

POLÍTICA DE PRIVACIDAD

ASSC Conexión Remota

Aplicación ASSC Connect · Cliente y Soporte

**ADMINISTRACIÓN Y SERVICIOS
SISTEMAS COLOMBIA S.A.S.**
NIT 901.926.771-3

Versión 1.0 · Documento preparado el 17 de septiembre de 2026

Aplicación: desde su adopción y publicación por ASSC SAS

Esta política explica qué datos personales pueden tratarse al instalar y utilizar ASSC Conexión Remota, para qué se emplean, quiénes intervienen y cómo ejercer los derechos de privacidad. Comprende la atención remota, el control del equipo y las funciones de archivos autorizadas por el cliente.

El acceso desatendido permite iniciar conexiones con las credenciales habilitadas sin que una persona pulse «Aceptar» en cada sesión. Por ello requiere autorización previa, información clara y la posibilidad de retirarlo. Que la aplicación se inicie con Windows no autoriza al técnico a revisar libremente la información del equipo.

Canal para protección de datos: cliente@sistemascolombia.com

Descarga y soporte: <https://www.sistemascolombia.com/soporte>

Este documento complementa la Política de Tratamiento y Protección de Datos Personales de ASSC SAS. Su publicación no sustituye la autorización del titular cuando sea exigible.

Página 1 de 10

1 Identificación y alcance

Responsable y canales de atención

ADMINISTRACIÓN Y SERVICIOS SISTEMAS COLOMBIA S.A.S., NIT 901.926.771-3, con domicilio en Bogotá D.C., es responsable de los datos de sus clientes, contactos y solicitudes de soporte respecto de los cuales determina las finalidades del tratamiento. Su representante legal es Darwin Parra Velandia. Atención al Cliente recibe y coordina las solicitudes de privacidad.

Correo: cliente@sistemascolombia.com. **WhatsApp:** +57 300 174 3544. **Dirección de notificaciones:** Carrera 13 # 61-47, Centro Comercial Chapicentro, Bogotá D.C., Colombia. **Sitio institucional:** <https://www.sistemascolombia.com>. Estos canales corresponden al cuerpo de la política general de ASSC; la información gráfica del membrete se conserva como referencia corporativa.

Personas y operaciones comprendidas

La política se aplica a usuarios que reciben asistencia, técnicos autorizados, contactos de empresas y personas cuyos datos puedan estar visibles en un equipo durante el soporte. Cubre recolección, consulta, uso, almacenamiento, transmisión, circulación restringida y supresión, cuando efectivamente ocurran en la prestación del servicio.

Tratamiento por cuenta de empresas clientes

Cuando ASSC acceda a bases de datos de una empresa cliente únicamente para atender sus instrucciones, actuará como encargado en los términos del acuerdo aplicable. El cliente conserva la responsabilidad por sus finalidades, por informar a sus titulares y por disponer de las autorizaciones o excepciones legales correspondientes. Ser dueño o administrador del equipo no otorga por sí solo autorización ilimitada sobre datos de terceros.

Marco de aplicación

Se observan los artículos 15 y 20 de la Constitución Política, la Ley 1581 de 2012 y su reglamentación compilada en el Decreto 1074 de 2015, junto con las instrucciones de la Superintendencia de Industria y Comercio que resulten aplicables. Rigen los principios de finalidad, libertad, transparencia, calidad, acceso restringido, seguridad y confidencialidad.

2 Datos tratados y finalidades

Identificación y atención

Pueden tratarse el nombre y los datos de contacto del solicitante, empresa, cargo cuando resulte pertinente, descripción del problema, comunicaciones de soporte y evidencia de la autorización. Se utilizan para verificar a quién se atiende, coordinar la intervención, responder solicitudes y documentar el servicio. No se exige un documento de identidad de manera indiscriminada para toda conexión.

Datos técnicos del equipo y de la sesión

El ID de conexión y los datos técnicos disponibles, como nombre del equipo, sistema operativo, versión de la aplicación, dirección IP, estado de conexión y registros de diagnóstico, pueden ser necesarios para establecer o resolver una conexión. Las fechas, duración, acciones y resultado del soporte podrán documentarse según las funciones habilitadas y el registro de atención. Esta política no afirma que todas esas funciones estén activas en cada instalación.

Contenido visible o utilizado durante el soporte

El técnico puede ver la pantalla y, según los permisos, interactuar con aplicaciones, archivos, nombres de carpetas, mensajes y datos que el usuario tenga abiertos. Los archivos transferidos y el portapapeles, si se utiliza su sincronización, pueden contener información personal. Ver información durante una sesión constituye tratamiento aunque no se descargue una copia.

Finalidades permitidas

Los datos se emplearán para prestar el soporte solicitado, diagnosticar y corregir fallas, realizar mantenimiento autorizado, instalar o actualizar programas, administrar el acceso acordado, proteger la operación, atender incidentes y cumplir deberes legales. La información disponible en el equipo no podrá aprovecharse para publicidad, venta de bases, contacto comercial ajeno al servicio ni elaboración de perfiles personales.

Solo se solicitará y conservará la información necesaria. Las acciones sobre archivos o sistemas deberán guardar relación con el caso y los permisos otorgados. La instalación de esta aplicación no implica inscripción automática en todos los servicios, nubes o plataformas de ASSC.



3 Autorización y acceso desatendido

Autorización informada

Antes del tratamiento que la requiera, ASSC deberá obtener autorización previa, expresa e informada por un medio que permita conservar y consultar su evidencia. Se informará el alcance de la asistencia, los permisos solicitados, las finalidades, los canales de atención y la manera de retirar el acceso. La mera publicación de esta política, el silencio o el hecho de descargar un archivo no reemplazan esa autorización.

Asistencia solicitada por el usuario

En el modo atendido, el usuario participa en la solicitud y habilita la sesión conforme a la configuración de su equipo. La entrega de un ID y una contraseña debe acompañarse de la información sobre el soporte autorizado. Si el técnico necesita ampliar la intervención, deberá explicar el cambio y obtener la autorización que corresponda.

Acceso permanente en segundo plano

La edición permanente puede instalar un servicio que arranca con Windows y mantiene el equipo disponible cuando está encendido y conectado. Con acceso desatendido, un técnico que disponga de credenciales válidas puede conectarse sin confirmación local en cada ocasión, incluso si el usuario no está frente al equipo. Un interruptor previamente activado no sustituye el consentimiento informado.

La habilitación deberá identificar el equipo, el solicitante facultado, el propósito, los técnicos o grupo autorizado, el periodo o condición de terminación y las restricciones pertinentes. El ID puede permanecer estable. La contraseña debe ser individual para el equipo, custodiarse con acceso restringido y cambiarse cuando pierda confidencialidad o cambien las personas autorizadas.

Retiro y control local

El usuario o administrador facultado puede cambiar la contraseña, desactivar el acceso desatendido o detener y desinstalar el servicio de ASSC mediante las opciones disponibles en Windows. Cerrar únicamente la ventana no equivale a detener el servicio. También puede solicitar el retiro a ASSC; se verificará la identidad y se coordinará la desconexión sin imponer trámites innecesarios.



4 Límites de la intervención y datos especiales

Control del equipo y archivos

Según los permisos disponibles, el soporte puede incluir teclado y mouse, ejecución de comandos, instalación o desinstalación de software, transferencia, copia, modificación o eliminación de archivos. Estas capacidades no son una autorización general: deben limitarse a lo necesario para la solicitud. Antes de acciones que puedan borrar información o afectar la operación, se confirmará el alcance y se acordará el respaldo que corresponda.

Confidencialidad durante la sesión

El personal de soporte deberá evitar abrir carpetas, correos, documentos o aplicaciones ajenos al caso. No copiará información por curiosidad ni la enviará a cuentas personales. Se recomienda cerrar previamente documentos privados y notificaciones no relacionadas con el soporte. Los permisos de portapapeles, archivos, audio, cámara u otros solo deberán habilitarse cuando sean necesarios y estén disponibles.

Contraseñas y credenciales

La contraseña de soporte es distinta de las claves bancarias, tributarias, de correo o de otros servicios del usuario. ASSC no deberá pedir esas claves por chat ni conservarlas dentro de tickets o capturas. Cuando sea necesario autenticarse en otro sistema, se procurará que el titular o administrador introduzca directamente sus credenciales mediante un procedimiento adecuado al caso.

Datos sensibles y de menores de edad

El soporte no tiene como finalidad recolectar datos de salud, biométricos, vida sexual, origen étnico, creencias u otros datos sensibles. Si una intervención exige tratarlos, se informará su carácter facultativo y se obtendrá autorización explícita u otra habilitación legal aplicable. Los datos de niños, niñas y adolescentes requieren respeto de sus derechos e interés superior, intervención de su representante cuando corresponda y consideración de su opinión según su madurez.

Capturas y grabaciones

La autorización general para recibir soporte no autoriza automáticamente grabaciones de pantalla, audio o video. Si fueran necesarias, deberá informarse su finalidad, contenido, destinatarios y conservación, y obtenerse la habilitación correspondiente antes de iniciarlas. No se establece en esta política una grabación automática de todas las sesiones.



5 Proveedores y circulación de información

Motor tecnológico HopToDesk

ASSC Conexión Remota utiliza tecnología de HopToDesk. La personalización de nombre, iconos y accesos no convierte toda su infraestructura en un servicio operado exclusivamente por ASSC. La política del proveedor, consultada el 17 de septiembre de 2026, identifica a Begonia Holdings LLC y distingue la aplicación, el sitio web y el Dashboard opcional.

HopToDesk declara que las sesiones están cifradas de extremo a extremo y que no accede a su contenido; indica que la aplicación conserva registros de diagnóstico localmente durante 31 días. Para equipos inscritos en su Dashboard, describe tratamiento de datos de cuenta, características del dispositivo, IP, indicadores de funcionamiento y datos de uso. Estas declaraciones son del proveedor y no equivalen a una auditoría independiente de cada instalación de ASSC. Fuente: <https://www.hoptodesk.com/privacy>.

Quién puede recibir información

Dentro de ASSC, el acceso se restringirá al personal que deba atender el caso, gestionar derechos o cumplir una función legítima. Los proveedores tecnológicos recibirán únicamente la información necesaria para la operación efectivamente contratada. Podrá comunicarse información a autoridades competentes mediante requerimiento válido y dentro de sus facultades legales.

Paneles y servicios opcionales

El uso de la aplicación no debe confundirse con la vinculación a un panel de gestión, una mesa de ayuda, grabaciones o funciones de inteligencia artificial. Antes de habilitar funciones adicionales, ASSC deberá informar su alcance y evaluar los datos que enviarán a proveedores. No se cargarán contenidos de sesiones o archivos del cliente a herramientas de inteligencia artificial sin habilitación específica.

Tratamiento fuera de Colombia

La infraestructura de terceros puede implicar circulación internacional. ASSC deberá identificar los servicios utilizados y distinguir transmisión a un encargado de transferencia a otro responsable. Se aplicarán los contratos, garantías, autorizaciones, excepciones o trámites exigibles por la normativa colombiana. Esta política no es una autorización irrestricta para enviar información a cualquier país ni asegura almacenamiento exclusivo en Colombia.

6 Seguridad conservación e incidentes

Medidas de protección

ASSC deberá aplicar controles proporcionados al riesgo: limitar técnicos autorizados, custodiar credenciales, mantener los equipos de soporte actualizados, restringir archivos y registros, definir permisos y exigir confidencialidad al personal. La información no se publicará ni se compartirá mediante enlaces abiertos. La disponibilidad de una función en el motor no acredita que esté configurada o contratada en todos los equipos.

El cifrado de la conexión no impide que un técnico autorizado vea datos, ni elimina riesgos por contraseñas compartidas, equipos comprometidos o acciones indebidas. No se ofrece seguridad absoluta. El acceso permanente deberá revisarse cuando finalice el contrato, cambie el responsable del equipo o se sospeche uso no autorizado.

Conservación según la finalidad

Los datos del caso y la evidencia de autorización se conservarán durante el tiempo necesario para prestar y acreditar el servicio, atender derechos y cumplir obligaciones legales o contractuales. ASSC deberá identificar y documentar el plazo aplicable a cada categoría; no se establece conservación indefinida por el solo hecho de haber instalado la aplicación.

Las copias temporales de archivos se eliminarán una vez concluida la tarea que las justificó, salvo necesidad documentada de conservación. Las grabaciones, si se autorizan, tendrán un plazo informado antes de su realización. Los respaldos se depurarán conforme a su ciclo documentado y, mientras subsistan, permanecerán restringidos. Desinstalar la aplicación no elimina automáticamente tickets, respaldos ni registros ya conservados por motivos legítimos.

Respuesta ante incidentes

Ante pérdida de credenciales, acceso indebido o exposición de datos, ASSC deberá evaluar el hecho, contener el acceso, preservar la evidencia necesaria y coordinar la respuesta con el cliente. Informará a los titulares, al responsable del tratamiento y a la autoridad cuando corresponda, según la naturaleza del incidente y las obligaciones aplicables. No deberá ocultarse un incidente por el hecho de que la sesión estuviera autenticada.

Reporte inmediato: cliente@sistemascolombia.com o WhatsApp +57 300 174 3544. Indique el equipo, momento aproximado y hechos observados, sin enviar contraseñas. Si sospecha una conexión indebida en curso, interrumpa el acceso desde el equipo o solicite apoyo a su administrador.

7 Derechos consultas y reclamos

Los titulares pueden conocer, actualizar y rectificar sus datos; solicitar prueba de la autorización cuando proceda; conocer el uso dado a su información; acceder gratuitamente a sus datos; solicitar revocatoria y supresión en los casos aplicables, y presentar quejas ante la Superintendencia de Industria y Comercio. La supresión no procede respecto de información que deba mantenerse por una obligación legal o contractual vigente.

Cómo presentar una solicitud

Escriba a cliente@sistemascolombia.com, utilice el WhatsApp +57 300 174 3544 o presente una solicitud escrita en la dirección de notificaciones indicada en este documento. Incluya nombre, medio de respuesta, petición concreta y datos que permitan ubicar el caso. Si actúa por otra persona, acredite esa representación. Solo se solicitará identificación adicional cuando sea necesaria para proteger los datos.

Consultas

Las consultas se atenderán dentro de los diez (10) días hábiles contados desde su recibo. Si no es posible responder en ese plazo, se informarán las razones y una nueva fecha, sin superar los cinco (5) días hábiles siguientes al vencimiento del término inicial, de conformidad con el artículo 14 de la Ley 1581 de 2012.

Reclamos

Los reclamos de corrección, actualización, supresión o presunto incumplimiento se atenderán en un máximo de quince (15) días hábiles desde el día siguiente al recibo. Si se requiere prórroga, se informarán las razones y la fecha de respuesta, que no podrá exceder ocho (8) días hábiles adicionales al vencimiento del término inicial.

Si el reclamo está incompleto, se requerirá subsanación dentro de los cinco (5) días siguientes a su recepción. Transcurridos dos (2) meses desde el requerimiento sin respuesta, se entenderá desistido. Si quien lo recibe no es competente, lo trasladará en máximo dos (2) días hábiles e informará al interesado. Recibido completo, se incorporará la leyenda «reclamo en trámite» en máximo dos (2) días hábiles y se mantendrá hasta la decisión, cuando corresponda a la base de datos.

La queja ante la SIC requiere agotar previamente el trámite de consulta o reclamo ante el responsable o encargado. Estos derechos son distintos del retiro técnico inmediato de una conexión, que puede realizarse mediante las opciones disponibles en el equipo.



8 Aplicación de la política y aviso para usuarios

Responsabilidades internas

Atención al Cliente coordinará solicitudes y evidencias; el área técnica verificará los permisos y el alcance de las intervenciones; la administración supervisará la aplicación de esta política. El técnico deberá identificar la solicitud o acuerdo que habilita el acceso y respetar las restricciones pactadas. La documentación de atención debe ser proporcional y evitar copiar innecesariamente contenidos del equipo.

Publicación y cambios

Esta versión se preparó el 17 de septiembre de 2026 y será aplicable desde su adopción y publicación por ASSC. Complementa la política general corporativa. Los cambios relevantes se comunicarán por los canales institucionales; si incorporan nuevas finalidades que requieran autorización, esta se obtendrá antes del nuevo tratamiento. La continuidad de uso no sustituye ese deber.

Aviso breve para la aplicación

ASSC SAS, NIT 901.926.771-3, tratará sus datos de contacto, identificación del equipo y la información necesaria para prestar el soporte autorizado. El técnico podrá visualizar la pantalla e interactuar con archivos y aplicaciones según los permisos concedidos. Utilizamos tecnología de HopToDesk. Consulte esta política y ejerza sus derechos en cliente@sistemascolombia.com.

Si habilita acceso desatendido: el servicio podrá iniciar con Windows y permitir conexiones con credenciales válidas sin pedir aceptación en cada sesión. Puede retirar este acceso cambiando sus credenciales, deshabilitando el modo o deteniendo y desinstalando el servicio. El técnico debe contar previamente con autorización para la intervención; la casilla activada no constituye por sí misma prueba de esa autorización.

Evidencia separada de autorización

La evidencia de autorización deberá identificar a la persona facultada, el equipo, las finalidades, los permisos, la fecha, la modalidad atendida o desatendida y las condiciones de retiro. El acceso desatendido deberá identificarse de forma expresa. Si se autorizan grabaciones o usos adicionales, se documentarán separadamente. Este texto informa el tratamiento y no certifica que la aplicación ya capture o almacene automáticamente esa evidencia.

9 Fuentes y relación con la política general

Este documento se elaboró para ASSC Conexión Remota tomando como referencia el membrete y los datos institucionales de la política general publicada por ASSC. No modifica las condiciones de licencia del motor tecnológico ni reemplaza los acuerdos de tratamiento de datos que correspondan con cada cliente o proveedor.

Política general de ASSC SAS

Política de Tratamiento y Protección de Datos Personales, versión 1.0, vigente desde el 9 de septiembre de 2026. Fuente de identificación y canales de atención.

<https://sistemascolombia.com/assets/politica-tratamiento-datos-assc.pdf>

Ley 1581 de 2012

Régimen general de protección de datos personales. Artículos 4 a 12, 14 a 18 y 26, entre otros aplicables.

<https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=49981>

Reglamentación de protección de datos

Decreto 1074 de 2015, disposiciones de protección de datos personales y transmisión de información que resulten aplicables.

<https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=76608>

Autoridad de protección de datos

Superintendencia de Industria y Comercio. Orientación y canales oficiales para protección de datos personales.

<https://www.sic.gov.co>

Consultas adicionales, soporte e información:

ADMINISTRACIÓN Y SERVICIOS SISTEMAS COLOMBIA S.A.S.

cliente@sistemascolombia.com

<https://www.sistemascolombia.com/soporte>