta Política.
- Frecuencia: al menos **una vez cada 1 años**, o antes si concurren cambios relevantes (nuevas plataformas, incidentes graves, cambios normativos).
- Objetivos de la auditoría:
 - Verificar cumplimiento de las reglas de creación, uso y supresión de grupos.
 - Evaluar eficacia de las medidas de seguridad y confidencialidad.
 - Revisar evidencias de información a los interesados y de formación impartida.
 - Comprobar la trazabilidad en el registro de incidentes y brechas.
- Los resultados se documentarán en un **Informe de Auditoría**, con medidas correctivas y plazos de implementación.

15.3. Actualización de la política en función de cambios normativos o tecnológicos

- La presente Política deberá revisarse y, en su caso, actualizarse:

- Cuando se aprueben **nuevas normas** en materia de protección de datos o comunicaciones electrónicas.
- Cuando la AEPD o el EDPB emitan **nuevas guías o resoluciones** aplicables al uso de mensajería.
- Cuando la entidad adopte **nuevas plataformas tecnológicas** o modifique las ya existentes.
- Tras incidentes graves que evidencien debilidades en la aplicación de la política.
- El **Área de Cumplimiento** será responsable de proponer modificaciones y someterlas a aprobación de la Dirección.
- Se mantendrá un **histórico de versiones** con registro de cambios, fechas y responsables de su validación.

16. Anexos

Los anexos de esta Política recogen **modelos, herramientas y recursos prácticos** que facilitan la correcta implementación de las medidas establecidas en las secciones anteriores.

Los anexos inherentes a esta Política son:

- **ANEXO I.** Modelos de Cláusulas Informativas para Grupos de Mensajería
- **ANEXO II.** Modelo de Consentimiento para inclusión en Grupos de Mensajería
- **ANEXO III.** Política de Privacidad para Grupos de Mensajería
- **ANEXO IV.** Manual de Uso para Miembros del Grupo de Mensajería
- **ANEXO V.** Procedimiento de Implementación y Configuración de WhatsApp