# Medidas técnicas y organizativas
## Rescue y Rescue Lens

## Resumen

Este documento de Medidas técnicas y organizativas ("MTO") establece los compromisos de privacidad, seguridad y responsabilidad de GoTo para Rescue y Rescue Lens. En concreto, GoTo mantiene sólidos programas globales de privacidad y seguridad, así como medidas de protección organizativas, administrativas y técnicas diseñadas para (i) garantizar la confidencialidad, integridad y disponibilidad del Contenido del cliente; (ii) ofrecer protección frente a amenazas y peligros para la seguridad del Contenido del cliente; (iii) proteger frente a cualquier pérdida, uso indebido, acceso no autorizado, divulgación, alteración y destrucción del Contenido del cliente; y (iv) mantener el cumplimiento de las leyes y normativas aplicables, incluidas las leyes de protección de datos y privacidad. Dichas medidas incluyen:

- **Cifrado:**
  - *En tránsito*: seguridad de la capa de transporte (TLS), versión 1.2.
  - *En reposo:* cifrado de datos transparente (TDE) mediante estándar de cifrado avanzado (AES) de 256 bits para el Contenido del cliente.
- **Centros de datos:**[1] ubicaciones de los centros de datos de Estados Unidos, Alemania e Irlanda para respaldar la redundancia y la estabilidad.
- **Seguridad física:** controles ambientales y de seguridad física adecuados preparados y diseñados para proteger, controlar y restringir el acceso físico a los sistemas y servidores que mantienen el Contenido del cliente para respaldar los compromisos de tiempo de actividad, rendimiento y escalabilidad.
- **Auditorías de cumplimiento:** Rescue cuenta con las certificaciones ISO/IEC 27001:2013, SOC 2 Tipo 2, PCI DSS, PCAOB, TRUSTe Enterprise Privacy y tanto CBPR como PRP de APEC.
- **Cumplimiento legal/normativo:** GoTo mantiene un programa integral de protección de datos con procesos y políticas diseñados para garantizar que el Contenido del cliente se gestiona de acuerdo con las leyes de privacidad aplicables, incluidas la RGPD, la CCPA/CPRA y la LGPD.
- **Evaluaciones de seguridad:** además de las pruebas internas, GoTo contrata a empresas externas para que realicen evaluaciones periódicas de seguridad o pruebas de penetración.
- **Controles de acceso lógico:** los controles de acceso lógico se implementan y diseñan para prevenir o mitigar la amenaza de acceso no autorizado a las aplicaciones y la pérdida de datos en entornos de empresa y de producción.
- **Segregación de datos**: GoTo emplea una arquitectura multiusuario y separa de forma lógica las cuentas de los clientes a nivel de base de datos.
- **Defensa del perímetro y detección de intrusiones**: las herramientas, técnicas y servicios de protección del perímetro están diseñados para impedir que el tráfico de red no autorizado entre en la infraestructura de los productos. La red GoTo cuenta con cortafuegos externos y segmentación de red interna.
- **Retención de datos:**
  - Los Clientes de Rescue pueden solicitar la devolución o eliminación del Contenido del cliente en cualquier momento, lo que se cumplirá en un plazo de treinta (30) días a partir de la solicitud del Cliente.
  - El Contenido del cliente se eliminará automáticamente durante los 140 días posteriores al vencimiento del plazo de suscripción del Cliente.

[1] Las ubicaciones de alojamiento pueden variar (por ejemplo, en función de la elección de residencia de los datos). Consulte la Divulgación del responsable secundario de Rescue, que se encuentra en la sección Recursos del producto del Centro de privacidad y confianza de GoTo (https://www.goto.com/company/trust/resource-center), para obtener más información.

# Índice

Haga clic en los números de página siguientes para ir a la sección de MTO correspondiente.

# 1 Introducción al producto

**Rescue** es un servicio de asistencia remota en línea utilizado por los técnicos para proporcionar asistencia remota por Internet, sin necesidad de software preinstalado. Con el permiso del usuario o de otra persona que utilice Rescue o reciba asistencia de un técnico (usuario final), Rescue permite a un técnico acceder, ver y asumir el control del ordenador de un usuario final. A través de una ventana de chat, el técnico puede examinar, diagnosticar y reparar problemas informáticos, así como ayudar de cualquier otro modo a un usuario final con problemas del sistema operativo y de las aplicaciones de software.

**Rescue Lens** permite a los usuarios finales transmitir las cámaras de sus dispositivos móviles (a través de la aplicación móvil Lens) a un técnico remoto para que vea el hardware que les causa problemas (por ejemplo, un router mal configurado o un componente de automoción dañado). Rescue Lens es una función opcional de Rescue que puede activarse en el Centro de administración de Rescue. Para obtener más información sobre Rescue Lens, consulte la Guía del usuario de Rescue Lens.

*Los términos en mayúsculas de este documento que no se definen en el texto, sino en las Términos del servicio.*

# 2 Medidas técnicas

Los productos de GoTo están diseñados para ofrecer soluciones seguras, fiables y privadas. Las medidas técnicas definidas a continuación describen cómo GoTo implementa ese diseño y lo aplica en la práctica para Rescue y Rescue Lens.

## 2.1 Medidas de protección

La implementación de medidas de protección, funciones y prácticas por parte de GoTo implica:

I. Construir productos que tengan en cuenta la seguridad y la privacidad por diseño y de forma predeterminada e incluir más capas de seguridad para proteger el contenido de los clientes;

II. mantener controles organizativos que implementen las políticas y los procedimientos internos relacionados con el cumplimiento de las normas, la gestión de incidentes, la seguridad de las aplicaciones, la seguridad del personal y los programas de formación habituales;

III. garantizar la existencia de prácticas de privacidad que rijan el tratamiento y la gestión de los datos de conformidad con la legislación aplicable, incluidos el RGPD, la CCPA/CPRA, la LGPD, así como nuestro propio Anexo de tratamiento de datos (DPA) y las políticas y compromisos aplicables de GoTo.

Al incorporar medidas de protección para añadir seguridad al producto, nos esforzamos por proteger el Contenido del cliente de GoTo frente a las amenazas y garantizar que los controles de seguridad sean adecuados a la naturaleza y el alcance de los Servicios. Las funciones de seguridad configurables de GoTo pueden ayudar a los administradores a minimizar las amenazas y los riesgos que suponen para los sistemas y las redes las personas que utilizan los servicios de GoTo.

# 3 Arquitectura del producto

Rescue es una solución de asistencia remota basada en software como servicio (SaaS) que consta de tres componentes principales: una Consola de técnico, una aplicación móvil o applet de escritorio para usuarios finales y un centro de administración.

La Consola de técnico es la interfaz utilizada por los técnicos para las sesiones de asistencia remota. Los técnicos pueden iniciar nuevas sesiones o responder a las solicitudes en línea de los usuarios finales que esperan en una cola compartida. Los técnicos se comunican con los usuarios finales y les proporcionan asistencia a través de la aplicación móvil (Android o iOS) o el applet de escritorio (Windows, macOS o Linux) de Rescue. El applet se descarga en el PC remoto del usuario final y está diseñado para eliminarse cuando concluya la sesión.

La Consola de técnico de Rescue interactúa con la aplicación o el applet de Rescue mediante una conexión de red punto a punto (P2P) (consulte la Figura 1 en la sección 3.1). Cuando se inicia el applet, el proceso P2P se inicia y conecta a una pasarela Rescue, donde se negocia la sesión con la Consola de técnico.

El protocolo de reenvío de intercambio de claves propio de GoTo está diseñado para evitar la interceptación o escucha de la infraestructura de GoTo. En particular, la puerta de enlace facilita la conexión entre el usuario final y host para que el usuario final pueda conectarse al host independientemente de la configuración de la red.

El host establece una conexión TLS con la puerta de enlace, que reenvía el intercambio de claves TLS del usuario final al host mediante una solicitud de renegociación de claves propias. De este modo, el usuario final y el host intercambian claves TLS sin que la puerta de enlace conozca la clave.

## 3.1 Acuerdo de claves

Cuando se inicia una sesión de asistencia técnica y se establece una conexión entre el usuario final al que se presta asistencia y el técnico, sus ordenadores deben acordar un algoritmo de cifrado entre las opciones compatibles disponibles y la clave correspondiente que se va a utilizar durante la sesión.

Los ordenadores utilizan certificados para validar sus identidades. Como ni el técnico ni el usuario final tienen software capaz de intermediar en la conexión y validar los certificados de seguridad instalados ni un certificado SSL instalado en sus ordenadores, ambos se ponen en contacto con unos de los servidores de Rescue y realizan la fase inicial del acuerdo de claves. La verificación del certificado por parte de la Consola de técnico y de la aplicación o el applet del usuario final garantiza que solo un servidor de Rescue pueda participar en el proceso.

## 3.2 Descripción general del proceso de conexión de la puerta de enlace de Rescue

Cuando la aplicación o el applet de Rescue firmados digitalmente se inician en un equipo, contienen un identificador único global (GUID) de autenticación de sesión. El GUID se incrusta en la aplicación o el applet ejecutable (por ejemplo, un archivo .exe) como un recurso del sitio cuando se descarga. A continuación, la aplicación o el applet descargan una lista de puertas de enlace disponibles en secure.logmeinrescue.com o secure.logmeinrescue.eu, eligen una pasarela de la lista y se conectan a ella mediante TLS. A continuación, el applet autentica la puerta de enlace con el certificado SSL. La puerta de enlace autentica el applet en la base de datos con el GUID y registra que el usuario final está esperando a un técnico.

Cuando un técnico inicia sesión en la Consola de técnico de Rescue, se envía una solicitud a la puerta de enlace con el GUID de autenticación de la sesión para retransmitir las conexiones entre la Consola de técnico y el applet o la aplicación del usuario final. La puerta de enlace es el intermediario que autentica la conexión y empieza a retransmitir los datos a nivel de transporte (no descifra los datos retransmitidos).

Cuando se inicia una retransmisión de conexión, las partes intentan establecer una conexión P2P. El proceso es el siguiente:

- El applet comienza a recibir datos de una conexión del protocolo de control de transmisión (TCP) en un puerto asignado por Windows, macOS o Linux.
- Si no puede establecerse la conexión TCP en 10 segundos, se intenta establecer una conexión de protocolo de datagramas de usuario (UDP) con ayuda de la puerta de enlace.
- Si se establece una conexión TCP o UDP, las partes autentican el canal P2P (utilizando el GUID de autenticación de la sesión) y se asume el tráfico de la conexión retransmitida.
- Si se ha establecido una conexión UDP, se emula el TCP sobre los datagramas de UDP con XTCP, un protocolo propiedad de GoTo basado en la pila TCP de Berkeley Software Distribution (“BSD”).
- Todas las conexiones están protegidas con el protocolo TLS (que utiliza el cifrado AES256 con controles de acceso al medio [MAC] SHA256). El GUID de autenticación de la sesión es un valor entero aleatorio de nivel de cifrado de 128 bits.

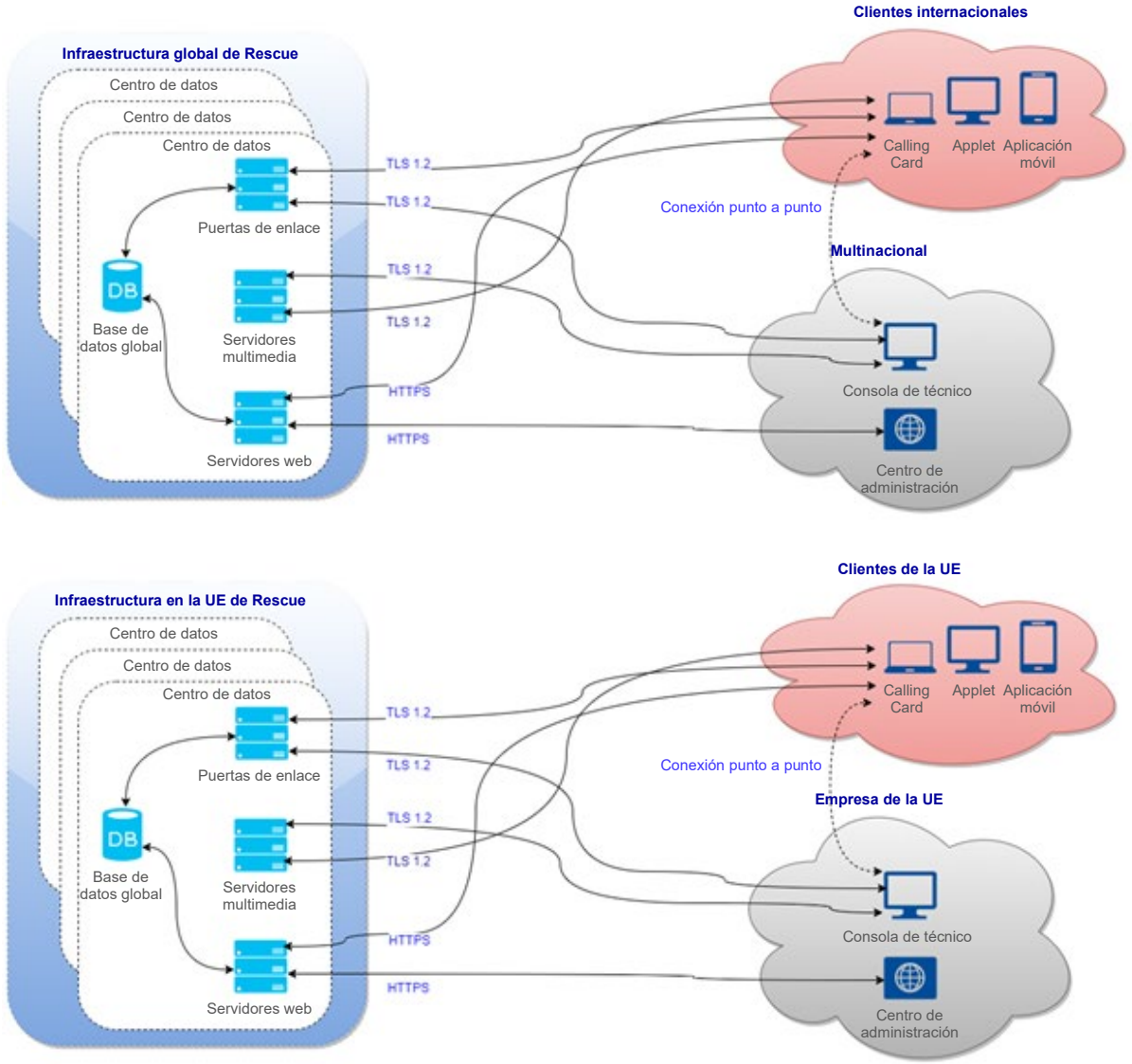


Figura 1: Arquitectura de Rescue

## 3.3 Arquitectura multimedia de Rescue

El servicio multimedia Rescue es un servicio independiente basado en la comunicación web en tiempo real (WebRTC) que impulsa la transmisión de vídeo con Rescue Lens. Gestiona las conferencias de las sesiones de Rescue que utilizan la función Lens. Los participantes en la conferencia (pares) entran y salen de ella, y los usuarios finales envían secuencias de vídeo y audio para que las reciban el resto de participantes. Lens envía el contenido de vídeo en un flujo unidireccional desde la aplicación Lens a la Consola de técnico.

El servicio multimedia consta de tres componentes principales: el kit de desarrollo de software multimedia (Media SDK), el gestor de sesiones y el servidor de transmisión. Estos componentes gestionan el proceso de crear/eliminar conferencias, y de unirse a ellas/salir de ellas. Se comunican por medio de las conexiones seguras existentes entre la Consola de técnico y el sitio web y entre la aplicación Lens y el sitio web.

### 3.3.1 Media SDK

El servicio multimedia está basado en WebRTC con una fina capa creada en torno a la base de código de WebRTC. La consola del técnico y la aplicación móvil Lens utilizan Media SDK.

### 3.3.2 Gestor de sesiones

El Gestor de sesiones es un sitio web de carga equilibrada que proporciona una API de transferencia de estado representacional (REST) para gestionar (crear/destruir/unirse) las conferencias. El Gestor de sesiones solo acepta solicitudes procedentes del sitio web.

### 3.3.3 Servidor de transmisión

El servicio multimedia utiliza una solución de servidor de transmisión personalizada para gestionar los flujos entre pares (la Consola de técnico y la aplicación Lens). Tanto la Consola de técnico como la aplicación Lens se conectan al servidor de transmisión. Una sesión de Lens engloba dos transmisiones (una que se envía y otra que se recibe). La aplicación Lens transmite su contenido de vídeo al servidor de transmisión, mientras que la Consola de técnico transmite el contenido de vídeo aguas abajo del servidor. El servidor de transmisión actúa como servidor de relé entre los pares.

# 4 Controles técnicos de seguridad

GoTo emplea controles técnicos de seguridad diseñados para proteger la infraestructura del Servicio y los datos que residen en ella.

## 4.1 Confidencialidad de los datos

El sistema en línea seguro de Rescue está respaldado por Secure Sockets Layer y Transport Layer Security (SSL/TLS), y cumple los siguientes objetivos:

- Autenticación de las partes que intervienen en la comunicación
- Negociación de claves de cifrado sin interceptación
- Intercambio confidencial de mensajes
- Capacidad de detectar si un mensaje se ha modificado durante la transmisión

Rescue utiliza OpenSSL y, en el momento de la publicación de este documento, emplea la versión 1.1.1n.

## 4.2 Cifrado

GoTo revisa periódicamente sus normas de cifrado y puede actualizar los cifradores o las tecnologías utilizadas de acuerdo con el riesgo evaluado y la aceptación en el mercado de nuevas normas.

### 4.2.1 Cifrado en tránsito

El tráfico de red que entra y sale de los centros de datos de Rescue, incluido todo el Contenido del cliente, se cifra en tránsito con TLS 1.2 y HTTPS. Además, las sesiones de asistencia de Rescue están protegidas con un cifrado AES de 256 bits y un hash MD5 para mejorar la trazabilidad de las transferencias de archivos.

Dado que los tres componentes del sistema de comunicaciones de Rescue están bajo el control de GoTo, el conjunto de cifrado que utilizan es siempre el mismo: AES256-SHA en modo de encadenamiento de bloques cifrados con acuerdo de claves RSA. Esto significa lo siguiente:

- El algoritmo de cifrado/descifrado es AES
- La clave de cifrado tiene una longitud de 256 bits.
- Las claves de cifrado se intercambian utilizando pares de claves RSA privadas/públicas, tal y como se ha descrito en la sección anterior.
- La base de MAC es SHA-2. Un MAC es una porción de información que se utiliza para autenticar un mensaje. El valor del MAC protege tanto la integridad de un mensaje como su autenticidad, pues permite que las partes que establecen comunicación detecten cualquier cambio en el mensaje.
- El modo de encadenamiento de bloques cifrados (CBC) garantiza que cada bloque de texto cifrado dependa de los bloques de texto plano hasta ese punto, de forma que los mensajes similares no se puedan identificar como tales.

La transmisión de datos entre el usuario final al que se presta asistencia y el técnico está completamente cifrada, y solo estas partes tienen acceso a la información contenida en el flujo de mensajes.

### 4.2.2 Cifrado en reposo

El contenido del cliente de Rescue se cifra en reposo tanto a nivel del servidor como de la base de datos con AES256 y TDE. Por ejemplo, el Contenido del cliente incluye registros de chat y campos personalizados, que son campos creados por el titular de la cuenta maestra o el administrador maestro.

## 4.3 Controles de acceso de Rescue

Los administradores de Rescue pueden personalizar los controles de acceso. Por ejemplo, los administradores de Rescue pueden configurar una política de contraseñas que incluya, entre otros, una seguridad mínima requerida y una antigüedad máxima de la contraseña. También pueden forzar el restablecimiento de contraseñas, aplicar la autenticación de dos factores para los inicios de sesión en Rescue, restringir el acceso de los técnicos a Rescue desde direcciones IP preaprobadas a tareas específicas o conceder a los técnicos acceso únicamente a aplicaciones predefinidas mediante un único ID de SSO para iniciar sesión en dichas aplicaciones. Si es necesario, los administradores pueden desactivar el ID de SSO de un técnico.

Los controles de acceso adicionales incluyen:

- Acceso basado en permisos con todo detalle (por ejemplo, permitir que algunos técnicos utilicen la visión remota, pero no el control remoto)
- No almacenar datos de dispositivos remotos en servidores GoTo. Solo se almacenan los registros de sesión, las direcciones IP de los usuarios finales y los registros de chat. Los registros de texto del chat pueden eliminarse de los detalles de la sesión
- Impedir que los técnicos transfieran archivos
- Exigir que el usuario final esté presente en el dispositivo remoto para permitir el acceso remoto
- Exigir que el usuario final mantenga el control y pueda finalizar la sesión en cualquier momento
- Impedir que los técnicos utilicen determinadas funciones hasta que el usuario final les haya concedido permiso explícito (por ejemplo, control remoto, vista del escritorio, transferencia de archivos, información del sistema, reinicio y reconexión)
- Revocación automática de los derechos de acceso al finalizar la sesión
- Posibilidad de forzar el cierre automático de la sesión tras un tiempo de inactividad predeterminado
- Bloqueo de una cuenta tras cinco intentos fallidos de inicio de sesión

### 4.3.1 Control de acceso basado en permisos

Los administradores de Rescue también pueden conceder o denegar permisos específicos en el centro de administración. Estos permisos de grupo incluyen:

- Permitir la sincronización del portapapeles
- Permitir compartir pantalla con usuarios y usuarios finales
- Implementar scripts
- Iniciar la visualización del escritorio
- Iniciar el gestor de archivos
- Iniciar el control remoto
- Reiniciar
- Grabar sesiones
- Solicitar credenciales
- Enviar y recibir archivos
- Enviar URL
- Iniciar sesiones privadas
- Transferir sesiones
- Utilizar un único indicador para todos los permisos
- Ver la información del sistema

Para obtener más información sobre los permisos de grupo, consulte la Guía para administradores de Rescue. Los técnicos de Rescue Lens se identifican por su dirección de correo electrónico y se autentican con una contraseña.

### 4.3.2 Autenticación

Las medidas de autenticación de Rescue están diseñadas para proteger el producto con medidas que solo permitan a los técnicos o administradores iniciar sesión en el sistema. Los administradores asignan a los técnicos identificadores de inicio de sesión (por ejemplo, que coincidan con sus direcciones de correo electrónico) y las contraseñas correspondientes. Los técnicos introducen estas credenciales en el formulario de inicio de sesión de la página web de Rescue como mínimo al comenzar su turno. Los administradores pueden configurar los controles para que exijan la autenticación con mayor frecuencia (por ejemplo, tras cinco minutos de inactividad).

El sistema Rescue se autentica primero en el navegador web del técnico con su certificado SSL RSA premium de 2048 bits, lo que garantiza que el técnico introducirá su nombre de usuario y contraseña en el sitio web correcto. A continuación, el técnico se conecta al sistema con sus credenciales. Rescue no almacena ninguna contraseña, sino que utiliza scrypt para crear hashes a partir de las contraseñas que luego se almacenan en la base de datos de Rescue. El algoritmo hash utiliza una cadena de 24 caracteres como "sal", generada por CSPRNG para cada contraseña exclusiva.

El sistema de Rescue se autentica también con el usuario final al que se presta asistencia técnica. La aplicación o el applet, descargados y ejecutados por el usuario final, se firman con el certificado de firma de código de GoTo (basado en una clave RSA de 2048 bits), y esta información suele mostrarse al usuario final en su navegador web cuando está a punto de ejecutar el software. Rescue no autentica al usuario final ante el técnico.

Rescue también permite a los administradores implementar una política de inicio de sesión único (SSO). Se emplea el lenguaje SAML (Security Assertion Markup Language), que es un estándar XML (Extensible Markup Language) para intercambiar datos de autenticación y autorización entre dominios de seguridad (es decir, entre un proveedor de identidades y un proveedor de servicios).

Los administradores también pueden exigir la verificación en dos pasos para iniciar sesión en Rescue. La función de verificación en dos pasos puede utilizar el correo electrónico, los SMS o cualquier autenticador de contraseña de un solo uso basado en el tiempo (TOTP) para proporcionar una segunda capa de protección a una cuenta de Rescue, así como exigir a los miembros seleccionados de la organización que establezcan una forma adicional de verificar su identidad. La configuración de la aplicación de autenticación se activa en cualquiera de los siguientes casos:

- El miembro seleccionado intenta iniciar sesión en la cuenta de Rescue en el sitio web seguro.
- El miembro seleccionado intenta iniciar sesión en la versión para ordenador de la Consola de técnico.
- El miembro seleccionado intenta cambiar su contraseña de Rescue.

### 4.3.3 Autorización

La autorización se produce al menos una vez durante cada sesión de asistencia remota. Tras descargar y ejecutar el applet, un técnico se pondrá en contacto con el usuario final compatible. El técnico puede chatear con el usuario final a través del applet, pero cualquier otra acción, como enviar un archivo o ver el escritorio del usuario final, requiere el permiso expreso de este. También se puede implementar una “solicitud única” para trabajos de asistencia remota prolongados en los que el usuario final podría no estar presente durante toda la sesión. Si este ajuste está activado para un grupo de técnicos, los técnicos de ese grupo pueden solicitar un permiso “global” al usuario final y, si se les concede, realizar acciones como ver información del sistema o entrar en una sesión de control remoto sin necesidad de que el usuario final les vuelva a autorizar. Los administradores también pueden imponer restricciones de direcciones IP para que los técnicos asignados a una tarea concreta solo puedan acceder a Rescue y realizar dicha tarea desde direcciones IP preaprobadas. Además, el administrador de un grupo de técnicos puede deshabilitar determinadas funciones en el Centro de administración.

Los permisos que un administrador puede conceder o denegar incluyen:

- Iniciar el control remoto
- Reiniciar
- Iniciar la visualización del escritorio
- Grabar sesiones
- Enviar y recibir archivos
- Iniciar sesiones privadas
- Iniciar el Gestor de archivos
- Solicitar credenciales
- Enviar las URL
- Permitir sincronización con portapapeles
- Ver información del sistema
- Implementar scripts
- Utilizar solicitudes únicas para todos los permisos
- Transferir sesiones
- Permitir compartir pantalla con usuarios y usuarios finales

## 4.4 Controles de auditoría

Los siguientes controles de auditoría están disponibles para los usuarios y usuarios finales de Rescue:

- Opción de forzar la grabación de sesiones, con capacidad para almacenar archivos de auditoría en un recurso compartido de la red seguro.
- La actividad de las sesiones remotas y las sesiones del técnico se registran en el ordenador host para garantizar la seguridad y mantener el control de calidad (inicios de sesión correctos, inicios de sesión erróneos, inicio de control remoto, fin de control remoto, comienzo del reinicio, cierre de sesión).
- Autenticación de personas o entidades.
- Autenticación del técnico con su dirección de correo electrónico única o a través de un ID SSO
- Permitir que los técnicos se conecten solo desde direcciones IP aprobadas
- El informe de auditoría disponible en el Centro de administración incluye los cambios realizados en la configuración de la cuenta y los datos de cada acción realizada por los Administradores en el elemento seleccionado del Árbol de la organización durante un periodo determinado.

# 5 Actualizaciones del programa de seguridad

GoTo revisa y actualiza su programa de seguridad y contrata a terceros independientes para que evalúen sus controles de seguridad pertinentes al menos una vez al año, con el fin de garantizar que evoluciona frente al panorama actual de amenazas y asegurar el cumplimiento de los marcos pertinentes, las normas del sector, los compromisos del Cliente y, según corresponda, los cambios en las leyes y normativas relativas a la seguridad de los datos de GoTo.

# 6 Copia de seguridad de datos, recuperación ante desastres y disponibilidad

La arquitectura de GoTo está diseñada para realizar la replicación casi en tiempo real en ubicaciones geográficamente diversas. Las copias de seguridad de las bases de datos se realizan mediante una estrategia de copia de seguridad incremental continua. En caso de desastre o de fallo total del emplazamiento en alguna de las varias ubicaciones activas, las ubicaciones restantes están diseñadas para equilibrar la carga de la aplicación. La recuperación en caso de desastre relacionada con estos sistemas se prueba periódicamente.

La base de datos de Rescue se sincroniza cada cinco minutos con otro centro de datos. Además, se realizan una copia de seguridad diferencial cada noche y varias copias de seguridad completas cada fin de semana. La base de datos de la copia de seguridad se almacena con el mismo cifrado que la original. Las copias de seguridad se conservan in situ durante un mes y después se rotan a un servicio en la nube, dejan de procesarse activamente y se conservan de acuerdo con nuestras políticas internas de conservación de registros. En caso de el centro de datos que aloja la base de datos principal falle por completo, la arquitectura de Rescue está diseñada para restaurarse rápidamente.

# 7 Centros de datos

La infraestructura de GoTo está diseñada para aumentar la fiabilidad del servicio y reducir el riesgo de tiempo de inactividad de cualquier punto único de fallo mediante:

a) centros de datos redundantes activos-pasivos; o
b) centros de datos de proveedores de alojamiento en la nube.

En el momento de la creación de la cuenta, los Clientes de Rescue pueden optar por utilizar la infraestructura de datos de GoTo global o de la Unión Europea para almacenar su Contenido del cliente. Las ubicaciones de alojamiento/almacenamiento se especifican a continuación:[2]

- **Unión Europea:** Alemania e Irlanda
- **Global:** Estados Unidos, Alemania, Australia y Reino Unido

Todos los centros de datos incluyen la supervisión de las condiciones medioambientales y cuentan con medidas de seguridad física las 24 horas del día, que se abordan a continuación.

## 7.1 Seguridad física del centro de datos

GoTo tiene contratos con centros de datos para proporcionar seguridad física y controles ambientales para los sistemas y servidores que contienen Contenido del cliente. Estos controles incluyen los siguientes:

- videovigilancia y grabación
- control de la temperatura de calefacción, ventilación y aire acondicionado
- extinción de incendios y detectores de humo
- sistema de alimentación ininterrumpida
- suelos elevados o gestión integral de cables
- supervisión continua y alertas
- protecciones contra las catástrofes naturales y las provocadas por el hombre más comunes, según lo exijan la geografía y la ubicación del centro de datos en cuestión
- mantenimiento programado y validación de todos los controles críticos de seguridad y medioambientales

GoTo limita el acceso físico a los centros de datos de producción únicamente a las personas autorizadas. El acceso a una sala de servidores local o a una instalación de alojamiento de terceros requiere el envío de una solicitud a través del sistema de tickets correspondiente y la aprobación por parte del responsable correspondiente, así como la revisión y aprobación por parte del equipo de operaciones técnicas de GoTo. Todos los accesos físicos a los centros de datos y salas de servidores se registran y la dirección de GoTo revisa los registros al menos trimestralmente. Además, la autorización de acceso físico al centro de datos se elimina rápidamente al cambiar de función (cuando dicho acceso ya no es necesario) o al cesar el personal previamente autorizado. El acceso multifactor (por ejemplo, biométrico, mediante tarjeta de identificación y teclado) es necesario para las zonas altamente sensibles, entre las que se incluyen los centros de datos.

# 8 Cumplimiento de las normas

GoTo evalúa regularmente su cumplimiento de los requisitos legales, de seguridad, financieros, de privacidad de datos y normativos aplicables. Los programas de privacidad y seguridad de GoTo han cumplido normas rigurosas y de reconocimiento internacional, se han evaluado de acuerdo con exhaustivas normas de auditoría externa y han logrado certificaciones clave, entre las que se incluyen:

- **Certificación de TRUSTe en materia de privacidad empresarial y prácticas de gobierno de datos** para abordar los controles operativos de privacidad y protección de datos que están alineados con las principales leyes de privacidad y marcos de privacidad reconocidos. Para obtener más información, visite nuestra entrada en el blog.

[2] Las ubicaciones de alojamiento pueden variar (es decir, en función de la elección de residencia de los datos), consulte la Declaraciones para representantes de Rescue aplicable que se encuentra en la sección Recursos del producto del Centro de privacidad y confianza de GoTo (https://www.goto.com/company/trust/resource-center).

- **Certificaciones CBPR y PRP de TRUSTe y APEC** para la transferencia de contenidos de clientes entre países miembros de la APEC obtenidas y validadas de forma independiente a través de TrustArc, una tercera parte que cuenta con la aprobación de la APEC líder en el cumplimiento de la protección de datos. Para obtener más información sobre nuestras certificaciones APEC, haga clic aquí.
- Certificación del Sistema de Gestión de la Seguridad de la Información (SGSI) de la Organización Internacional de Estandarización – **ISO/IEC 27001:2013**.
- Informe de atestación del Instituto Americano de Contables Públicos Certificados (AICPA) de **Control de Organizaciones de Servicios (SOC) 2 Tipo II**.
- Cumplimiento de la **Norma de seguridad para la industria de las tarjetas de pago (PCI DSS)** para los entornos de comercio electrónico y de pago de GoTo.
- Evaluación de los controles internos exigidos en una auditoría anual de los estados financieros del **Consejo de Supervisión de Contabilidad de Empresas Públicas (PCAOB)**.

# 9 Seguridad de las aplicaciones

El programa de seguridad de aplicaciones de GoTo sigue el ciclo de vida de desarrollo de seguridad (SDL) de Microsoft para asegurar el código de los productos. El programa SDL de Microsoft incluye revisiones manuales del código, modelado de amenazas, análisis estático del código, análisis dinámico y refuerzo del sistema. Los equipos de GoTo también realizan periódicamente pruebas de vulnerabilidad de aplicaciones dinámicas y estáticas y actividades de pruebas de penetración para entornos específicos.

# 10 Registro, supervisión y alertas

GoTo mantiene políticas y procedimientos en torno al registro, la supervisión y las alertas, que establecen los principios y controles que se aplican para reforzar nuestra capacidad de detectar actividades sospechosas y responder a ellas a tiempo. GoTo recopila el tráfico anómalo o sospechoso identificado en los registros de seguridad pertinentes de los sistemas de producción aplicables.

Los registros de chat de Rescue se guardan en la base de datos de Rescue. La Consola de técnico envía este registro de la conversación en tiempo real a los servidores de Rescue; el registro contiene sucesos y mensajes de chat de una sesión de asistencia técnica determinada. Los archivos de registro mostrarán las siguientes acciones de los técnicos: hora de inicio y fin de una sesión de control remoto, casos de técnicos que comparten archivos con usuarios finales, y metadatos relacionados con el intercambio de archivos (por ejemplo, el nombre y la huella digital MD5 Hash de un archivo transmitido). Desde el centro de administración pueden realizarse consultas de la base de datos de registros de conversaciones.

En el caso de las cuentas activas, el contenido de los registros estará disponible en línea durante los dos años siguientes a la finalización de una sesión de asistencia remota y se archivará durante los dos años siguientes.

Para facilitar la integración con los sistemas CRM, Rescue puede publicar los detalles de la sesión en una URL, y los administradores pueden optar por excluir el texto del chat de estos detalles. El texto del chat se incluye de forma predeterminada, pero los clientes pueden cambiar esa configuración en el centro de administración. Además, todos los registros de texto de chat entre técnicos y usuarios finales pueden omitirse automáticamente de los detalles de sesión almacenados en un centro de datos de Rescue. Rescue permite a los técnicos grabar en un archivo de vídeo los acontecimientos que tienen lugar durante una sesión de visualización de escritorio o de control remoto. Los archivos grabados se almacenan en un directorio especificado por el técnico.

# 11 Detección y respuesta a terminales

El software de detección y respuesta a terminales con registro de auditoría se implementa en todos los servidores GoTo para minimizar las interrupciones o el impacto en el rendimiento del Servicio. Se iniciarán investigaciones de seguridad de acuerdo con nuestros procedimientos de respuesta a incidentes si se detecta una actividad sospechosa, según proceda y sea necesario. Consulte la sección 17 para obtener más información sobre el Centro de Operaciones de Seguridad de GoTo y los procedimientos de respuesta ante incidentes.

# 12 Gestión de amenazas

El Equipo de respuesta a incidentes de ciberseguridad ("CSIRT") de GoTo está compuesto por varios equipos y es responsable de la protección frente a ciberamenazas. En concreto, el equipo de inteligencia sobre ciberamenazas dentro del CSIRT recopila, examina y difunde información relativa a las amenazas actuales y emergentes. GoTo se mantiene al día con la inteligencia y mitigación de amenazas mediante la revisión de fuentes abiertas y cerradas, así como la participación en grupos de intercambio y membresías de la industria (IT-ISAC, FIRST.org, etc.).

# 13 Gestión de parches y escaneado de seguridad y vulnerabilidades

GoTo mantiene un programa formal de gestión de parches y, al menos trimestralmente, realiza actividades de gestión de parches en todos los sistemas, dispositivos, firmware, sistemas operativos, aplicaciones y demás software relevantes que procesan el Contenido del cliente. GoTo evalúa y escanea las vulnerabilidades a nivel de sistema, host/red internas y externas (“Sistemas”), con una periodicidad no inferior a un mes, así como después de cualquier cambio material en dichos Sistemas y remedia las vulnerabilidades relevantes descubiertas de acuerdo con las políticas documentadas que priorizan la resolución en función del riesgo.

# 14 Control de acceso lógico de GoTo

Existen procedimientos de control de acceso lógico para reducir el riesgo de acceso no autorizado a las aplicaciones y la pérdida de datos en entornos de empresa y de producción. A los empleados de GoTo se les concede acceso a los sistemas, aplicaciones, redes y dispositivos GoTo especificados en función del principio del menor privilegio. Los privilegios de los usuarios se segregan en función del rol funcional (control de acceso basado en roles) y del entorno con controles, procesos o procedimientos de segregación de funciones.

# 15 Segregación de datos

GoTo aprovecha una arquitectura multiusuario, separada de forma lógica a nivel de base de datos, basada en la cuenta GoTo de un usuario o de una organización. Las partes deben autenticarse para acceder a una cuenta. GoTo también ha implementado controles para evitar que los usuarios o usuarios finales vean los datos de otros usuarios o usuarios finales.

# 16 Defensa perimetral y detección de intrusiones

GoTo utiliza herramientas, técnicas y servicios de protección perimetral para protegerse contra el tráfico de red no autorizado que entra en la infraestructura de productos de GoTo. Estos incluyen, pero no se limitan a:

- sistemas de detección de intrusos que supervisan sistemas, servicios, redes y aplicaciones en busca de accesos no autorizados;
- Supervisión de sistemas críticos y archivos de configuración para evitar o reducir la probabilidad de modificaciones no autorizadas
- Cortafuegos de aplicaciones web (WAF) y servicio de prevención de DDoS en la capa de aplicación, a través del cual se aplica un proxy al tráfico de GoTo para bloquear el tráfico malicioso del servidor
- Cortafuegos de aplicaciones local que proporciona una capa más de protección contra las diez principales vulnerabilidades de OWASP y otras vulnerabilidades o tráfico malicioso de las aplicaciones web
- cortafuegos basados en host en los servidores web GoTo que filtran las conexiones de entrada y salida, incluidas las conexiones internas entre sistemas GoTo.

# 17 Operaciones de seguridad y gestión de incidentes

El Centro de Operaciones de Seguridad (SOC) de GoTo se encarga de detectar y responder a los eventos de seguridad. El SOC utiliza sensores de seguridad y sistemas de análisis para identificar posibles problemas y ha desarrollado procedimientos de respuesta a incidentes, incluido un Plan de respuesta a incidentes documentado.

El Plan de respuesta a incidentes de GoTo está alineado con los procesos críticos de comunicación, las políticas y los procedimientos operativos estándar de GoTo. Está diseñado para gestionar, identificar y resolver eventos de seguridad relevantes, sospechosos o identificados, en todos sus sistemas y servicios, incluido Rescue. El Plan de respuesta a incidentes establece los mecanismos para que los empleados informen sobre sospechas de incidentes de seguridad y las vías de escalada que seguir cuando corresponda. Los sucesos sospechosos se documentan y escalan según corresponda a través de tickets de sucesos estandarizados y se clasifican en función de su criticidad.

# 18 Eliminación y devolución de contenidos

**Eliminación o devolución:** los clientes pueden solicitar la devolución o eliminación de su Contenido del cliente al enviar una solicitud desde el Portal de gestión de derechos individuales ("IRM") de GoTo, a través de support.logmeinrescue.com o mediante un correo electrónico a privacy@goto.com. Las solicitudes se tramitarán en un plazo de treinta (30) días a partir de su recepción por parte de GoTo; no obstante, en el improbable caso de que necesitemos más tiempo, notificaremos lo antes posible cualquier retraso previsto y revisaremos el plazo de finalización.

**Calendario de retención del Contenido del cliente:** a menos que la legislación aplicable exija lo contrario, el Contenido del cliente se eliminará automáticamente durante los 140 días posteriores a la terminación, cancelación o caducidad y, en cada caso, el desabastecimiento de la suscripción del Cliente en ese momento.

Previa solicitud por escrito, GoTo podrá proporcionar una confirmación o certificación por escrito de la eliminación del Contenido.

# 19 Controles organizativos

## 19.1 Políticas y procedimientos de seguridad

GoTo mantiene un amplio conjunto de políticas y procedimientos de seguridad que se revisan y actualizan periódicamente según sea necesario para apoyar los objetivos de seguridad de GoTo, los cambios en la legislación aplicable, las normas del sector y los esfuerzos de cumplimiento.

## 19.2 Gestión de cambios

GoTo mantiene un proceso de gestión de cambios adecuado y los cambios en los sistemas GoTo se evalúan, prueban y aprueban antes de su implementación para reducir el riesgo de interrupción de los servicios de GoTo.

## 19.3 Programas de sensibilización y formación en materia de seguridad

El programa de concienciación sobre privacidad y seguridad de GoTo implica la formación de los empleados sobre la importancia de la gestión de datos personales y la información confidencial de forma ética, responsable, de acuerdo con la legislación aplicable y con el debido cuidado. Se informa a los empleados, contratistas y becarios recién contratados de las políticas de seguridad y del Código de conducta y ética empresarial de GoTo durante su incorporación. Los empleados de GoTo realizan una formación de concienciación sobre privacidad y seguridad al menos una vez al año. Las actividades de concienciación tienen lugar a lo largo del año y pueden incluir campañas para el Día de la Privacidad de los Datos, el Mes de la Concienciación sobre Ciberseguridad, seminarios web con el director de seguridad de la información y un programa de campeones de seguridad.

Cuando proceda, también se podrá exigir a los empleados que completen cursos de formación específicos para su función. Además, todos los empleados, contratistas y filiales de GoTo deben revisar y adherirse a las políticas de GoTo relacionadas con la seguridad y la protección de datos.

# 20 Prácticas de privacidad

GoTo se toma muy en serio la privacidad de nuestros Clientes, Usuarios y Usuarios finales y se compromete a divulgar las prácticas relevantes del tratamiento y gestión de datos de forma abierta y transparente.

## 20.1 Programa de privacidad

GoTo mantiene un amplio programa de privacidad que implica la coordinación de numerosas funciones dentro de la empresa, incluidas la privacidad, seguridad, gobierno, riesgo y cumplimiento (GRC), aspectos legales, producto, ingeniería y marketing. Este programa de privacidad se centra en los esfuerzos de cumplimiento e implica la aplicación y el mantenimiento de políticas internas y externas, normas y anexos para regir las prácticas de la empresa.

## 20.2 Cumplimiento de la normativa

### 20.2.1 RGPD

El Reglamento General de Protección de Datos (RGPD) es una ley de la Unión Europea (UE) relativa a la protección de datos y la privacidad de las personas dentro de la UE. GoTo mantiene un programa integral de cumplimiento del RGPD

y, en la medida en que GoTo participe en el procesamiento de Datos Personales sujetos al RGPD en nombre del Cliente, lo haremos de conformidad con los requisitos aplicables del RGPD. Si desea más información, visite https://www.goto.com/company/trust/privacy.

### 20.2.2 CCPA

La Ley de Privacidad del Consumidor de California, modificada por la Ley de Derechos de Privacidad de California (denominadas colectivamente "CCPA", por sus siglas en inglés), otorga a los californianos derechos y protecciones adicionales sobre la forma en que las empresas pueden utilizar su información personal. GoTo mantiene un programa de cumplimiento exhaustivo y, en la medida en que GoTo participe en el procesamiento de Datos personales sujetos a la CCPA en nombre del Cliente, lo haremos de conformidad con los requisitos aplicables de la CCPA. Para obtener más información sobre nuestro cumplimiento de la CCPA, consulte la Política de privacidad de GoTo y las Declaraciones complementarias de la Ley de Privacidad del Consumidor de California.

### 20.2.3 LGPD

La Ley Brasileña de Protección de Datos (LGPD) regula el tratamiento de Datos personales en Brasil o de individuos ubicados en Brasil en el momento de su recogida. GoTo mantiene un programa de cumplimiento exhaustivo y, en la medida en que GoTo participe en el procesamiento de Datos personales sujetos a la LGPD en nombre del Cliente, lo haremos de conformidad con los requisitos aplicables de la LGPD. Si desea más información, visite https://www.goto.com/company/trust/privacy.

## 20.3 Anexo de tratamiento de datos

GoTo ofrece un Anexo de tratamiento de datos (ATD) global, disponible en inglés y alemán. Este ATD cumple los requisitos de RGPD, CCPA, LGPD y otras normativas aplicables y regula el procesamiento por parte de GoTo del Contenido del cliente.

En concreto, nuestro ATD incorpora varias protecciones de la privacidad de los datos centradas en el RGPD, entre las que se incluyen:

(a) los detalles del procesamiento de datos y las revelaciones de los subprocesadores, tal y como exige el artículo 28;
(b) las Cláusulas Contractuales Tipo revisadas (2021) (es decir, las Cláusulas modelo de la UE); y
(c) las medidas técnicas y organizativas específicas del producto de GoTo.

Además, para dar cuenta de los requisitos de la CCPA, nuestro ATD global incluye:

a) definiciones revisadas y adaptadas a la CCPA;
b) derechos de acceso y supresión, y
c) garantías de que GoTo no venderá la información personal de nuestros Clientes, Usuarios y Usuarios finales.

Nuestro ATD global también incluye disposiciones para:

(a) abordar el cumplimiento de la LGPD por parte de GoTo;
(b) apoyar las transferencias legales de Datos personales a/desde Brasil; y
(c) garantizar que nuestros usuarios disfruten de los mismos beneficios de privacidad que el resto de nuestros usuarios globales

## 20.4 Marcos de transferencia

GoTo apoya las transferencias internacionales legales de datos bajo los siguientes marcos:

### 20.4.1 Cláusulas Contractuales Tipo

Las Cláusulas Contractuales Tipo (CCT), a veces denominadas Cláusulas modelo de la UE, son cláusulas contractuales estandarizadas, reconocidas y adoptadas por la Comisión Europea, para garantizar que cualquier dato personal que salga del Espacio Económico Europeo (EEE) se transferirá de conformidad con la legislación de la UE en materia de protección de datos. Las CCT, revisadas y publicadas en 2021, se incorporan al ATD global de GoTo para permitir a los clientes de GoTo transferir datos fuera del EEE de conformidad con el RGPD.

### 20.4.2 Certificaciones CBPR y PRP de APEC

GoTo ha obtenido las certificaciones Reglas de Privacidad Transfronteriza (CBPR) y Reconocimiento de Privacidad para Procesadores (PRP) de la Cooperación Económica Asia-Pacífico (APEC). Los marcos de CBPR y PRP de APEC son los primeros marcos de regulación de datos aprobados para la transferencia de datos personales entre países miembros de APEC y se obtuvieron y validaron de forma independiente a través de TrustArc, un proveedor externo de cumplimiento de protección de datos que cuenta con la aprobación de APEC.

## 20.5 Medidas complementarias

Además de las medidas especificadas en estas MTO, GoTo ha creado una lista de preguntas frecuentes para resumir las medidas complementarias implementadas para apoyar las transferencias legales bajo el Capítulo 5 del RGPD y abordar y guiar cualquier análisis caso por caso recomendado por el Tribunal de Justicia Europeo en conjunción con el uso de las CCT.

## 20.6 Solicitudes de datos

GoTo mantiene procesos exhaustivos para facilitar la recepción de solicitudes relacionadas con la protección de datos y la seguridad, incluido el portal IRM, la dirección de correo electrónico sobre privacidad (privacy@goto.com) y el servicio de atención al cliente en https://support.goto.com.

## 20.7 Declaraciones para representantes y centros de datos

GoTo publica las Declaraciones para representantes en el Trust & Privacy Center (https://www.goto.com/company/trust/resource-center). Estas divulgaciones muestran los nombres, ubicaciones y propósitos de procesamiento de los proveedores de alojamiento de datos y otros terceros que procesan el Contenido del cliente como parte de la prestación del Servicio a los Clientes de GoTo.

## 20.8 Restricciones de tratamiento de datos sensibles

A menos que GoTo lo solicite expresamente o que el Cliente haya recibido permiso por escrito de GoTo, los siguientes tipos de datos confidenciales no deben cargarse en Rescue ni proporcionarse de otro modo a GoTo:

- números de identificación emitidos por el gobierno e imágenes de documentos de identificación
- información relacionada con la salud de una persona, incluida, entre otras, la Información Protegida sobre la Salud (IPS), tal y como se identifica en la Ley de

Portabilidad y Responsabilidad de los Seguros Sanitarios (HIPAA) de EE. UU., así como otras leyes y normativas pertinentes aplicables.

- información relacionada con cuentas financieras e instrumentos de pago, incluidos, entre otros, los datos de tarjetas de crédito La única excepción general a esta disposición se extiende a los formularios y páginas de pago explícitamente identificados que GoTo utiliza para cobrar el pago del Servicio.
- Cualquier información especialmente protegida por las leyes y normativas aplicables, en concreto información sobre la raza, etnia, creencias religiosas o políticas, pertenencia a organizaciones, etc. de la persona.

### 20.9 Cumplimiento en entornos regulados

Los clientes son responsables de aplicar las políticas, procedimientos y otras medidas de seguridad adecuadas en relación con su uso de Rescue para ofrecer compatibilidad con dispositivos en entornos regulados.

## 21 Controles de seguridad y privacidad de terceros

Antes de contratar a proveedores externos que procesen Contenido del cliente o datos confidenciales, sensibles o de los empleados, GoTo revisará y analizará las prácticas de seguridad y privacidad del proveedor a través de los canales de Adquisición correspondientes. Según proceda, GoTo podrá obtener y evaluar periódicamente la documentación o los informes de cumplimiento de los proveedores para asegurarse de que su entorno de control y sus normas siguen siendo suficientes.

GoTo celebra acuerdos por escrito con todos los proveedores externos y utiliza plantillas de contratación aprobadas por GoTo o negocia los términos y condiciones estándar de dichos terceros para cumplir las normas de privacidad y seguridad que ha aceptado GoTo, cuando lo considera necesario. Los equipos de finanzas, jurídico, privacidad y seguridad participan en el proceso de revisión de proveedores y verifican que estos cumplan los requisitos contractuales y de tratamiento de datos obligatorios específicos, según sea necesario o apropiado. Las políticas de riesgo de terceros de GoTo regulan los requisitos de privacidad y seguridad de los proveedores en función del tipo y la duración del procesamiento de datos y el nivel de acceso. Cuando procede (por ejemplo, cuando se procesa o almacena el Contenido del cliente), los acuerdos con los proveedores incluyen requisitos de “cumplimiento de la legislación aplicable”, un ATD o un documento similar que aborde temas como el RGPD, la CCPA, la LGPD y restricciones de uso y venta, según corresponda. Del mismo modo, se establecen anexos de seguridad con controles y requisitos de sistemas adecuados con los proveedores pertinentes. La DPA del proveedor de GoTo tiene restricciones en torno a la “venta” de datos según la definición de la CCPA.

## 22 Contactar con GoTo

Los clientes pueden ponerse en contacto con GoTo en https://support.goto.com para consultas generales. Para enviar preguntas o solicitudes relacionadas con los datos personales o la privacidad, visite nuestro portal IRM o envíe un correo electrónico a privacy@goto.com.