DECLARATORIA FORMAL

Declaratoria de seguridad, privacidad y transparencia operativa

Documento informativo para clientes, socios y responsables de decisión sobre el uso seguro de soluciones con inteligencia artificial de Control A Group.

Principio rector: Control A no solicita confianza ciega. Establece límites, revisión humana, separación de información, canales verificables y responsabilidades claras.

Alcance: aplica a asistentes, automatizaciones, paneles, documentos, reportes, flujos de atención y operaciones digitales implementadas para clientes.

Control A Group
You dream it, we build it

Versión formal
31 de julio de 2026

1. Objeto de la declaratoria

> Esta declaratoria explica, en términos formales y comprensibles, cómo Control A Group protege la información de sus clientes y cómo define límites operativos para el uso responsable de inteligencia artificial.

Control A Group desarrolla e implementa soluciones digitales y agentes de inteligencia artificial orientados a mejorar atención, productividad, organización, generación de entregables, seguimiento comercial y operación interna. Estas soluciones pueden interactuar con usuarios, clientes, colaboradores o responsables del negocio, siempre bajo un marco de autorización, control y revisión.

El objetivo de este documento es dejar una posición clara: la tecnología puede apoyar el trabajo, pero no debe sustituir el criterio humano en decisiones sensibles ni obligar al cliente a confiar en mensajes, audios, videos o capturas sin verificación.

Declaración principal. Control A Group opera bajo el principio de información autorizada, separación por cliente, control de accesos, revisión humana, canales verificables y límites explícitos para decisiones sensibles.

2. Principios de seguridad y privacidad

MINIMIZACIÓN

Se debe usar solo la información necesaria para cumplir el servicio acordado, evitando recolectar datos innecesarios.

AUTORIZACIÓN

La solución trabaja con información entregada, aprobada o habilitada por el cliente dentro del alcance definido.

SEPARACIÓN

La información de un cliente no debe mezclarse, reutilizarse ni exponerse frente a otro cliente o proyecto.

CONTROL HUMANO

Las decisiones económicas, contractuales, de acceso, pago o reputación requieren intervención o confirmación humana.

3. Información utilizada por Control A

Según el proyecto contratado, Control A puede trabajar con datos como productos, servicios, horarios, precios, políticas comerciales, preguntas frecuentes, documentos internos autorizados, conversaciones, solicitudes, reportes, indicadores operativos y registros necesarios para prestar el servicio.

La finalidad de uso es operativa: responder mejor, ordenar solicitudes, asistir ventas, producir documentos, generar reportes, apoyar seguimiento, resumir información y dar visibilidad a la gestión del negocio.

3.1 Información que no debe solicitarse sin necesidad

- Contraseñas personales, códigos de verificación, llaves privadas o credenciales bancarias.
- Datos financieros sensibles que no formen parte del alcance aprobado.
- Información personal o médica innecesaria para la atención contratada.
- Documentos privados que no sean requeridos para el servicio específico.

4. Compromisos expresos de privacidad

Compromiso	Declaración
No venta de datos	Control A no vende la información de sus clientes, usuarios o conversaciones.
No mezcla entre clientes	La información de una empresa no se usa para operar, responder o entrenar el servicio de otra empresa.
No publicación de datos internos	La información interna del negocio no debe mostrarse en páginas públicas, demos abiertas o documentos externos sin autorización.
No exposición de credenciales	Claves, tokens, accesos técnicos y configuraciones sensibles deben mantenerse fuera del frontend, documentos públicos y pantallas visibles.
Uso limitado al servicio	La información se utiliza para cumplir la finalidad operativa acordada con el cliente.

5. Separación por cliente, proyecto y usuario

Cada cliente debe operar con su propia información, usuarios, registros, permisos y contexto. La separación no es un detalle técnico: es una condición esencial de confianza.

Cuando una plataforma o infraestructura atiende a más de un cliente, deben existir mecanismos de aislamiento lógico, permisos y control para impedir accesos cruzados, confusión de contextos o exposición accidental.

6. Accesos, permisos y responsabilidades

Los accesos a paneles, reportes, conversaciones, archivos, métricas o datos operativos deben estar reservados a usuarios autorizados por el cliente. Cada negocio puede definir responsables, niveles de permiso y criterios de revisión.

- Los usuarios deben evitar compartir contraseñas o accesos personales por mensajería informal.
- Los responsables del negocio deben revisar periódicamente quién tiene acceso a información sensible.
- Las credenciales técnicas deben quedar protegidas y no deben circular en chats, capturas, documentos abiertos o páginas públicas.
- Cuando un acceso deje de ser necesario, debe retirarse o actualizarse.

7. Uso responsable de inteligencia artificial

La inteligencia artificial puede atender, clasificar, resumir, responder, organizar, generar entregables y apoyar operaciones. Sin embargo, debe operar dentro de límites conocidos y con información autorizada.

> **Límite operativo.** La IA no reemplaza a los responsables del negocio. Ayuda a ejecutar y ordenar, pero las decisiones sensibles siguen bajo control humano.

Los casos fuera de política, reclamos, descuentos excepcionales, devoluciones, cambios de cuentas bancarias, decisiones económicas, instrucciones contractuales o solicitudes ambiguas deben escalarse a una persona autorizada.

8. Control humano primero

Control A considera indispensable que el cliente mantenga control sobre decisiones relevantes. Por ello, se recomienda aplicar revisión humana obligatoria en los siguientes supuestos:

Tipo de acción	Regla recomendada
Pagos, transferencias o cobros	No ejecutar sin confirmación de una persona autorizada y canal verificable.
Contratos o compromisos comerciales	No aprobar ni modificar sin revisión del responsable del negocio.
Cambio de cuenta bancaria	Tratar como alerta de alto riesgo hasta confirmar por canal oficial.
Descuentos, devoluciones o compensaciones	Escalar si excede la política aprobada.
Datos sensibles o credenciales	No solicitar ni recibir por canales informales.
Reclamos o crisis reputacional	Derivar a un responsable humano antes de responder en nombre de la empresa.

9. Verificación antes de actuar

Un mensaje convincente no equivale a autorización. Un video, audio, captura de pantalla, enlace reenviado o texto con tono urgente no debe considerarse prueba suficiente de identidad.

Antes de realizar pagos, entregar accesos, cambiar condiciones, aprobar contratos o compartir información sensible, el cliente debe verificar por canales oficiales: dominio corporativo, correo institucional, número autorizado, contrato firmado o confirmación directa de un responsable identificado.

> Si una instrucción parece urgente, secreta, demasiado rentable, emocionalmente presionante o difícil de verificar, debe detenerse hasta confirmar su autenticidad.

10. Transparencia frente a promesas falsas

Control A Group no ofrece inversiones, no promete multiplicar dinero, no solicita pagos bajo promesa de retornos extraordinarios y no pide actuar únicamente por confianza en una imagen, audio, video o mensaje reenviado.

Si un tercero usa el nombre, marca, imagen, voz, firma o identidad visual de Control A para prometer ganancias rápidas, pedir dinero, exigir urgencia o solicitar datos sensibles, el receptor debe verificar directamente con Control A por canales oficiales antes de actuar.

11. Infraestructura y protección técnica

Según el alcance de cada proyecto, Control A puede aplicar medidas como conexión segura HTTPS, usuarios con permisos diferenciados, almacenamiento no público, validación del lado servidor, respaldos, registros de actividad y protección de credenciales.

La base de datos y los archivos internos no deben quedar expuestos como descargas públicas. Las llaves, tokens y configuraciones sensibles deben mantenerse en entornos protegidos y nunca dentro de interfaces visibles para usuarios finales.

12. Registro, trazabilidad y revisión

Las conversaciones, entregables, acciones relevantes y derivaciones pueden quedar registradas para permitir revisión posterior. Esta trazabilidad ayuda al negocio a entender qué ocurrió, qué respondió el asistente, qué datos utilizó y cuándo fue necesario escalar a una persona.

El cliente puede solicitar explicación sobre qué información usa el sistema, qué puede responder, qué no debe responder y quién tiene acceso a los datos dentro del alcance contratado.

13. Responsabilidades del cliente

La seguridad también depende de que el cliente mantenga información actualizada, responsables claros y políticas internas conocidas. Control A puede proveer tecnología y criterios de protección, pero el negocio conserva responsabilidad sobre la veracidad de sus datos, la aprobación de decisiones y el uso adecuado de accesos.

- Mantener actualizada la información autorizada que usará el asistente.
- Definir precios, horarios, políticas, responsables y límites de respuesta.
- Revisar decisiones sensibles y casos fuera de política.
- No compartir contraseñas, códigos ni accesos personales.
- Confirmar por canales oficiales pagos, contratos, inversiones, cambios de cuenta bancaria o entrega de datos sensibles.

14. Señales de alerta y conducta esperada

Señal de alerta	Conducta recomendada
Prometen multiplicar dinero rápido.	No actuar. Verificar por canal oficial.
Piden pago urgente, secreto o fuera del procedimiento normal.	Detenerse y confirmar con una persona responsable.
Envían video, audio o captura como única prueba.	No considerarlo prueba suficiente.
Piden claves, accesos o códigos por chat informal.	No enviar. Usar canales autorizados.
Cambian una cuenta bancaria o condición de pago.	Confirmar por canal oficial antes de cualquier transferencia.
El mensaje presiona con miedo, urgencia o secreto.	Pausar la acción y solicitar verificación directa.

15. Compromiso institucional

Control A Group promueve el uso de inteligencia artificial como una herramienta de productividad, atención y organización, no como un reemplazo irresponsable del criterio humano ni como una excusa para opacidad.

Compromiso final. Operar con información autorizada, límites claros, separación por cliente, trazabilidad, revisión humana y canales verificables. La seguridad no se basa en creer: se basa en controlar, revisar y confirmar.

16. Declaratoria para clientes y terceros

Para efectos informativos y comerciales, Control A Group declara que sus soluciones deben implementarse bajo criterios de seguridad, privacidad, transparencia, control humano y responsabilidad operativa. Esta declaratoria no sustituye contratos específicos, acuerdos de confidencialidad, políticas de privacidad, términos de servicio ni obligaciones legales aplicables a cada cliente o industria; los complementa como una declaración pública de criterio y estándar operativo.

Cuando un proyecto requiera tratamiento de datos especialmente sensibles, integraciones financieras, información médica, datos de menores, credenciales críticas, obligaciones regulatorias o procesos de alto impacto, el alcance deberá definirse con controles adicionales y aprobación expresa de los responsables correspondientes.

Control A Group
Declaratoria de seguridad, privacidad y transparencia operativa
Versión formal · 31 de julio de 2026

Principio rector
Información autorizada. Control humano. Canales verificables. Separación por cliente.