# MEDIDAS TÉCNICAS Y ORGANIZATIVAS PARA GOTOMYPC

**CONTROLES OPERATIVOS DE SEGURIDAD Y PRIVACIDAD**

**Fecha de publicación: febrero de 2022**

# 1 Productos y servicios

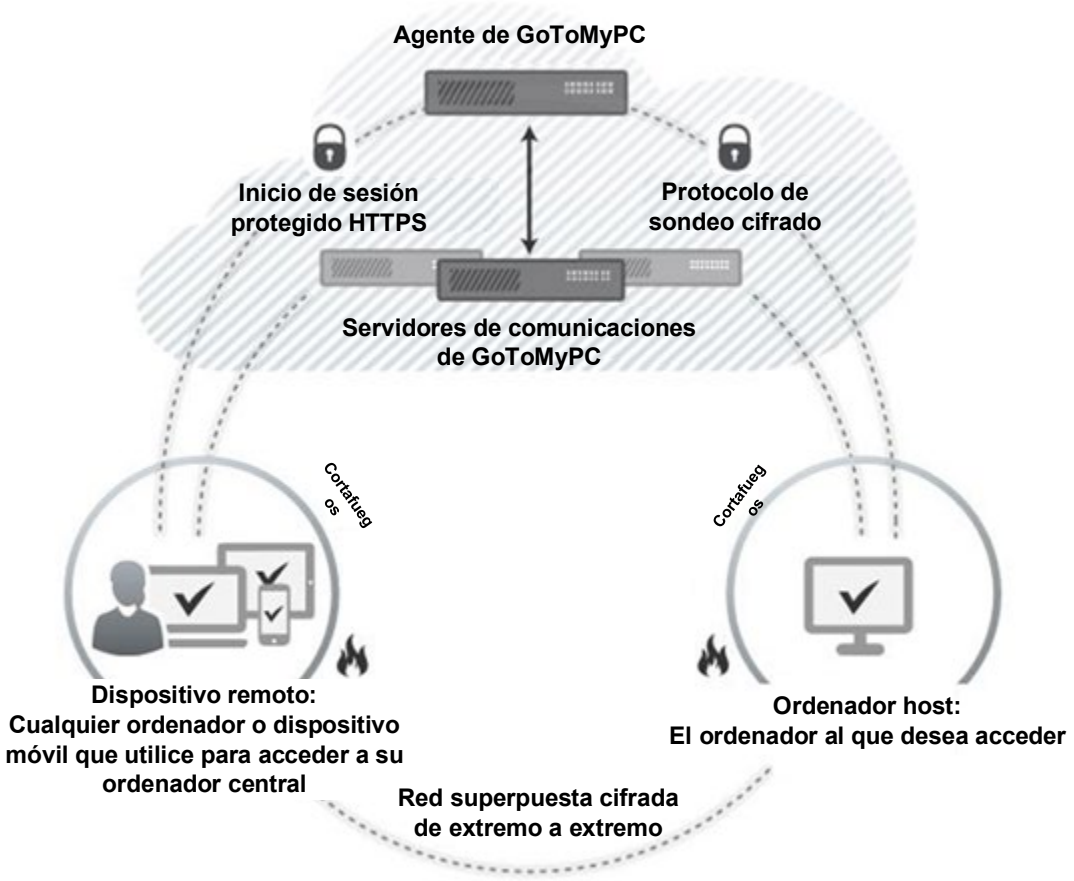
Este documento analiza las medidas técnicas y organizativas (TOM) de GoToMyPC, un servicio alojado que permite el acceso remoto seguro a un ordenador host basado en Windows o Mac conectado a Internet desde cualquier ordenador remoto, iPad, iPhone o dispositivo Android. Entre sus funciones se incluyen un visor para compartir pantalla, transferencia de archivos mediante arrastrar y soltar, impresión remota, invitaciones, uso con varios monitores, aplicaciones móviles y chat. Existen tres versiones de GoToMyPC para satisfacer las necesidades de profesionales, equipos, y pequeñas y medianas empresas (PYMES).

# 2 Arquitectura del producto

GoToMyPC es un servicio alojado que consta de cinco componentes:

- *Ordenador host:* normalmente, un ordenador doméstico o de oficina con acceso permanente a Internet en el que se instala un servidor de pequeño tamaño. Este servidor se registra y autentica con el agente GoToMyPC.
- *Navegador:* desde el ordenador remoto, denominado cliente, el usuario inicia un navegador web, visita el sitio web seguro de GoToMyPC, introduce su nombre de usuario y contraseña y hace clic en “Conectar” para enviar al intermediario una solicitud autenticada y cifrada de acceso al ordenador anfitrión deseado. Como alternativa, el usuario puede instalar la aplicación GoToMyPC en una tablet o smartphone compatible, introducir los datos de su cuenta y hacer clic en “Conectar” para iniciar la solicitud.
- *Agente:* intermediario que escucha las solicitudes de conexión y las asigna a los ordenadores registrados. Cuando se produce una coincidencia, el intermediario asigna la sesión a un servidor de comunicación. A continuación, nuestra herramienta de lanzamiento automático carga automáticamente el visor del cliente, un applet ejecutable específico de la sesión.
- *Servidor de comunicación:* el servidor de comunicación es un sistema intermedio que retransmite un flujo cifrado opaco y altamente comprimido entre los ordenadores cliente y anfitrión durante cada sesión de GoToMyPC.
- *Conexiones directas:* una vez que el usuario se ha autenticado y conectado, GoToMyPC intenta establecer una conexión directa entre el cliente y el host. Para ello, evita el servidor de comunicaciones de GoToMyPC siempre que sea posible para aumentar la velocidad de conexión y mejorar el rendimiento durante la sesión. La función de conexiones directas indica tanto al cliente como al host que escuchen durante un tiempo limitado las conexiones entrantes y que intenten establecer conexiones salientes entre sí; la señal que llegue primero establece la conexión. A continuación, el cliente y el host proceden a ejecutar un acuerdo de claves autenticadas basado en el protocolo de contraseña remota segura (SRP) y establecen una conexión segura que está diseñada de forma que se reduzca o elimine la susceptibilidad a los ataques “man-in the-middle”. Si la conexión directa se bloquea o se interrumpe, la conexión establecida previamente a través del servidor de comunicación mantiene el servicio de acceso remoto. La función de conexiones directas está

siempre activa en las cuentas de GoToMyPC y GoToMyPC Pro, y es opcional en las de GoToMyPC Corporate.




La infraestructura está diseñada de forma resistente y segura. Se diseñan y emplean enrutadores, conmutadores, grupos de servidores y sistemas de copia de seguridad redundantes para garantizar una alta disponibilidad. Para una mayor escalabilidad y fiabilidad, los conmutadores distribuyen de forma transparente las solicitudes entrantes entre los servidores web. Con el fin de garantizar un rendimiento óptimo, el agente de GoToMyPC equilibra la carga de las sesiones cliente/servidor entre servidores de comunicación distribuidos geográficamente.

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

Como el host ya ha establecido una conexión TLS con la puerta de enlace, esta reenvía el intercambio de claves TLS del cliente al host a través de una solicitud de renegociación de claves propias. De este modo, el cliente y el host intercambian claves TLS sin que la puerta de enlace conozca la clave.

# 3 Controles técnicos de GoToMyPC

GoTo utiliza controles técnicos de seguridad estándar en el sector, adecuados a la naturaleza y el alcance de los Servicios (tal y como se define el término en las Términos del servicio) y diseñados para proteger la infraestructura del Servicio y los datos que residen en ella. Puede consultar los Términos del servicio en https://www.goto.com/company/legal/terms-and-conditions.

## 3.1. Control de acceso lógico

Existen procedimientos de control de acceso lógicos, diseñados para prevenir o mitigar la amenaza del acceso no autorizado a las aplicaciones y la pérdida de datos en entornos corporativos y de producción. A los empleados se les concede un acceso básico (o con "privilegios mínimos") a los sistemas, las aplicaciones, las redes y los dispositivos GoTo especificados según sea necesario. Además, los privilegios de los usuarios se segregan según el rol funcional y del entorno.

## 3.2. Defensa perimetral y detección de intrusiones

GoTo utiliza herramientas, técnicas y servicios de protección perimetral estándar del sector, diseñados para evitar que el tráfico de red no autorizado entre en la infraestructura de sus productos. La red GoTo cuenta con cortafuegos externos y segmentación de red interna.

En particular, la seguridad perimetral multicapa la proporcionan un par de cortafuegos: uno entre Internet y los servidores web, y otro entre el agente GoToMyPC y las bases de datos de back-end. Los recursos en la nube también utilizan cortafuegos basados en host. Además, GoTo emplea medidas de protección perimetral, incluido un servicio de prevención de denegación de servicio distribuido (DDoS) de terceros basado en la nube para protegerse contra ataques DDoS volumétricos. Este servicio se prueba al menos una vez al año. Los archivos críticos del sistema están diseñados para ser protegidos contra infecciones o destrucciones maliciosas y no intencionadas.

## 3.3. 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. Solo las partes autenticadas tienen acceso a las cuentas pertinentes.

## 3.4. Seguridad física

**Seguridad física del centro de datos**

GoTo contrata a los centros de datos la seguridad física y los controles ambientales de las salas que albergan los servidores de producción. Estos controles incluyen:

- videovigilancia y grabación
- Autenticación multifactor para zonas muy sensibles
- control de la temperatura de calefacción, ventilación y aire acondicionado
- extinción de incendios y detectores de humo
- Sistema de alimentación ininterrumpida (SAI)
- suelos elevados o gestión integral de cables
- supervisión continua y alertas

- Protección contra las catástrofes naturales o provocadas por el hombre más comunes, según lo exijan la geografía y la ubicación del centro de datos correspondiente
- 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 la presentación de una solicitud a través del sistema de tickets correspondiente y la aprobación del responsable aplicable, así como la revisión y aprobación del Departamento de Operaciones Técnicas. La dirección de GoTo revisa los registros de acceso físico a los centros de datos y las salas de servidores al menos una vez cada trimestre. Además, el acceso físico a los centros de datos se elimina al cesar al personal previamente autorizado.

## 3.5. Copia de seguridad de datos, recuperación ante desastres y disponibilidad

GoToMyPC replica la base de datos casi en tiempo real a un sitio secundario situado en un lugar geográficamente diverso. 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 el sistema se prueba periódicamente.

## 3.6. Protección contra malware

En todos los servidores de GoToMyPC se instala un software de protección contra malware con función de registro de auditoría. Las alertas que indican una posible actividad maliciosa se envían a un equipo de respuesta adecuado.

## 3.7. Cifrado

GoTo mantiene una norma de cifrado que se ajusta a las recomendaciones de grupos industriales, publicaciones gubernamentales y otros grupos de normas aplicables. La norma de cifrado se revisa periódicamente, y las tecnologías y los cifrados seleccionados se actualizan en función del riesgo evaluado y de la aceptación en el mercado de nuevas normas.

### 3.7.1. Cifrado en tránsito

GoToMyPC Corporate ofrece un cifrado Advanced Encryption Standard (AES) de 256 bits. El tráfico entre el cliente del navegador de GoToMyPC y el ordenador host se comprime y cifra. GoToMyPC genera claves de cifrado únicas y secretas para cada conexión mediante un acuerdo de claves totalmente contributivas y autenticadas mutuamente.

## 3.8. Gestión de vulnerabilidades

El análisis de vulnerabilidades de los sistemas internos y externos o de la red se realiza una vez al mes. También realiza periódicamente pruebas de vulnerabilidad y actividades de penetración de aplicaciones dinámicas y estáticas para entornos específicos. Estos resultados del escaneado y las pruebas se comunican a las herramientas de supervisión de la red y, si procede, se adoptan medidas correctoras.

GoTo comunica y gestiona las vulnerabilidades mediante el envío de informes mensuales a los equipos de desarrollo y a la dirección.

### 3.9. Registro y alerta

GoTo recopila el tráfico anómalo o sospechoso identificado en los registros de seguridad de los sistemas de producción aplicables.

# 4 Controles organizativos

GoTo mantiene un amplio conjunto de controles organizativos y administrativos para proteger la postura de seguridad y privacidad de GoToMyPC.

## 4.1. Políticas y procedimientos de seguridad

GoTo mantiene un amplio conjunto de políticas y procedimientos de seguridad alineados con los objetivos empresariales, los programas de cumplimiento y la gobernanza corporativa general. Estas políticas y procedimientos se revisan periódicamente y se actualizan según sea necesario para garantizar un cumplimiento continuo.

## 4.2. Cumplimiento de las normas

GoTo cumple con los requisitos legales, financieros, de privacidad de datos y normativos aplicables, y mantiene el cumplimiento de las siguientes certificaciones e informes de auditoría externa:

- 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.
- Informe de certificación de tipo 2 sobre el control de las organizaciones de servicios (SOC) 2 del Instituto Americano de Contables Públicos Certificados (AICPA)
- Informe de atestación del Instituto Americano de Contables Públicos Certificados (AICPA) de Control de Organizaciones de Servicios (SOC) 3 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).

## 4.3. Operaciones de seguridad y gestión de incidentes

El Centro de Operaciones de Seguridad (SOC) de GoTo cuenta con personal del equipo de operaciones de seguridad y 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 un plan de respuesta a incidentes que rige las respuestas correspondientes.

El plan de respuesta a incidentes se ajusta a los procesos críticos de comunicación de GoTo, la Política de gestión de incidentes de seguridad de la información y los procedimientos operativos estándar asociados. Está diseñado para gestionar, identificar y resolver posibles

incidentes de seguridad en todos sus sistemas y servicios, incluido GoToMyPC. De acuerdo con el plan de respuesta a incidentes, el personal técnico identificará posibles eventos y vulnerabilidades relacionados con la seguridad de la información y escalará cualquier evento sospechoso o confirmado a la dirección. Los empleados pueden informar de los incidentes de seguridad por correo electrónico, teléfono o ticket, según el proceso documentado en el sitio de la intranet de GoTo. Los sucesos identificados o sospechosos se documentan y escalan a través de tickets de sucesos estandarizados y se clasifican en función de su criticidad.

### 4.4. Seguridad de las aplicaciones

El programa de seguridad de aplicaciones de GoTo se basa en el ciclo de vida de desarrollo de seguridad (SDL) de Microsoft para asegurar el código de los productos. Los elementos centrales de este programa son las revisiones manuales del código, el modelado de amenazas, el análisis estático del código, el análisis dinámico y el refuerzo del sistema.

### 4.5. Seguridad del personal

Los antecedentes de los nuevos empleados se comprobarán antes de la fecha de contratación en la medida que lo permita la legislación aplicable y según corresponda al puesto. Los resultados se mantienen en el expediente laboral del empleado. Los criterios de comprobación de antecedentes variarán en función de las leyes, la responsabilidad laboral y el nivel de liderazgo del posible empleado, y están sujetos a las prácticas comunes y aceptables del país en cuestión.

### 4.6. Programas de sensibilización y formación en materia de seguridad

Se informa a los nuevos empleados de las políticas de seguridad y del Código de conducta y ética empresarial de GoTo durante la orientación. Esta formación anual obligatoria sobre seguridad y privacidad se imparte al personal correspondiente y la gestiona el Departamento de Desarrollo de Talentos con el apoyo del equipo de seguridad.

Los empleados y trabajadores temporales de GoTo reciben información sobre las directrices, procedimientos, políticas y normas de seguridad y privacidad periódicamente a través de diversos medios, entre los que se incluyen kits de incorporación para nuevos empleados, campañas de concienciación, seminarios web con el CISO, un programa de campeones de seguridad y exhibiciones de carteles u otros materiales, que se rotan al menos dos veces al año e ilustran los métodos para proteger los datos, los dispositivos y las instalaciones.

## 5 Prácticas de privacidad

GoTo se toma muy en serio la privacidad de los Clientes, los suscriptores de los Servicios GoTo y los usuarios finales, y se compromete a divulgar las prácticas de gestión y manejo de datos de forma abierta y transparente.

### 5.1. RGPD

El Reglamento General de Protección de Datos (RGPD) es una ley de la Unión Europea (UE) que rige la protección y privacidad de los datos de los residentes en la Unión Europea. El objetivo principal del RGPD es ceder el control de sus datos personales a los ciudadanos y residentes, y también simplificar el entorno reglamentario en la UE. GoToMyPC cumple

con las disposiciones aplicables del RGPD. Para obtener más información, visite https://www.goto.com/company/trust/privacy.

## 5.2. CCPA

GoTo garantiza que cumple con la Ley de Privacidad del Consumidor de California (CCPA). Para obtener más información, visite https://www.goto.com/company/trust/privacy.

## 5.3. Protección de datos y política de privacidad

GoTo ofrece un Anexo de tratamiento de datos (DPA) global y completo, disponible en inglés y alemán, para cumplir con los requisitos del RGPD, la CCPA y otras normativas, y que rige el tratamiento de datos personales por parte de GoTo.

En concreto, el DPA abarca varios aspectos de la protección la privacidad de datos en relación con el RGPD, entre los que se incluyen: (a) detalles del tratamiento de datos, divulgaciones de subprocesadores, etc., tal y como exige el artículo 28; (b) las Cláusulas contractuales tipo de la UE, y (c) la inclusión de las medidas técnicas y organizativas de GoTo. Además, para preparar la entrada en vigor de la CCPA, hemos actualizado nuestro APD global para incluir: (a) definiciones revisadas vinculadas a la CCPA; (b) derechos de acceso y eliminación y (c) garantías de que GoTo no va a vender la "información personal" de los usuarios.

Para los visitantes de nuestras páginas web, GoTo revela los tipos de información que recoge y utiliza para proporcionar, mantener, mejorar y asegurar los Servicios en su Política de Privacidad, en la página web pública. La empresa puede actualizar la Política de privacidad ocasionalmente para reflejar cambios en sus prácticas de información o en la legislación aplicable, pero avisará de ello en su página web antes de que dichos cambios entren en vigor.

## 5.4. Marcos de transferencia

GoTo cuenta con un programa global de protección de datos que tiene en cuenta la ley aplicable y respalda las transferencias internacionales legales conforme a los marcos siguientes:

### 5.4.1. Cláusulas Contractuales Tipo

Las Cláusulas contractuales tipo ("CCT") son cláusulas contractuales estándar, reconocidas y adoptadas por la Comisión Europea, cuyo objetivo principal es garantizar que los datos personales que salgan del Espacio Económico Europeo ("EEE") se transferirá conforme a la legislación de la UE en materia de protección de datos. GoTo ha invertido en un programa de privacidad de datos de primera clase para cumplir con los requisitos de las CCT al transferir datos personales. GoTo proporciona a los clientes las CCT, que establecen garantías específicas para la transferencia de datos personales en los servicios de GoTo como parte del DPA global. La ejecución de las CCT garantiza que los clientes de GoTo puedan transferir datos libremente del EEE al resto del mundo.

#### Medidas complementarias

Aparte de las medidas especificadas en estas TOM, GoTo ha creado las siguientes preguntas frecuentes para esbozar las medidas complementarias que respaldarán

las transferencias legales conforme al capítulo 5 del RGPD y regir los análisis “caso por caso” recomendados por el Tribunal de Justicia Europeo junto con las CCT.

### 5.4.2. Certificaciones CBPR y PRP de APEC

GoTo también 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 líder en el cumplimiento de la protección de datos de APEC.

## 5.5. Devolución y eliminación del Contenido del cliente

En cualquier momento, los Clientes de GoToMyPC podrán solicitar la devolución o eliminación de sus Contenidos a través de interfaces estandarizadas. Si estas interfaces no están disponibles o GoTo no puede completar la solicitud, GoTo hará todo lo posible para ayudar al Cliente a recuperar o eliminar su Contenido, sujeto a la viabilidad técnica.

El Contenido del cliente se eliminará en un plazo de treinta (30) días a partir de la solicitud del Cliente. Además, el Contenido del cliente en GoToMyPC se eliminará automáticamente en un plazo de noventa (90) días tras la expiración o finalización del último periodo de suscripción. Previa solicitud por escrito, GoTo certificará la eliminación del Contenido.

## 5.6. Datos sensibles

Aunque GoTo intenta proteger el Contenido del cliente, las limitaciones normativas y contractuales nos obligan a restringir el uso de GoToMyPC a determinados tipos de información. A menos que el Cliente haya recibido permiso por escrito de GoTo, los siguientes datos no deben cargarse, generarse ni introducirse en GoToMyPC:

- 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 o recibir el pago de GoToMyPC.
- 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.

## 5.7. Seguimiento y análisis

GoTo mejora continuamente sus sitios web y productos mediante herramientas de análisis web de terceros, que ayudan a GoTo a comprender cómo utilizan los visitantes sus sitios web, herramientas de escritorio y aplicaciones móviles, así como las preferencias y los problemas de los usuarios. Para obtener más información, consulte la Política de privacidad.

# 6 Terceros

## 6.1. Uso de terceros

Como parte de la evaluación interna y de los procesos relacionados con proveedores y terceros, las evaluaciones de proveedores pueden realizarlas varios equipos en función de su relevancia y aplicabilidad. El equipo de seguridad evalúa a los proveedores que prestan servicios basados en la seguridad de la información, incluida la evaluación de las instalaciones de alojamiento de terceros. Los equipos del Departamento Jurídico y de Adquisiciones pueden evaluar los contratos, las declaraciones de trabajo y los acuerdos de servicio según sea necesario, de acuerdo con los procesos internos. La documentación o los informes de cumplimiento se pueden obtener y evaluar al menos una vez al año, según se considere oportuno, para garantizar que el entorno de control funciona adecuadamente y que se abordan los controles de consideración del usuario correspondientes. Además, los terceros alojen datos sensibles y confidenciales (o a los que GoTo conceda acceso a ellos) deben firmar un contrato por escrito en el que se indiquen los requisitos para el acceso a la información o su almacenamiento y manipulación, según proceda.

## 6.2. Prácticas contractuales

Para garantizar la continuidad del negocio y que se apliquen las medidas adecuadas para proteger la confidencialidad y la integridad de los procesos empresariales y el tratamiento de datos de terceros, GoTo revisa los términos y condiciones de los terceros pertinentes y utiliza las plantillas de contratación aprobadas por GoTo o negocia dichos términos de terceros si lo considera necesario.

# 7 Contactar con GoTo

Los clientes pueden ponerse en contacto con GoTo en https://support.goto.com para consultas generales o enviar un correo electrónico a privacy@goto.com para preguntas relacionadas con la privacidad.