# Medidas técnicas y organizativas
## GoTo Meeting, GoTo Webinar, GoTo Training y GoTo Stage

## Resumen

Este documento de Medidas técnicas y organizativas ("MTO") establece los compromisos de privacidad, seguridad y responsabilidad de GoTo para GoTo Meeting, GoTo Webinar, GoTo Training y GoTo Stage. 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) o seguridad de la capa de transporte de datagramas (DTLS).
  - *En reposo:* cifrado de datos transparente (TDE) y estándar de cifrado avanzado (AES) de 256 bits para el Contenido del cliente que se cifra en reposo.
- **Centros de datos:** GoTo recurre a proveedores de alojamiento en la nube que emplean medidas para proporcionar seguridad lógica y física, disponibilidad y escalabilidad elevadas.
- **Auditorías de cumplimiento:** GoTo Meeting, GoTo Webinar and GoTo Training tienen las certificaciones SOC 2 Tipo II, C5, PCI DSS, PCAOB, TRUSTe Enterprise Privacy, y CBPR y PRP de APEC.
- **Cumplimiento legal/normativo:** GoTo mantiene un programa integral de protección de datos con procesos y políticas, diseñado para garantizar que el Contenido del cliente se gestione de acuerdo con las leyes de privacidad aplicables (RGPD, CCPA/CPRA y 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 en la capa de almacenamiento.
- **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 GoTo Meeting, GoTo Webinar, GoTo Training y GoTo Stage 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.
  - Para GoTo Meeting, GoTo Webinar y GoTo Training, el Contenido del Cliente se eliminará automáticamente entre 90 y 100 días después de la expiración del plazo de suscripción del Cliente en ese momento.

Versión 4.0 | Abril de 2024

# Índice

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


*Resumen* ..... *1*

*Índice* ..... *2*

*1 Introducción al producto* ..... *3*

*2 Medidas técnicas* ..... *5*

*3 Arquitectura del producto* ..... *5*

*4 Controles técnicos de seguridad* ..... *7*

*5 Actualizaciones del programa de seguridad* ..... *11*

*6 Copia de seguridad de datos, recuperación ante desastres y disponibilidad* ..... *11*

*7 Centros de datos* ..... *11*

*8 Cumplimiento de las normas* ..... *12*

*9 Seguridad de las aplicaciones* ..... *12*

*10 Registro, supervisión y alertas* ..... *12*

*11 Detección y respuesta a terminales* ..... *13*

*12 Gestión de amenazas* ..... *13*

*13 Gestión de parches y escaneado de seguridad y vulnerabilidades* ..... *13*

*14 Control de acceso lógico* ..... *13*

*15 Segregación de datos* ..... *13*

*16 Defensa perimetral y detección de intrusiones* ..... *14*

*17 Operaciones de seguridad y gestión de incidentes* ..... *14*

*18 Eliminación y devolución de contenidos* ..... *14*

*19 Controles organizativos* ..... *15*

*20 Prácticas de privacidad* ..... *16*

*21 Controles de seguridad y privacidad de terceros* ..... *19*

*22 Contactar con GoTo* ..... *19*

# 1 Introducción al producto

GoTo Meeting, GoTo Webinar, GoTo Training y GoTo Stage (en conjunto, el “Servicio”) son soluciones de comunicación en línea que permiten a las personas y a las organizaciones interactuar mediante diversas funciones según la oferta de servicios. Esto incluye el uso compartido de la pantalla del escritorio, las videoconferencias, el chat y el audio integrado. GoTo Meeting, GoTo Webinar, GoTo Training y GoTo Stage comparten infraestructura y se entregan a través de una CDN a navegadores web o aplicaciones instalables.

- GoTo Meeting, GoTo Webinar y GoTo Training permiten a los organizadores programar, convocar y moderar sesiones en línea que incluyen audio, cámara web, pantalla compartida y mucho más mediante las aplicaciones web, móviles y de escritorio de GoTo.
- GoTo Training ofrece características específicas aplicables a la formación web, como el acceso en línea a pruebas y materiales o un catálogo de cursos alojado.
- GoTo Webinar proporciona asistencia especial para organizar eventos de presentación de información impartidos por una persona y para varios asistentes, destinados a asistentes locales y globales a través de Internet.
- GoTo Stage es una extensión de GoTo Webinar donde los organizadores de GoTo Webinar pueden crear canales personalizables y publicar las grabaciones de sus seminarios web. Las grabaciones publicadas se muestran en la página de inicio de GoTo Stage, organizadas por categorías de negocio. Los organizadores pueden retirar en cualquier momento su grabación a través de GoTo Webinar, que elimina el sitio y el vídeo de su página de canal y del ecosistema de GoTo Stage.

## 1.1 Gestión y registro de conferencias

Los organizadores pueden programar las sesiones directamente en el Servicio. Pueden ajustar la configuración de las próximas sesiones y preparar tanto el contenido como los asistentes.

## 1.2 Audio

Las audioconferencias integradas para las sesiones de GoTo Meeting, GoTo Webinar y GoTo Training están disponibles a través del protocolo de voz sobre Internet (VoIP) y la red telefónica pública conmutada (RTPC).

## 1.3 Vídeo

Todos los productos ofrecen vídeo por cámara web de alta calidad, que se ajusta al ancho de banda y la latencia del usuario.

## 1.4 Carga de contenidos (solo Webinar y Training)

Los organizadores pueden cargar archivos y medios para utilizarlos durante las sesiones, ya sea antes o después de que estas comiencen.

## 1.5 Informes sobre las sesiones

Los organizadores pueden ver las estadísticas de participación y otras estadísticas de la sesión en su historial de sesiones.

## 1.6 Grabaciones y transcripciones

Las sesiones pueden grabarse localmente y en la nube. Los administradores de cuentas y los organizadores de sesiones pueden activar las grabaciones en la nube además o en lugar de las grabaciones locales. Las grabaciones locales se almacenan en el sistema del organizador y no están sujetas a los límites de retención de GoTo, enumerados en la sección 18 ("Eliminación y devolución de contenidos").

Las grabaciones en la nube aparecen directamente en el historial de sesiones del organizador, y las transcripciones se crean automáticamente cuando el administrador habilita esta función. Las transcripciones de grabaciones de las sesiones se crean con la tecnología GoTo Voice AI o Google Cloud Speech-to-Text.

En el caso de **GoTo Meeting**, el administrador de la cuenta puede activar las grabaciones y decidir si estas se almacenan localmente o en la nube. Si las grabaciones en la nube están activadas, el organizador de la reunión puede grabar una reunión determinada y almacenarla en la nube. Las transcripciones se crean automáticamente para las grabaciones en la nube.

En el caso de **GoTo Webinar**, los organizadores pueden transcribir automáticamente todas las grabaciones en la nube. Solo un organizador puede iniciar una grabación; si su configuración de transcripción automática está activada, se creará una transcripción.

En el caso de **GoTo Training**, los administradores de cuentas pueden controlar si los organizadores guardan las grabaciones en la nube. Los administradores de cuentas no pueden impedir que los organizadores graben sesiones localmente. Los cursos de formación no pueden transcribirse.

## 1.7 Mensajería empresarial (solo reunión)

Mensajería empresarial, una extensión de GoTo Meeting, permite a los usuarios de GoTo Meeting ver si otros usuarios de su cuenta están presentes, intercambiar mensajes instantáneos y compartir archivos. El administrador de la cuenta define el ámbito de visibilidad y detección de los distintos usuarios.

Los usuarios de Mensajería empresarial pueden ver si cualquier otro usuario de su cuenta está presente, siempre que lo hayan agregado a su lista de contactos. Se pueden intercambiar mensajes con todos los miembros de un equipo y, si se agregan explícitamente a través de una invitación por correo electrónico, con usuarios externos. Los usuarios externos son usuarios de Mensajería empresarial que no pertenecen al equipo interno de un cliente (por ejemplo, un cliente, un posible cliente o un socio). Los mensajes pueden ser directos (entre dos participantes), en un grupo privado o en un grupo público.

Los usuarios también pueden compartir contenidos arbitrarios en Mensajería empresarial simplemente subiendo y descargando archivos. Los archivos compartidos están disponibles para que los descarguen todos los usuarios con acceso a los mensajes de una conversación o un grupo determinados.

## 1.8 Webcast (solo Webinar)

Los webcasts de GoTo Webinar utilizan puertas de enlace de difusión, motores de transmisión de terceros y redes de entrega de contenidos diseñadas para entregar la pantalla compartida, el audio y el vídeo a los asistentes que se unan desde un navegador web. Las puertas de enlace reciben los datos multimedia de los servidores multimedia y los transcodifican en códecs estándar. El motor de transmisión genera transmisiones en vivo HTTP (HLS) a varias velocidades de bits para permitir la entrega adaptativa a usuarios con conexiones de red subóptimas.

## 1.9 GoTo Stage (solo Webinar)

Todos los vídeos publicados en GoTo Stage pueden encontrarse buscando en la página de inicio de GoTo Stage y en los resultados de motores de búsqueda, a menos que el organizador limite el acceso con los ajustes de administrador en su página de canal. Cualquier persona registrada en GoTo Stage puede acceder a las grabaciones no detectadas mediante una URL directa al canal o a la página exclusiva “Ver ahora” del vídeo. Los visitantes se registran en GoTo Stage con su nombre y dirección de correo electrónico o se conectan a través de sus cuentas de redes sociales (por ejemplo, LinkedIn, Facebook y Gmail). Las direcciones URL para que los visitantes accedan a los vídeos se activan durante un tiempo limitado para limitar los intercambios no deseados.

# 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 en GoTo Meeting, GoTo Webinar y GoTo Training.

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 el RGPD, la CCPA/CPRA, la LGPD y nuestro Anexo de tratamiento de datos (DPA), así como las políticas y divulgaciones públicas 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 que pueden configurarse en el servicio ayudan a los administradores a minimizar las amenazas y los riesgos para el Contenido del cliente.

# 3 Arquitectura del producto

GoTo Meeting, GoTo Webinar, GoTo Training y GoTo Stage son soluciones de software como servicio (SaaS) diseñadas para proporcionar rendimiento, fiabilidad, escalabilidad y seguridad elevados. Estos Servicios están respaldados por servidores y equipos de red de alta capacidad con unos controles de seguridad adecuados, así como una infraestructura redundante diseñada para evitar puntos únicos de fallo. Existen servidores en clúster y sistemas de copia de seguridad para respaldar los procesos de las aplicaciones aunque haya cargas pesadas o errores del sistema.

La carga de las sesiones de aplicación/servidor se equilibra a través de clústeres distribuidos geográficamente y diseñados a fin de garantizar un rendimiento y una latencia adecuados.

La infraestructura y los datos del Servicio se ubican en proveedores de alojamiento en la nube.

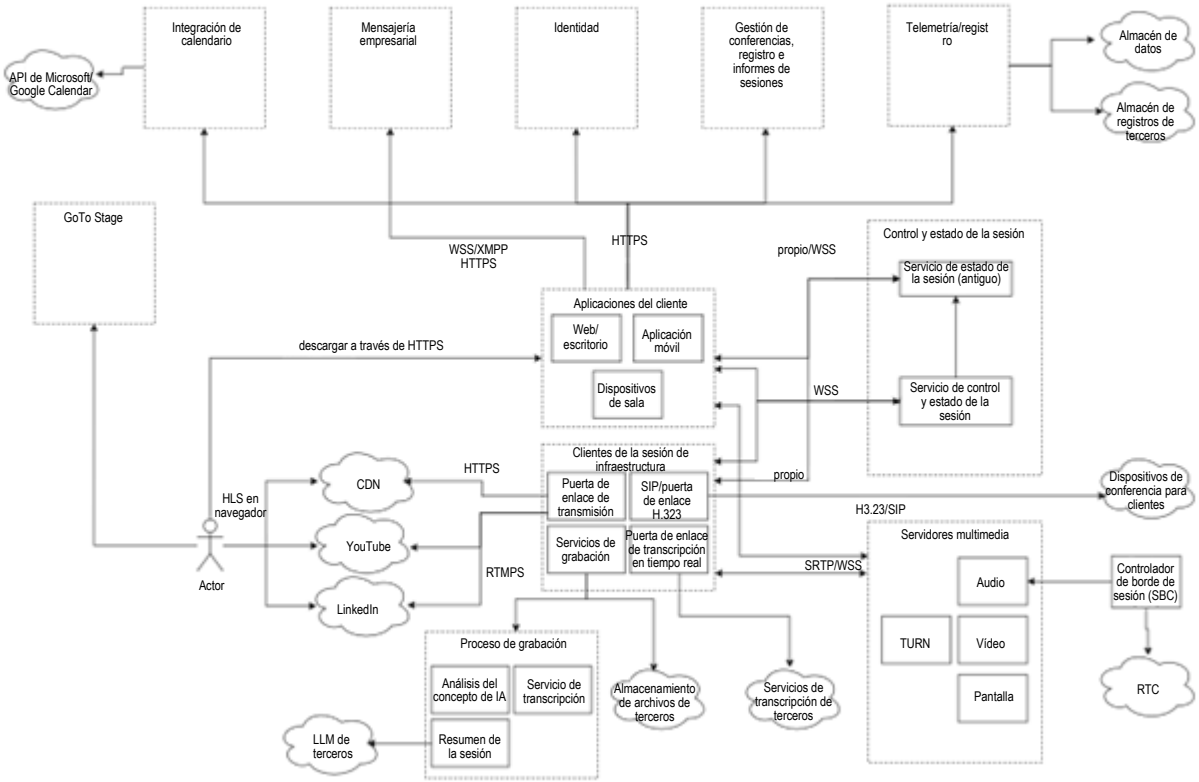


*Figura 1: arquitectura de Central*

*Aplicaciones del cliente (aplicaciones web, móviles y de escritorio de GoTo o "clientes"; un dispositivo llamado GoTo Room [solo para Meeting])*: las aplicaciones del cliente proporcionan la funcionalidad del Servicio descrita anteriormente en la sección 1 ("Presentación del producto").

*Servicios de identidad*: gestiona las cuentas de usuario y permite autorizar cuentas e iniciar sesión de forma segura y estándar.

*Servicios de gestión de conferencias, registro e informes de sesiones:* la gestión de Conferencias proporciona información sobre las sesiones programadas y permite programar sesiones nuevas o ajustar las existentes. Los servicios de registro permiten inscribirse en las sesiones que lo requieran. Los informes de sesiones proporcionan información sobre las sesiones anteriores, incluidas grabaciones, transcripciones, asistencia y mucho más.

*Mensajería empresarial*: gestión de canales; envío, recepción y almacenamiento de mensajes y archivos adjuntos. Se utiliza únicamente con mensajes fuera de la sesión.

*Integración con el calendario*: permite a los usuarios sincronizar sus calendarios de Microsoft Outlook o Google para recibir notificaciones sobre las sesiones de GoTo.

*Telemetría/registro*: envío de sondas de telemetría o declaraciones de registro para recopilar estadísticas de uso y diagnosticar problemas.

*Servicios de control y estado de la sesión*: proporcionan la funcionalidad utilizada por las aplicaciones del cliente para iniciar y recibir cambios no relacionados con los medios en el estado de la sesión.

*Servidores de medios*: responsables de recibir, modificar y distribuir contenidos de audio, vídeo y pantalla compartida.

*RTC*: red telefónica pública conmutada, que permite a los usuarios acceder a las sesiones a través de teléfonos físicos o IP.

*Controlador de borde de sesión*: conecta el protocolo Voz sobre Internet (VoIP) de GoTo con los proveedores de telefonía comercial.

*Servicios de grabación*: permiten grabar el audio de la sesión, el vídeo, la pantalla compartida y el contenido de Mensajería empresarial.

*Puerta de enlace de transmisión*: se utiliza para los webcasts de GoTo Webinar. Permite maquetar, transcodificar o empaquetar los flujos multimedia en flujos HLS, que se distribuyen a clientes que utilizan el navegador a través de CDN o se envían a plataformas de transmisión habilitadas para RTMP, como YouTube o LinkedIn.

*Puerta de enlace H.323/SIP*: permite conectarse a la sesión de audio a través de dispositivos de conferencia SIP o H.323.

*Puerta de enlace de transcripción en tiempo real (RTT)*: proporciona la transcripción en directo del discurso de los participantes en la sesión.

*Servicios GoTo Stage*: gestión del contenido de vídeo de GoTo Webinar por parte de los organizadores; proporciona una experiencia de visualización a los visitantes.

# 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 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.

### 4.1.1 Cifrado en tránsito

GoTo implementa medidas de seguridad para los datos en tránsito, diseñadas para evitar ataques pasivos y activos contra la confidencialidad, la integridad y la disponibilidad. Se implementan controles de seguridad de las comunicaciones para el uso compartido de pantalla y vídeo, VoIP, el vídeo de cámara web, el control del teclado o el ratón, la información de chat de texto y otros datos de la sesión.

GoTo utiliza los protocolos TLS estándar del Grupo de Trabajo de Ingeniería de Internet (IETF) para proteger la comunicación TCP entre terminales.

HTTPS y WSS se utilizan para proteger los datos que no son multimedia, mientras que los datos multimedia de la sesión se protegen con SRTP, WSS o DTLS.

Internamente, GoTo también utiliza la autenticación mutua basada en certificados (mTLS) en los servidores que manejan datos multimedia.

#### 4.1.1.1 Seguridad de audio y vídeo

Para proteger la confidencialidad y la integridad de las conexiones VoIP entre los terminales y los servidores, se utiliza un protocolo basado en SRTP que emplea mecanismos de cifrado estándar con AES128 como mínimo.

#### 4.1.1.2 Seguridad de sitios web, API y servicios web internos

Todas las conexiones a los sitios web, las API y los servicios web internos del Servicio están protegidos mediante TLS. Esto incluye la carga de contenidos, los informes de sesiones, las grabaciones y transcripciones, etc.

#### 4.1.1.3 Mensajería empresarial

Las actualizaciones de presencia, los mensajes y los archivos se transfieren a través de un canal protegido con TLS a los servicios de chat y de ahí a los usuarios. El contenido del archivo se transmite enlazado a través de URL con firma criptográfica.

#### 4.1.1.4 Seguridad de webcast (solo Webinar)

Las puertas de enlace de transmisión de webcast reenvían el tráfico al motor de transmisión a través de SRTP dentro de la red interna segura de GoTo. Las CDN extraen datos del motor de transmisión de forma segura a través de HTTPS. Los clientes también extraen datos de forma segura de las CDN a través de HTTPS.

### 4.1.2 Cifrado en reposo

#### 4.1.2.1 Datos del perfil

El contenido se almacena en una base de datos relacional con cifrado AES de 256 bits.

#### 4.1.2.2 Gestión de conferencias, registro e informes de sesiones

El contenido se almacena en una base de datos relacional con cifrado AES de 256 bits.

#### 4.1.2.3 Carga de contenidos

El contenido subido y los metadatos asociados se almacenan en AWS S3, Amazon Aurora y Amazon Dynamo DB con cifrado AES de 256 bits. Además, los metadatos se almacenan en Apache Cassandra sin cifrado en reposo.

#### 4.1.2.4 Grabaciones y transcripciones

Las grabaciones en la nube se almacenan en AWS S3. Los archivos se cifran en reposo mediante cifrado en el lado del servidor con AES de 256 bits.

Los archivos de audio para la transcripción se cifran con AES256 y se eliminan justo después de que finalice el procesamiento de voz a texto.

#### 4.1.2.5 Seguridad de Mensajería empresarial

Los mensajes se almacenan en una base de datos de AWS Aurora, mientras que los archivos compartidos se almacenan en AWS S3. Ambos cuentan con cifrado AES de 256 bits en reposo.

#### 4.1.2.6 GoTo Stage

El contenido subido y los metadatos asociados se almacenan en AWS S3 con cifrado AES de 256 bits. Los metadatos se almacenan en Apache Cassandra y el índice de búsqueda en Elasticsearch, ambos sin cifrado en reposo.

## 4.2 Compatibilidad de cortafuegos y proxies

El Servicio incluye detección de proxy integrada y una lógica de gestión de conexiones para automatizar la instalación del software, evitar la necesidad de configuraciones (y reconfiguraciones) de red complejas y maximizar la productividad de los usuarios. Los cortafuegos y proxies ya presentes en la red de un usuario no suelen necesitar ninguna configuración especial para permitir el uso del Servicio.

Para obtener más información y ver los dominios, IP y puertos exactos que se utilizan, visite las páginas de asistencia correspondientes para Meeting, Webinar y Training.

## 4.3 Funciones de seguridad de clientes instalables

Los clientes instalables se diseñan con características de seguridad apropiadas y emplean medidas de cifrado fuertes, incluidos software para terminales firmado y conexiones “solo para clientes”.

### 4.3.1 Software para terminales firmado

Los archivos ejecutables del Servicio se firman digitalmente para proteger su integridad y autenticidad. El software de la aplicación cliente de GoTo sigue procedimientos de control de calidad adecuados, procedimientos de gestión de la configuración y un modelo de ciclo de vida del desarrollo de seguridad (SDL) durante el desarrollo y la implementación.

### 4.3.2 Conexiones “solo para clientes”

Para reducir el riesgo de que los sistemas remotos sufran ataques de malware y virus, los clientes instalables no se configuran para recibir conexiones entrantes. Esto evita que los usuarios que participan en una sesión sean infectados por el host que utiliza otro asistente.

### 4.3.3 Implementación del subsistema criptográfico

Las funciones criptográficas y los protocolos de seguridad implementados en los clientes instalables utilizan las bibliotecas criptográficas de código abierto BoringSSL u OpenSSL. No se exponen API externas que permitan a otro software acceder a las bibliotecas criptográficas incluidas en el cliente.

La aplicación web utiliza las bibliotecas criptográficas del navegador. No existen ajustes criptográficos configurables por el usuario final que den lugar a una configuración errónea, ya sea accidental o intencionada.

## 4.4 Autenticación de usuarios

La autorización basada en roles y los controles de acceso adecuados dependen de la posibilidad de identificar y autenticar a los usuarios. Para garantizar que los organizadores y los asistentes tienen los privilegios correctos, se han integrado funciones de autenticación de cuenta y sesión en el Servicio.

### 4.4.1 Inicio de sesión en la cuenta

Los sitios web del Servicio ofrecen los siguientes métodos de inicio de sesión:

- Inicio de sesión directo con nombre de usuario y contraseña.
- Inicie sesión a través de un proveedor de cuentas sociales o de otro tipo mediante LastPass, Google, Facebook, LinkedIn, Microsoft o Apple (https://support.goto.com/meeting/help/connect-your-social-or-other-account-for-sign-in).
- Inicio de sesión único basado en SAML.

Para el inicio de sesión directo, todas las contraseñas tienen unos requisitos mínimos de caracteres y complejidad. Existen mecanismos de protección contra los ataques de fuerza bruta al iniciar sesión y contra la actividad inusual de inicio de sesión.

GoTo no almacena las contraseñas de las cuentas en texto plano. En su lugar, las contraseñas se almacenan mediante una función hash criptográfica con sal diseñada para ser resistente a los ataques de diccionario y de fuerza bruta. Las contraseñas se transmiten a través de conexiones seguras (TLS).

### 4.4.2 Autenticación de los asistentes a las sesiones

Para habilitar las sesiones con asistencia restringida, cada sesión tiene un ID único y aleatorio. Los organizadores también pueden optar por exigir una contraseña a los participantes para unirse a una sesión.

Para unirse a una sesión, los asistentes deben proporcionar el ID único haciendo clic en una URL que contenga el ID o introduciendo manualmente el valor en un formulario presentado por el Servicio. Si utiliza la marcación telefónica para unirse a la reunión, el asistente debe introducir el ID con su teclado. Si el ID es válido, cada asistente recibe un token de rol que se presenta a los servidores de comunicación al unirse a la reunión.

### 4.4.3 Control de acceso basado en funciones

Se pueden asignar roles definidos por la aplicación a los usuarios del Servicio y ayudar a los Clientes a aplicar las políticas de acceso de la empresa relacionadas con el uso del Servicio y de las características. Los usuarios pueden acceder a los controles y privilegios en función de su rol asignado:

Los **organizadores** (o formadores en el caso de GoTo Training) están autorizados a programar reuniones, seminarios web o sesiones de formación. El organizador configura la sesión, invita a los asistentes, inicia y finaliza la sesión y designa al presentador.

Los **asistentes** son las personas invitadas a participar en las sesiones. Los asistentes pueden ver la pantalla compartida del presentador, chatear con otros asistentes y ver la lista de asistentes.

Los **presentadores** son asistentes que pueden compartir su pantalla con otros asistentes. Los presentadores también pueden permitir que otros asistentes tengan el control compartido del teclado y del mouse.

Los **administradores** son personas autorizadas a gestionar una cuenta multiusuario. Los administradores externos pueden configurar características de las cuentas, autorizar organizadores y acceder a distintas herramientas para generar informes.

Los **administradores internos de GoTo** son miembros del personal de GoTo autorizados a gestionar los servicios y cuentas de GoTo Meeting, GoTo Webinar y GoTo Training en nombre de nuestros Clientes.

## 4.5 Control de acceso a grabaciones

Después de una sesión, los organizadores pueden compartir fácilmente las grabaciones a través de enlaces únicos y directos, y los asistentes pueden reproducir la grabación desde su navegador web.

En el caso de GoTo Webinar, las URL para compartir no caducan mientras la grabación esté disponible. Para deshabilitar el acceso a una grabación, los organizadores pueden borrarla en cualquier momento.

En el caso de GoTo Meeting, las grabaciones pueden compartirse a través de URL que utilizan un token aleatorio con validez limitada. El uso compartido puede restringirse a partes definidas del contenido, y estar disponible para todos los que tengan la URL o solo para usuarios con direcciones de correo electrónico configurables. Estas restricciones pueden ajustarse incluso después de compartir la URL.

# 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.

# 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 los centros de datos de los proveedores de alojamiento en la nube.

Para conocer los detalles del proveedor del centro de datos y su ubicación, consulte el documento Sub-Processor Disclosure (Declaración de subencargados del tratamiento) del Servicio en el Trust & Privacy Center de GoTo.

Todos ellos incluyen la supervisión de las condiciones ambientales y ofrecen medidas de seguridad física 24 horas.

## 7.1 Seguridad física del centro de datos

Los proveedores de alojamiento en la nube proporcionan 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

Los proveedores de alojamiento en la nube limitan el acceso físico a los centros de datos de producción únicamente a las personas autorizadas. El acceso a las salas de servidores requiere la presentación de una solicitud a través del sistema de tickets pertinente y la aprobación del responsable correspondiente, así como su revisión y aprobación. Los

proveedores minimizan, registran y revisan al menos trimestralmente todos los accesos físicos a los centros de datos y salas de servidores. 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, 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.
- **Certificaciones CBPR y PRP de TRUSTe y APEC** para la transferencia del Contenido del cliente 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 las certificaciones APEC, haga clic aquí.
- Informe de atestación del Instituto Americano de Contables Públicos Certificados (AICPA) de **Control de Organizaciones de Servicios (SOC) 2 Tipo** II, incluido el **Catálogo de computación en la nube (C5) de BSI**.
- 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 tiempo. GoTo recopila el tráfico anómalo o sospechoso identificado en los registros de seguridad pertinentes de los sistemas de producción aplicables.

# 11 Detección y respuesta a terminales

El software de detección y respuesta de terminales (EDR) 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 y sistemas operativos pertinentes que procesan el Contenido del cliente. GoTo evalúa y escanea las vulnerabilidades de host/red (“Sistemas”) a nivel de sistema, 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

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 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 vean los datos de otros usuarios.

# 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;
- cortafuegos de la red en la nube que filtran las conexiones de entrada y salida, incluidas las conexiones internas entre sistemas GoTo; y
- segmentación de la red interna.

# 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, incluidos Central y Pro. 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 revolución:** los clientes pueden solicitar la devolución o eliminación de su Contenido del cliente al enviar una solicitud a través del Portal de gestión de derechos individuales ("IRM") de GoTo, a través de support.goto.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 etiquetará automáticamente para su eliminación en un plazo de 90 días y se eliminará correctamente en un plazo de 100 días a partir de la rescisión, cancelación o caducidad y, en cada caso, del desaprovisionamiento 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.

Los plazos anteriores son aplicables a todos los Servicios, y a continuación se establecen plazos adicionales de eliminación específicos de cada Servicio:

**GoTo Meeting**

Durante el periodo de suscripción: el historial de sesiones de GoTo Meeting y las grabaciones en la nube se eliminarán automáticamente de forma continua en un año

durante el plazo de suscripción activo del Cliente, en el caso tanto de las cuentas de pago como de las gratuitas.

Tras la finalización de la suscripción: tras la finalización de una suscripción de pago a GoTo Meeting, las cuentas del Cliente que contengan una licencia gratuita volverán a ser cuentas gratuitas y se conservará el Contenido. En el caso de las cuentas que no contengan una licencia gratuita o que se cancelen o rescindan explícitamente, el Contenido se etiquetará automáticamente para su eliminación en un plazo de 90 días y se eliminará correctamente en un plazo de 100 días a partir de la rescisión, cancelación o caducidad y, en cada caso, del desaprovisionamiento de la suscripción del Cliente vigente en ese momento. Además, las cuentas gratuitas de GoTo Meeting se eliminarán automáticamente tras dos (2) años de inactividad del usuario (por ejemplo, sin inicios de sesión).

Eliminación de un usuario de una cuenta de pago: si un usuario se elimina o quita de otro modo de una cuenta de pago activa, las sesiones programadas se etiquetan automáticamente para su eliminación transcurridos 90 días y se eliminan correctamente transcurridos 100 días desde la eliminación del usuario.

GoTo Stage: los usuarios de GoTo Stage con una suscripción activa a GoTo Webinar pueden anular la publicación de cualquier seminario web publicado o eliminarlo en cualquier momento, ya sea por su cuenta desde el entorno de servicios de GoTo Webinar o enviando una solicitud de soporte a GoTo.

# 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 otras personas que usan los servicios de GoTo ("Usuarios"), 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. Para obtener 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, la CCPA 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), 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 Marco de privacidad de datos

Los marcos de privacidad de datos (DPF) y la extensión del Reino Unido a la UE-EE. UU. DPF son marcos voluntarios que, respectivamente, proporcionan mecanismos para que las empresas transfieran datos personales de la UE, Suiza y el Reino Unido a EE. UU. de conformidad con la normativa de protección de datos de estas jurisdicciones. GoTo cumple con todos estos marcos en lo que respecta a la recopilación, uso y retención de datos personales de la UE, Suiza y el Reino Unido, respectivamente. Para obtener más información sobre los DPF y ver la certificación de GoTo, visite el sitio web de DPF.

### 20.4.3 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.

### 20.4.4 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.

## 20.5 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.

## 20.6 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 especifican los nombres, las ubicaciones y los 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.

## 20.7 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 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.

## 20.8 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 GoTo Resolve 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. Por ejemplo, el ATD de proveedores de GoTo tiene restricciones en torno a la “venta” de datos según la definición de la CCPA. Del mismo modo, se establecen anexos de seguridad con controles y requisitos de sistemas adecuados con los proveedores pertinentes.

# 22 Contactar con GoTo

Los clientes pueden ponerse en contacto con GoTo en support.goto.com para consultas generales. Para enviar preguntas o solicitudes relacionadas con la protección de datos o la seguridad, visite nuestro portal IRM o envíe un correo electrónico a privacy@goto.com.