# Medidas Técnicas e Organizacionais
## GoTo Meeting, GoTo Webinar, GoTo Training e GoTo Stage

## Resumo Executivo

Este documento denominado Medidas Técnicas e Organizacionais ("TOMs") define os compromissos de privacidade, segurança e responsabilidade da GoTo em relação ao GoTo Meeting, GoTo Webinar, GoTo Training e GoTo Stage. A GoTo mantém programas globais robustos de privacidade e segurança e proteções organizacionais, administrativas e técnicas projetadas para: (i) garantir a confidencialidade, a integridade e a disponibilidade do Conteúdo do Cliente; (ii) proteger contra ameaças e riscos à segurança do Conteúdo do Cliente; (iii) proteger contra qualquer perda, uso indevido, acesso não autorizado, divulgação, alteração e destruição do Conteúdo do Cliente; e (iv) manter a conformidade com as leis e regulamentos aplicáveis, incluindo leis de proteção de dados e privacidade. Essas medidas incluem:

- **Criptografia:**
  - Transport Layer Security (TLS) ou Datagram Transport Layer Security (DTLS) *em trânsito*
  - Transparent Data Encryption (TDE) e Advanced Encryption Standard (AES) de 256 bits para o Conteúdo do Cliente *em repouso*.
- **Data centers:** a GoTo utiliza provedores de hospedagem em nuvem que empregam medidas para fornecer alta segurança lógica e física, disponibilidade e escalabilidade.
- **Auditorias de conformidade:** GoTo Meeting, GoTo Webinar e GoTo Training possuem as certificações SOC 2 Tipo II, C5, PCI DSS, PCAOB, TRUSTe Enterprise Privacy e APEC CBPR e PRP.
- **Conformidade legal/regulatória:** a GoTo mantém um programa abrangente de proteção de dados com processos e políticas projetados para garantir que o Conteúdo do Cliente seja tratado de acordo com as leis de privacidade aplicáveis, incluindo RGPD, CCPA/CPRA e LGPD.
- **Avaliações de segurança**: além dos testes internos, a GoTo contrata empresas externas para realizar avaliações regulares de segurança e/ou testes de penetração.
- **Controles de acesso lógico:** os controles de acesso lógico são implementados e projetados para evitar ou atenuar a ameaça de acesso não autorizado a aplicativos e a perda de dados em ambientes corporativos e de produção.
- **Segregação de Dados**: a GoTo emprega uma arquitetura multilocatário e separa logicamente as contas dos clientes na camada de armazenamento.
- **Defesa de perímetro e detecção de intrusão**: as ferramentas, as técnicas e os serviços de proteção de perímetro são projetados para impedir que o tráfego de rede não autorizado entre na infraestrutura dos produtos. A rede da GoTo tem firewalls externos e segmentação de rede interna.
- **Retenção de dados:**
  - Os Clientes do GoTo Meeting, GoTo Webinar, GoTo Training e GoTo Stage podem solicitar a devolução ou a exclusão do Conteúdo do Cliente a qualquer momento, o que será atendido em até 30 (trinta) dias após a solicitação do Cliente.
  - No caso do GoTo Meeting, GoTo Webinar e GoTo Training, o Conteúdo do Cliente será automaticamente excluído entre noventa e cem (90 e 100) dias após a expiração do período de assinatura final do Cliente.

# Índice

Clique nos números das páginas abaixo para acessar a seção relevante das TOMs.


*Resumo Executivo* ..... 1

*Índice* ..... 2

1 *Introdução ao produto* ..... 3

2 *Medidas técnicas* ..... 5

3 *Arquitetura do produto* ..... 5

4 *Controles técnicos de segurança* ..... 7

5 *Atualizações do programa de segurança* ..... 11

6 *Backup de dados, recuperação de desastres e disponibilidade* ..... 11

7 *Data centers* ..... 11

8 *Conformidade com os padrões* ..... 12

9 *Segurança do aplicativo* ..... 13

10 *Registro em log, monitoramento e alertas* ..... 13

11 *Detecção e resposta de endpoints* ..... 13

12 *Gerenciamento de ameaças* ..... 13

13 *Varredura de segurança e vulnerabilidade e gerenciamento de patches* ..... 13

14 *Controle de acesso lógico* ..... 14

15 *Segregação de dados* ..... 14

16 *Defesa de perímetro e detecção de intrusão* ..... 14

17 *Operações de segurança e gerenciamento de incidentes* ..... 14

18 *Exclusão e devolução de conteúdo* ..... 15

19 *Controles organizacionais* ..... 15

20 *Práticas de privacidade* ..... 16

21 *Controles de segurança e privacidade de terceiros* ..... 19

22 *Como entrar em contato com a GoTo* ..... 20

# 1 Introdução ao produto

O GoTo Meeting, o GoTo Webinar, o GoTo Training e o GoTo Stage (juntos, o "Serviço") são soluções de comunicação online que permitem que indivíduos e organizações interajam usando vários recursos, dependendo da oferta de serviço, incluindo compartilhamento de tela de desktop, videoconferência, bate-papo e áudio integrado. O GoTo Meeting, o GoTo Webinar, o GoTo Training e o GoTo Stage têm infraestrutura compartilhada e são fornecidos por meio de uma CDN para navegadores da Web ou aplicativos instaláveis.

- O GoTo Meeting, o GoTo Webinar e o GoTo Training permitem que os organizadores agendem, reúnam e moderem sessões online, incluindo áudio, webcam, compartilhamento de tela e muito mais, usando os aplicativos GoTo para Web, desktop e dispositivos móveis.
- O GoTo Training oferece recursos específicos aplicáveis ao treinamento baseado na Web, como acesso online a testes e materiais e um catálogo de cursos hospedado.
- O GoTo Webinar oferece suporte especial para a realização de eventos de apresentação de informações de um para muitos, alcançando participantes locais e globais pela Internet.
- O GoTo Stage é uma extensão do GoTo Webinar em que os organizadores do GoTo Webinar podem criar canais personalizáveis e publicar as gravações de seus webinars. As gravações publicadas são exibidas na página inicial do GoTo Stage, organizadas por categorias de negócios. A qualquer momento, os organizadores podem cancelar a publicação da gravação pelo GoTo Webinar, o que remove o vídeo da página do canal e do ecossistema do GoTo Stage.

## 1.1 Gerenciamento e registro de conferências

Os organizadores podem agendar sessões diretamente no Serviço. Eles podem ajustar várias configurações das próximas sessões e preparar o conteúdo e os participantes.

## 1.2 Áudio

A audioconferência integrada para sessões do GoTo Meeting, GoTo Webinar e GoTo Training está disponível por meio de VoIP (Voice over Internet Protocol) e da rede telefônica pública comutada (PSTN).

## 1.3 Vídeo

Todos os produtos oferecem vídeo de webcam de alta qualidade que se ajusta à largura de banda e à latência do usuário.

## 1.4 Upload de conteúdo (somente para Webinar e Training)

Os organizadores podem fazer upload de arquivos e mídia para uso durante as sessões, tanto antes quanto depois do início da sessão.

## 1.5 Relatórios das sessões

Os organizadores podem ver as estatísticas de participação e outros dados da sessão no histórico dela.

## 1.6 Gravação e transcrições

As sessões podem ser gravadas localmente e na nuvem. Os administradores da conta e os organizadores de sessões podem optar por ativar as gravações na nuvem, além das gravações locais ou em vez delas. As gravações locais são armazenadas no sistema do organizador e não estão sujeitas aos limites de retenção da GoTo, definidos na Seção 18 ("Exclusão e devolução de conteúdo") deste documento.

As gravações na nuvem ficam automaticamente disponíveis diretamente no histórico de sessões do organizador, e as transcrições são criadas automaticamente quando esse recurso é ativado pelo administrador. As transcrições das gravações das sessões são criadas usando a tecnologia GoTo Voice AI ou Google Cloud Speech-to-Text.

No **GoTo Meeting**, um administrador de conta pode optar por ativar as gravações e decidir se elas serão armazenadas localmente ou na nuvem. Se as gravações na nuvem estiverem ativadas, o organizador da reunião poderá optar por gravar uma determinada reunião e armazená-la na nuvem. As transcrições são criadas automaticamente para as gravações na nuvem.

No **GoTo Webinar**, os organizadores podem optar por transcrever automaticamente todas as gravações na nuvem. Somente um organizador pode iniciar uma gravação. Se a configuração de transcrição automática estiver ativada, será criada uma transcrição.

No **GoTo Training**, os administradores da conta podem controlar se os organizadores podem salvar as gravações na nuvem. Os administradores da conta não podem impedir que os organizadores gravem sessões localmente. Os treinamentos não podem ser transcritos.

## 1.7 Business Messaging (somente para Meeting)

Business Messaging é uma extensão do GoTo Meeting e permite que os usuários do GoTo Meeting vejam o status de presença de outros usuários da conta, troquem mensagens instantâneas e compartilhem arquivos. O administrador da conta define o escopo da visibilidade e da capacidade de descoberta de vários usuários.

Os usuários do Business Messaging podem ver o status de presença de qualquer outro usuário da conta, desde que ele faça parte da sua lista de contatos. As mensagens podem ser trocadas com todos os membros de uma equipe e com usuários externos caso eles tenham sido explicitamente incluídos por meio de um convite por e-mail. Os usuários externos são usuários do Business Messaging que não são membros da equipe interna de um Cliente (por exemplo, cliente, cliente potencial ou parceiro). As mensagens podem enviadas diretamente (entre dois participantes), em um grupo privado ou em um grupo público.

Os usuários também podem compartilhar outros conteúdos no Business Messaging ao fazer upload e download de arquivos. Os arquivos compartilhados estão disponíveis para download por todos os usuários com acesso às mensagens em uma determinada conversa ou grupo.

## 1.8 Webcast (somente Webinar)

Os webcasts do GoTo Webinar usam gateways de transmissão, mecanismos de streaming de terceiros e redes de fornecimento de conteúdo projetadas para fornecer, de forma confiável, compartilhamento de tela, áudio e mídia de vídeo aos participantes que se conectam a partir de um navegador da Web. Os gateways recebem dados de mídia dos servidores de mídia e os transcodificam em codecs padrão. O mecanismo de streaming produz HTTP Live Streaming (HLS) em várias taxas de bits para permitir o fornecimento adaptável para usuários com conexões de rede abaixo do ideal.

## 1.9 GoTo Stage (somente Webinar)

Os vídeos publicados no GoTo Stage ficam disponíveis para descoberta na página inicial do GoTo Stage e nos resultados dos mecanismos de pesquisa, a menos que o organizador restrinja a capacidade de descoberta usando as configurações administrativas na página do canal. As gravações não detectáveis podem ser acessadas por qualquer pessoa registrada no GoTo Stage usando um URL direto para o canal ou para a página exclusiva "Assista agora" do vídeo. Os visitantes se registram no GoTo Stage usando seu nome e endereço de e-mail ou podem se conectar por meio de contas de algumas redes sociais, como LinkedIn, Facebook e Gmail. Os URLs para os visitantes acessarem os vídeos ficam ativos por período limitado para minimizar o compartilhamento indesejado.

# 2 Medidas técnicas

Os produtos da GoTo são projetados para fornecer soluções seguras, confiáveis e privadas. As medidas técnicas definidas abaixo descrevem como o GoTo implementa esse design e o aplica na prática para ao GoTo Meeting, ao GoTo Webinar e ao GoTo Training.

A implementação de salvaguardas, recursos e práticas da GoTo envolve:

I. Criar produtos que levem em conta a segurança e a privacidade por design e padrão, e incluir camadas adicionais de segurança para proteger o Conteúdo do Cliente;

II. Manutenção de controles organizacionais que operacionalizam políticas e procedimentos internos relacionados à conformidade com padrões, gerenciamento de incidentes, segurança de aplicativos, segurança de pessoal e programas de treinamento regulares; e

III. Garantir que as práticas de privacidade estejam em vigor para reger o manuseio e o gerenciamento de dados conforme o RGPD, CCPA/CPRA e LGPD, bem como com nosso próprio Adendo de Processamento de Dados (DPA) e políticas e divulgações públicas aplicáveis da GoTo.

Ao incorporar salvaguardas de segurança ao produto, nós nos esforçamos para proteger o Conteúdo do Cliente da GoTo contra ameaças e garantir que os controles de segurança sejam adequados à natureza e ao escopo dos Serviços. Os recursos de segurança que podem ser configurados no serviço ajudam os administradores a minimizar as ameaças e os riscos ao Conteúdo do Cliente.

# 3 Arquitetura do produto

O GoTo Meeting, o GoTo Webinar, o GoTo Training e o GoTo Stage são soluções de software como serviço (SaaS) projetadas para oferecer alto desempenho, confiabilidade, escalabilidade e segurança. Esses Serviços são viabilizados por servidores de alta capacidade e equipamentos de rede com controles de segurança adequados e infraestrutura redundante projetada para evitar pontos únicos de falha. Servidores em cluster e sistemas de backup foram implementados para dar suporte ao funcionamento dos processos de aplicativos em caso de carga pesada ou falha do sistema.

As sessões de aplicativos/servidores são balanceadas em clusters geograficamente distribuídos, projetados para garantir o desempenho e a latência adequada.

A infraestrutura e os dados do Serviço são hospedados por provedores de hospedagem em nuvem.

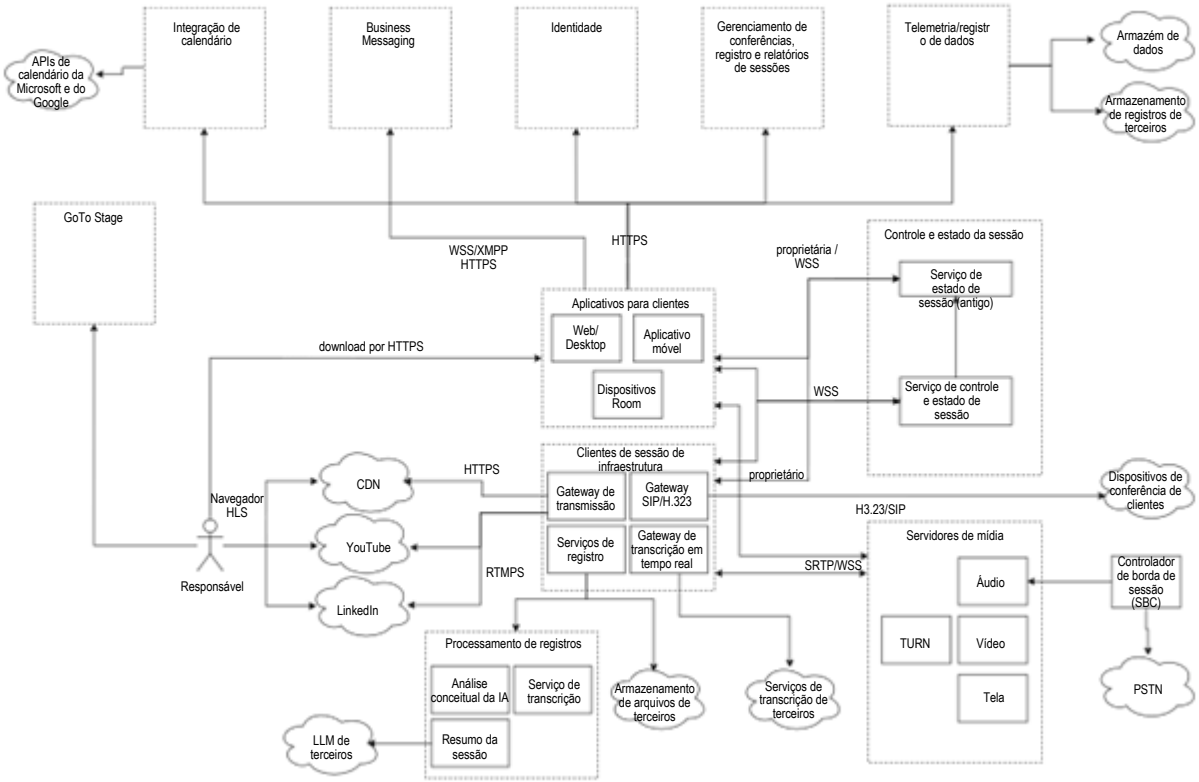


*Figura 1: arquitetura do Central*

*Aplicativos clientes (aplicativos GoTo para Web, desktop e dispositivos móveis ou "clientes"; um dispositivo chamado GoTo Room [somente para Meeting])*: fornecem a funcionalidade do Serviço conforme descrito acima na Seção 1 ("Introdução ao produto").

*Serviços de identidade*: gerenciam contas de usuários e permitem a autorização e o login seguros e padronizados de contas.

*Serviços de gerenciamento de conferências, registro e relatórios de sessões:* o gerenciamento de conferências fornece informações sobre as sessões agendadas e permite o agendamento de novas sessões e o ajuste das sessões existentes. Os serviços de registro permitem o registro para sessões em que isso é necessário. Os relatórios de sessões fornecem informações sobre sessões anteriores, incluindo gravações, transcrições, presença e mais.

*Business Messaging*: gerenciamento de canais, bem como envio, recebimento e armazenamento de mensagens e anexos; usado apenas para mensagens fora da sessão.

*Integração com calendário*: permite que os usuários sincronizem seus calendários do Microsoft Outlook ou do Google para receber notificações sobre as sessões da GoTo.

*Telemetria/log*: envio de sondas de telemetria ou declarações de log para ajudar a reunir estatísticas de uso e diagnosticar problemas.

*Serviços de controle e estado da sessão*: fornecem funcionalidade usada pelos aplicativos clientes para iniciar e receber alterações não relacionadas à mídia no estado da sessão.

*Servidores de mídia*: responsáveis por receber, modificar e distribuir conteúdo de áudio, vídeo e compartilhamento de tela.

*PSTN*: a rede telefônica pública comutada permite que os usuários disquem para sessões por meio de telefones físicos ou IP.

*Controlador de borda de sessão*: conecta o VoIP (Voice over Internet Protocol) da GoTo a provedores de telefonia comerciais.

*Serviços de gravação*: permite a gravação de sessões de áudio, vídeo, compartilhamento de tela e conteúdo do Business Messaging.

*Gateway de transmissão*: usado para webcasts do GoTo Webinar e suporta layout, transcodificação e empacotamento dos fluxos de mídia em fluxos HLS, que são distribuídos via CDN para clientes baseados em navegador ou enviados para plataformas de streaming compatíveis com RTMP, como YouTube ou LinkedIn.

*Gateway H.323/SIP*: permite a conexão com o áudio da sessão por meio de dispositivos de conferência SIP ou H.323.

*Gateway de transcrição em tempo real (RTT)*: fornece transcrição em tempo real das falas dos participantes da sessão.

*Serviços do GoTo Stage*: permitem o gerenciamento do conteúdo de vídeo do GoTo Webinar pelos organizadores; oferecem experiência de visualização aos visitantes.

# 4 Controles técnicos de segurança

A GoTo emprega controles técnicos de segurança desenvolvidos para proteger a infraestrutura do Serviço e os dados que residem nela.

## 4.1 Criptografia

A GoTo revisa regularmente seus padrões de criptografia e pode atualizar as cifras e/ou tecnologias usadas de acordo com o risco avaliado e a aceitação de novos padrões pelo mercado.

### 4.1.1 Criptografia em trânsito

A GoTo implementa medidas de segurança para dados em trânsito que são projetadas para oferecer proteção contra ataques passivos e ativos à confidencialidade, integridade e disponibilidade. Os controles de segurança de comunicações são implementados para compartilhamento de tela e vídeo, VoIP, vídeo de webcam, controle de teclado e mouse, informações de bate-papo baseadas em texto e outros dados de sessão.

A GoTo usa os protocolos TLS padrão da Internet Engineering Task Force (IETF) para proteger a comunicação TCP entre os endpoints.

O HTTPS e o WSS são usados para proteger dados que não sejam de mídia, enquanto os dados de mídia na sessão são protegidos por SRTP, WSS ou DTLS.

Internamente, a GoTo também usa autenticação baseada em certificado mútuo (mTLS) em servidores que lidam com dados de mídia.

#### 4.1.1.1 Segurança de áudio e vídeo

Um protocolo baseado em SRTP usando mecanismos de criptografia padrão compatíveis no mínimo com AES128 é adotado para proteger a confidencialidade e a integridade das conexões VoIP entre os endpoints e os servidores.

#### 4.1.1.2 Segurança de sites, APIs e serviços internos da Web

Todas as conexões com os sites, APIs e serviços internos da Web do Serviço são protegidas por TLS. Isso inclui upload de conteúdo, relatórios de sessões, gravações e transcrições, entre outros.

#### 4.1.1.3 Business Messaging

Atualizações de presença, mensagens e arquivos são transferidos por um canal protegido por TLS para os serviços de bate-papo e para os usuários. O conteúdo é disponibilizado por URLs com assinatura criptografada que os ligam ao conteúdo.

#### 4.1.1.4 Segurança do webcast (somente Webinar)

Os gateways de streaming do webcast encaminham o tráfego para o mecanismo de streaming por SRTP, tudo dentro da rede interna segura da GoTo. As CDNs extraem dados do mecanismo de streaming de forma segura por HTTPS. Os clientes também extraem dados de forma segura das CDNs por HTTPS.

### 4.1.2 Criptografia em repouso

#### 4.1.2.1 Dados do perfil

O conteúdo é armazenado em um banco de dados relacional com criptografia AES de 256 bits.

#### 4.1.2.2 Gerenciamento de conferências, registro e relatórios de sessões

O conteúdo é armazenado em um banco de dados relacional com criptografia AES de 256 bits.

#### 4.1.2.3 Upload de conteúdos

O conteúdo carregado e os metadados relacionados são armazenados no AWS S3, no Amazon Aurora e no Amazon Dynamo DB, todos com criptografia AES de 256 bits. Além disso, os metadados são armazenados no Apache Cassandra sem criptografia em repouso.

#### 4.1.2.4 Gravações e transcrições

As gravações na nuvem são armazenadas no AWS S3. Os arquivos são criptografados em repouso usando criptografia no lado do servidor com AES256.

Os arquivos de áudio para transcrição são criptografados usando AES256 e excluídos imediatamente após a conclusão do processamento de fala para texto.

#### 4.1.2.5 Segurança do Business Messaging

As mensagens são armazenadas em um banco de dados do AWS Aurora, e os arquivos compartilhados são armazenados no AWS S3, ambos com criptografia AES de 256 bits em repouso.

#### 4.1.2.6 GoTo Stage

O conteúdo carregado e os metadados relacionados são armazenados no AWS S3 com criptografia AES de 256 bits. Os metadados são armazenados no Apache Cassandra, e o índice de pesquisa, no Elasticsearch; ambos não criptografados em repouso.

## 4.2 Compatibilidade com firewall e proxy

O Serviço inclui recursos incorporados de lógica de detecção de proxy e de gerenciamento de conexão para ajudar a automatizar a instalação do software, evitar a necessidade de (re)configuração complexa da rede e maximizar a produtividade do usuário. Os firewalls e proxies já presentes na rede de um usuário geralmente não precisam de configuração especial para permitir o uso do Serviço.

Para obter mais detalhes e os domínios, IPs e portas exatos usados, visite as respectivas páginas de suporte do Meeting, do Webinar e do Training.

## 4.3 Recursos de segurança do cliente instalável

Os clientes instaláveis são projetados com recursos de segurança apropriados e empregam medidas criptográficas robustas, incluindo software de endpoint assinado e conexões "somente de cliente".

### 4.3.1 Software de endpoint assinado

Os executáveis do Serviço são assinados digitalmente para proteção da integridade e da autenticidade. O software de aplicativo cliente da GoTo segue procedimentos adequados de controle de qualidade, procedimentos de gerenciamento de configuração e um modelo de ciclo de vida de desenvolvimento de segurança (SDL) durante o desenvolvimento e a implantação.

### 4.3.2 Conexões "somente de cliente"

Para reduzir o risco de que os sistemas remotos possam atacá-los com malware e vírus, os clientes instaláveis não são configurados para receber conexões de entrada. Isso ajuda a proteger os usuários que participam de uma sessão de serem infectados por um host comprometido usado por outro participante.

### 4.3.3 Implementação do subsistema criptográfico

As funções criptográficas e os protocolos de segurança implementados nos clientes instaláveis usam as bibliotecas criptográficas de código aberto BoringSSL ou OpenSSL. Não há APIs externas expostas que permitam que outros softwares acessem as bibliotecas criptográficas incluídas no cliente.

O aplicativo da Web usa as bibliotecas criptográficas do navegador. Não há configurações criptográficas configuráveis pelo usuário final que permitam uma configuração incorreta acidental ou intencional.

## 4.4 Autenticação do Usuário

A autorização baseada em funções e os controles de acesso adequados dependem da capacidade de identificar e autenticar usuários. Para garantir que os organizadores e participantes tenham os privilégios corretos, os recursos de autenticação de conta e sessão são incorporados ao Serviço.

### 4.4.1 Login de conta

Os sites do Serviço oferecem os seguintes métodos de login:

- Login direto com nome de usuário e senha;

- Login por meio de um provedor de conta social ou outro provedor de conta usando LastPass, Google, Facebook, LinkedIn, Microsoft ou Apple (https://support.goto.com/meeting/help/connect-your-social-or-other-account-for-sign-in); e
- Login único baseado em SAML.

Para o login direto, todas as senhas têm requisitos mínimos de caracteres e complexidade. Existem mecanismos para proteger contra ataques de login de força bruta e atividades de login incomuns.

A GoTo não armazena senhas de contas como texto não criptografado. As senhas são armazenadas usando uma função de hash criptográfica salgada projetada para ser resistente a ataques de dicionário e de força bruta. As senhas são transmitidas por conexões seguras (TLS).

### 4.4.2 Autenticação dos participantes nas sessões

Para permitir sessões com participação restrita, cada sessão tem um ID exclusivo e aleatório. Os organizadores também podem optar por exigir uma senha para que os participantes entrem em uma sessão.

Para participar de uma sessão, os participantes devem fornecer o ID exclusivo clicando em um URL que contenha o ID ou inserindo manualmente o valor em um formulário apresentado pelo Serviço. Quando a participação for pelo telefone, os participantes precisam discar o ID. Se o ID for válido, é atribuído a cada participante um token de função, que é informado aos nossos servidores de comunicação durante o processo de entrada na sessão.

### 4.4.3 Controle de acesso baseado em função

As funções definidas pelo aplicativo podem ser atribuídas aos usuários do Serviço e ajudar os clientes na exigência das políticas de acesso da empresa relacionadas ao Serviço e ao uso de recursos. Os usuários podem acessar controles e privilégios com base na função atribuída:

Os **organizadores** (ou instrutores do GoTo Training) têm autorização para agendar reuniões, webinars e/ou sessões de treinamento. Eles podem criar sessões, convidar participantes, iniciar e encerrar sessões e definir quem é o apresentador atual.

Os **participantes** são as pessoas convidadas para estar nas sessões. Eles podem visualizar a tela compartilhada do apresentador, conversar com outros participantes e ver quem está presente.

Os **apresentadores** são participantes que podem compartilhar a tela com quem estiver presente na sessão. Eles também podem conceder a outros participantes o controle compartilhado do seu teclado e mouse.

Os **administradores** têm autorização para gerenciar uma conta multiusuário. Eles podem configurar os recursos da conta, autorizar organizadores e acessar diversas ferramentas de relatórios.

Os **administradores internos da GoTo** são membros da equipe da GoTo autorizados a gerenciar os serviços e as contas do GoTo Meeting, do GoTo Webinar e do GoTo Training em nome de nossos Clientes.

## 4.5 Controle de acesso a gravações

É fácil para os organizadores compartilhar gravações com os participantes após uma sessão por meio de links únicos e diretos, pelos quais os participantes podem visualizar a gravação no navegador.

No caso do GoTo Webinar, os URLs de compartilhamento não expiram enquanto a gravação está disponível. Para desativar o acesso a uma gravação, os organizadores podem excluí-la a qualquer momento.

No GoTo Meeting, as gravações podem ser compartilhadas por meio de URLs que usam um token aleatório com validade limitada. O compartilhamento pode ser restrito a partes definidas do conteúdo e ficar disponível para todos com o URL ou somente para usuários com endereços de e-mail configuráveis. Essas restrições podem ser ajustadas mesmo após o compartilhamento do URL.

# 5 Atualizações do programa de segurança

A GoTo revisa e atualiza seu programa de segurança e contrata terceiros independentes para avaliar seus controles de segurança relevantes pelo menos uma vez por ano. Isso é feito para garantir que ela está se desenvolvendo em relação ao cenário atual de ameaças, bem como para assegurar a conformidade com estruturas relevantes, padrões do setor, comprometimentos com o Cliente e, conforme aplicável, alterações nas leis e nos regulamentos relativos à segurança dos dados da GoTo.

# 6 Backup de dados, recuperação de desastres e disponibilidade

A arquitetura da GoTo foi projetada para realizar a replicação quase em tempo real em locais geograficamente diferentes. O backup dos bancos de dados é feito usando uma estratégia de backup incremental contínuo. No caso de um desastre ou falha total da instalação de qualquer um dos vários locais ativos, os locais restantes são projetados para equilibrar a carga do aplicativo. A recuperação de desastres relacionada a esses sistemas é testada periodicamente.

# 7 Data centers

A infraestrutura da GoTo foi projetada para aumentar a confiabilidade do serviço e reduzir o risco de tempo de inatividade provocado por um único ponto de falha usando data centers de provedores de hospedagem em nuvem.

Para obter detalhes sobre o fornecedor e a localização dos data centers, consulte o documento de divulgação de subprocessadores do Serviço (Sub-Processor Disclosure) no Trust & Privacy Center da GoTo.

Todos os data centers incluem o monitoramento das condições ambientais e adotam medidas de segurança física ininterruptas.

## 7.1 Segurança física do data center

Os provedores de hospedagem em nuvem fornecem segurança física e controles ambientais para sistemas e servidores que contêm o Conteúdo do Cliente. Esses controles incluem:

- Vigilância e gravação de vídeo

- Controle de temperatura por aquecimento, ventilação e ar-condicionado
- Supressão de incêndio e detectores de fumaça
- Fonte de alimentação ininterrupta
- Pisos elevados ou gerenciamento abrangente de cabos
- Monitoramento e alertas contínuos
- Proteções contra desastres naturais e causados pelo homem, conforme exigido pela geografia e localização do data center relevante
- Manutenção programada e validação de todos os controles críticos de segurança e ambientais

Os provedores de hospedagem em nuvem limitam o acesso físico aos data centers de produção somente a pessoas autorizadas. O acesso às salas de servidores requer o envio de uma solicitação por meio do sistema de emissão de tíquetes relevante e a aprovação do gerente apropriado, além de revisão e aprovação. Todos os acessos físicos aos data centers e salas de servidores são minimizados, registrados e revisados pelos provedores pelo menos trimestralmente. Além disso, a autorização de acesso físico ao data center é removida imediatamente após a mudança de função (quando esse acesso não é mais necessário) ou após o desligamento de qualquer pessoa previamente autorizada. O acesso com vários fatores (por exemplo, biometria, crachá e teclado) é necessário para áreas altamente sensíveis, que incluem data centers.

# 8 Conformidade com os padrões

A GoTo avalia regularmente sua conformidade com os requisitos legais, financeiros, de privacidade de dados e regulatórios aplicáveis. Os programas de privacidade e segurança da GoTo atendem a padrões rigorosos e reconhecidos internacionalmente, foram avaliados de acordo com padrões abrangentes de auditoria externa e obtiveram certificações importantes, incluindo:

- **Certificação de Privacidade Empresarial e Práticas de Governança de Dados da TRUSTe** para abordar a privacidade operacional e os controles de proteção de dados que estão alinhados com as principais leis de privacidade e estruturas de privacidade reconhecidas. Para saber mais, acesse nossa publicação no blog.
- **Certificações TRUSTe APEC CBPR e PRP** para a transferência do Conteúdo do Cliente entre países-membros da APEC, obtidas e validadas de forma independente pela TrustArc, uma líder terceirizada aprovada pela APEC em conformidade com a proteção de dados. Para saber mais sobre nossas certificações da APEC, clique aqui.
- Relatório de atestado do **Service Organization Control (SOC) 2 Tipo II do** American Institute of Certified Public Accountants (AICPA), incluindo o **BSI Cloud Computing Catalogue (C5)**.
- Conformidade com o **Payment Card Industry Data Security Standard (PCI DSS)** para os ambientes de comércio eletrônico e pagamento da GoTo.
- Avaliação dos controles internos, conforme exigido pela auditoria anual das demonstrações financeiras feitas pelo **Public Company Accounting Oversight Board (PCAOB)**.

# 9 Segurança do aplicativo

O programa de segurança de aplicativos da GoTo segue o Microsoft Security Development Lifecycle (SDL) para proteger o código do produto. O programa Microsoft SDL inclui revisões manuais de código, modelagem de ameaças, análise estática de código, análise dinâmica e fortalecimento do sistema. As equipes da GoTo também realizam periodicamente testes de vulnerabilidade de aplicativos dinâmicos e estáticos e atividades de teste de penetração para ambientes específicos.

# 10 Registro em log, monitoramento e alertas

A GoTo mantém políticas e procedimentos de registro em log, monitoramento e alerta, que definem os princípios e controles implementados para reforçar nossa capacidade de detectar atividades suspeitas e reagir em tempo hábil. A GoTo coleta o tráfego anômalo ou suspeito identificado nos registros de segurança relevantes nos sistemas de produção aplicáveis.

# 11 Detecção e resposta de endpoints

O software de detecção e resposta de endpoints (EDR) com registro em log de auditoria é implantado em todos os servidores da GoTo para minimizar a interrupção ou o impacto no desempenho do Serviço. As investigações de segurança serão iniciadas de acordo com nossos procedimentos de resposta a incidentes se for detectada atividade suspeita, conforme apropriado e necessário. Consulte a seção 17 para obter mais informações sobre o Centro de Operações de Segurança da GoTo e os procedimentos de resposta a incidentes.

# 12 Gerenciamento de ameaças

A Equipe de Resposta a Incidentes de Segurança Cibernética ("CSIRT") da GoTo é composta por várias equipes e é responsável pela proteção contra ameaças cibernéticas. Especificamente, a Equipe de Inteligência de Ameaças Cibernéticas da CSIRT coleta, examina e divulga informações relativas a ameaças atuais e emergentes. A GoTo se mantém atualizada com a inteligência e a mitigação de ameaças por meio da análise de fontes abertas e fechadas e da participação em grupos de compartilhamento e associações do setor (IT-ISAC, FIRST.org, etc.).

# 13 Varredura de segurança e vulnerabilidade e gerenciamento de patches

A GoTo mantém um programa formal de gerenciamento de patches e, pelo menos trimestralmente, realiza atividades de gerenciamento de patches em todos os sistemas, dispositivos, firmware e sistemas operacionais relevantes que processam o Conteúdo do Cliente. A GoTo avalia e examina as vulnerabilidades de host/rede em nível de sistema ("Sistemas"), no mínimo mensalmente, bem como após qualquer alteração material nesses Sistemas, e corrige as vulnerabilidades relevantes descobertas de acordo com políticas documentadas que priorizam a correção com base no risco.

# 14 Controle de acesso lógico

Os procedimentos de controle de acesso lógico estão em vigor para reduzir o risco de acesso não autorizado a aplicativos e de perda de dados em ambientes corporativos e de produção. Os funcionários recebem acesso a sistemas, aplicativos, redes e dispositivos da GoTo específicos com base no "princípio do menor privilégio". Os privilégios do Usuário são segregados com base na função funcional (controle de acesso baseado na função) e no ambiente, usando controles, processos e/ou procedimentos de segregação de funções.

# 15 Segregação de dados

A GoTo utiliza uma arquitetura multilocatário, logicamente separada no nível do banco de dados, com base na conta GoTo de um Usuário ou organização. As partes devem ser autenticadas para obter acesso a uma conta. A GoTo também implementou controles para impedir que os Usuários ou Usuários Finais vejam os dados de outros Usuários.

# 16 Defesa de perímetro e detecção de intrusão

A GoTo utiliza ferramentas, técnicas e serviços de proteção de perímetro para impedir que tráfego de rede não autorizado entre na infraestrutura de produtos da GoTo. Isso inclui, sem limitações:

- Sistemas de detecção de intrusão que monitoram sistemas, serviços, redes e aplicativos em busca de acesso não autorizado;
- Monitoramento crítico do sistema e dos arquivos de configuração;
- Firewalls da rede de nuvem que filtram conexões de entrada e saída, incluindo conexões internas entre sistemas GoTo; e
- Segmentação da rede interna.

# 17 Operações de segurança e gerenciamento de incidentes

O Centro de Operações de Segurança (SOC) da GoTo é responsável por detectar e responder a eventos de segurança. O SOC usa sensores de segurança e sistemas de análise para identificar possíveis problemas e desenvolveu procedimentos de resposta a incidentes, incluindo um Plano de Resposta a Incidentes documentado.

O Plano de Resposta a Incidentes da GoTo está alinhado com nossas medidas críticas de processos de comunicação, políticas e procedimentos operacionais padrão. Ele foi projetado para gerenciar, identificar e resolver eventos de segurança relevantes, suspeitos ou identificados, em seus sistemas e serviços, incluindo o Central e o Pro. O Plano de Resposta a Incidentes estabelece mecanismos para que os funcionários relatem suspeitas de eventos de segurança e rotas de encaminhamento a serem seguidas quando apropriado. Os eventos suspeitos são documentados e encaminhados conforme apropriado por tickets de eventos padronizados e são organizados conforme o nível de gravidade.

# 18 Exclusão e devolução de conteúdo

**Exclusão e/ou Devolução:** os Clientes podem solicitar a devolução e/ou exclusão de seu Conteúdo do Cliente ao enviar uma solicitação pelo Portal de Gerenciamento de Direitos Individuais ("IRM") da GoTo, pelo site support.goto.com ou pelo e-mail privacy@goto.com. As solicitações serão processadas no prazo de 30 (trinta) dias após o recebimento pela GoTo. No entanto, na eventualidade improvável de precisarmos de mais tempo, avisaremos o mais rápido possível sobre qualquer atraso previsto e informaremos o novo prazo de conclusão.

**Cronograma de Retenção de Conteúdo do Cliente:** a menos que exigido de outra forma pela legislação aplicável, o Conteúdo do Cliente deverá ser automaticamente marcado para exclusão dentro de 90 (noventa) dias e excluído com sucesso dentro de 100 (cem) dias após a rescisão, o cancelamento ou a expiração e, em cada caso, o desprovisionamento da assinatura final do Cliente. Mediante solicitação por escrito, a GoTo poderá fornecer confirmação/certificação por escrito da exclusão do Conteúdo.

Os prazos acima são aplicáveis a todos os Serviços, e os prazos adicionais de exclusão específicos de cada Serviço estão definidos abaixo:

**GoTo Meeting**

Durante o período de assinatura: o histórico de sessões do GoTo Meeting e as gravações na nuvem serão excluídos automaticamente em uma base contínua de um (1) ano durante o período de assinatura ativa do Cliente, tanto para contas pagas quanto para contas gratuitas.

Após a vigência da assinatura: após a conclusão de uma assinatura paga do GoTo Meeting, as contas do Cliente que contêm uma licença gratuita serão revertidas para uma conta gratuita, e o Conteúdo será mantido. Para contas que não contenham uma licença gratuita ou que sejam explicitamente canceladas ou rescindidas, o Conteúdo do Cliente deverá ser automaticamente marcado para exclusão dentro de 90 (noventa) dias e excluído com sucesso dentro de 100 (cem) dias após a rescisão, o cancelamento ou a expiração e, em cada caso, o desprovisionamento da assinatura final do Cliente. Além disso, as contas gratuitas do GoTo Meeting serão automaticamente excluídas após 2 (dois) anos de inatividade do usuário (por exemplo, sem logins).

Remoção de usuário de conta paga: se um usuário for excluído ou removido de uma conta paga ativa, as sessões agendadas serão automaticamente marcadas para exclusão após 90 (noventa) dias e excluídas dentro de 100 (cem) dias da remoção do usuário.

GoTo Stage: os usuários do GoTo Stage com uma assinatura ativa do GoTo Webinar podem remover qualquer webinar publicado a qualquer momento por meio de autoatendimento no ambiente de serviços do GoTo Webinar e/ou enviando uma solicitação de suporte à GoTo.

# 19 Controles organizacionais

## 19.1 Políticas e procedimentos de segurança

A GoTo mantém um conjunto abrangente de políticas e procedimentos de segurança que são periodicamente revisados e atualizados conforme necessário para apoiar os objetivos de segurança da GoTo, as mudanças na legislação aplicável, os padrões do setor e os esforços de conformidade.

## 19.2 Gerenciamento de mudanças

A GoTo mantém um processo adequado de gerenciamento de mudanças, e as mudanças nos sistemas da GoTo são avaliadas, testadas e aprovadas antes da implementação para reduzir o risco de interrupção dos serviços da GoTo.

## 19.3 Programas de conscientização e treinamento em segurança

O programa de conscientização sobre privacidade e segurança da GoTo envolve o treinamento de funcionários sobre a importância de manusear Dados Pessoais e informações confidenciais com ética, responsabilidade, conformidade com a lei aplicável e o devido cuidado. Os funcionários, prestadores de serviços e estagiários recém-contratados são informados sobre as políticas de segurança e o Código de Conduta e Ética Comercial da GoTo durante a integração. Os Funcionários da GoTo recebem treinamento em conscientização sobre privacidade e segurança pelo menos uma vez por ano. As atividades de conscientização ocorrem durante todo o ano e podem incluir campanhas para o Dia da Privacidade de Dados, Mês de Conscientização sobre Segurança Cibernética, webinars com o Chief Information Security Officer e um programa de campeões de segurança.

Quando apropriado, os funcionários também podem ser solicitados a realizar treinamentos específicos para suas funções. Além disso, todos os funcionários, contratantes e subsidiárias da GoTo devem analisar e aderir às políticas da GoTo relacionadas à segurança e à proteção de dados.

# 20 Práticas de privacidade

A GoTo leva muito a sério a privacidade de nossos Clientes, Usuários e outros indivíduos que utilizam os serviços da GoTo ("Usuários Finais") e tem o compromisso de divulgar práticas relevantes de manuseio e gerenciamento de dados de forma aberta e transparente.

## 20.1 Programa de privacidade

A GoTo mantém um programa de privacidade abrangente que envolve a coordenação de várias funções dentro da empresa, como Privacidade, Segurança, Governança, Risco e Conformidade (GRC), Jurídico, Produto, Engenharia e Marketing. Esse programa de privacidade está centrado nos esforços de conformidade e envolve a implementação e a manutenção de políticas internas e externas, padrões e adendos para reger as práticas da empresa.

## 20.2 Conformidade regulatória

### 20.2.1 RGPD

O Regulamento Geral de Proteção de Dados (RGPD) é uma lei da União Europeia (UE) referente à proteção de dados e à privacidade de indivíduos na UE. A GoTo mantém um programa abrangente de conformidade com o RGPD e, na medida em que a GoTo se envolver no processamento de Dados Pessoais sujeitos ao RGPD em nome do Cliente, nós o faremos de acordo com os requisitos aplicáveis do RGPD. Para mais informações, acesse https://www.goto.com/company/trust/privacy.

### 20.2.2 CCPA

A Lei de Privacidade do Consumidor da Califórnia, conforme alterada pela Lei de Direitos de Privacidade da Califórnia (coletivamente denominadas "CCPA"), concede aos californianos direitos e proteções adicionais em relação à forma como as empresas podem usar suas informações pessoais. A GoTo mantém um programa de conformidade abrangente e, na medida em que a GoTo se envolver no processamento de Dados Pessoais sujeitos à CCPA em nome do Cliente, nós o faremos de acordo com os requisitos aplicáveis da CCPA. Para obter mais informações sobre nossa conformidade com a CCPA, consulte a Política de Privacidade da GoTo e as Divulgações Suplementares da Lei de Privacidade do Consumidor da Califórnia.

### 20.2.3 LGPD

A Lei Geral de Proteção de Dados (LGPD) regulamenta o processamento de Dados Pessoais no Brasil e/ou de indivíduos localizados no Brasil no momento da coleta. A GoTo mantém um programa de conformidade abrangente e, na medida em que a GoTo se envolver no processamento de Dados Pessoais sujeitos à LGPD em nome do Cliente, nós o faremos de acordo com os requisitos aplicáveis da LGPD. Para mais informações, acesse https://www.goto.com/company/trust/privacy.

## 20.3 Adendo de Processamento de Dados

A GoTo oferece um Adendo de Processamento de Dados (DPA) global, disponível em inglês e alemão. Este DPA atende aos requisitos do RGPD, CCPA e outros regulamentos aplicáveis e rege o processamento do Conteúdo do Cliente pela GoTo.

Especificamente, nosso DPA incorpora várias proteções de privacidade de dados com foco no RGPD, incluindo:

(a) detalhes de processamento de dados e divulgações de subprocessadores, conforme exigido pelo Artigo 28;
(b) Cláusulas Contratuais Padrão revisadas (2021) (também conhecidas como Cláusulas Modelo da UE); e
(c) medidas técnicas e organizacionais específicas dos produtos da GoTo.

Além disso, para atender aos requisitos da CCPA, nosso DPA global inclui:

a) definições revisadas mapeadas conforme a CCPA;
b) direitos de acesso e exclusão; e
c) garantias de que a GoTo não venderá as informações pessoais de nossos Clientes, Usuários e Usuários Finais.

Nosso DPA global também inclui disposições para:

(a) abordar a conformidade da GoTo com a LGPD;
(b) respaldar transferências legais de Dados Pessoais de/para o Brasil; e
(c) garantir que nossos Usuários desfrutem dos mesmos benefícios de privacidade que nossos outros Usuários globais.

## 20.4 Estruturas de transferência

A GoTo executa transferências de dados internacionais legais de acordo com as seguintes estruturas:

### 20.4.1 Cláusulas Contratuais Padrão

As Cláusulas Contratuais Padrão (SCCs), às vezes chamadas de Cláusulas Modelo da UE, são termos contratuais padronizados, reconhecidos e adotados pela Comissão Europeia, para garantir que quaisquer Dados Pessoais que saiam do Espaço Econômico Europeu (EEE) sejam transferidos em conformidade com a lei de proteção de dados da UE. As SCCs, revisadas e emitidas em 2021, são incorporadas ao DPA global da GoTo para permitir que os clientes da GoTo transfiram dados para fora do EEE em conformidade com o RGPD.

### 20.4.2 Estrutura de Privacidade de Dados

A Estruturas de Privacidade de Dados (DPF) entre UE e EUA e a entre Suíça e EUA, bem como o Adendo do Reino Unido à DPF entre UE e EUA, são estruturas voluntárias que, respectivamente, fornecem mecanismos para que as empresas transfiram dados pessoais da UE, da Suíça e do Reino Unido para os EUA em conformidade com os regulamentos de proteção de dados nessas jurisdições. A GoTo está em conformidade com cada uma dessas estruturas com relação à coleta, ao uso e à retenção de dados pessoais da UE, da Suíça e do Reino Unido, respectivamente. Para saber mais sobre a DPF e ver a certificação da GoTo, visite o site da DPF.

### 20.4.3 Certificações APEC CBPR e PRP

A GoTo obteve as certificações CBPR (Cross-Border Privacy Rules) e PRP (Privacy Recognition for Processors) da Cooperação Econômica Ásia-Pacífico (APEC). As estruturas CBPR e PRP da APEC são as primeiras estruturas de regulamentação de dados aprovadas para a transferência de dados pessoais entre os países membros da APEC e foram obtidas e validadas de forma independente pela TrustArc, um fornecedor terceirizado de conformidade de proteção de dados aprovado pela APEC.

### 20.4.4 Medidas Suplementares

Além das medidas especificadas nestas TOMs, a GoTo criou um documento de perguntas frequentes destinado a delinear as medidas suplementares implementadas para executar as transferências legais nos termos do Capítulo 5 do RGPD e abordar e orientar quaisquer análises caso a caso recomendadas pelo Tribunal de Justiça Europeu em conjunto com o uso das SCCs.

## 20.5 Solicitações de dados

A GoTo mantém processos abrangentes para facilitar o recebimento de solicitações relacionadas à proteção de dados e à segurança, incluindo o portal IRM, o endereço de e-mail de privacidade (privacy@goto.com) e o suporte ao Cliente em https://support.goto.com.

## 20.6 Divulgações de subprocessadores e data centers

A GoTo publica as divulgações de subprocessadores em seu Trust & Privacy Center (https://www.goto.com/company/trust/resource-center). Essas divulgações especificam os nomes, os locais e as finalidades de processamento dos provedores de hospedagem de

dados e outros terceiros que processam o Conteúdo do Cliente como parte do fornecimento do Serviço aos Clientes da GoTo.

## 20.7 Restrições de processamento de dados sensíveis

A menos que expressamente solicitado pela GoTo ou que o Cliente tenha recebido permissão por escrito da GoTo, os seguintes tipos de dados sensíveis não devem ser carregados nem fornecidos de outra forma à GoTo:

- Números de identificação emitidos pelo governo e imagens de documentos de identificação.
- Informações relacionadas à saúde de um indivíduo, incluindo, entre outras, Informações Protegidas de Saúde (PHI), conforme identificadas na Lei de Portabilidade e Responsabilidade de Seguro de Saúde (HIPAA) dos EUA, bem como em outras leis e regulamentações relevantes aplicáveis.
- Informações relacionadas a contas financeiras e instrumentos de pagamento, incluindo, entre outras, dados de cartão de crédito. A única exceção geral a essa disposição se estende aos formulários e páginas de pagamento explicitamente identificados usados pela GoTo para coletar o pagamento pelo Serviço.
- Quaisquer informações especialmente protegidas pelas leis e regulamentos aplicáveis, especificamente informações sobre raça, etnia, crenças religiosas ou políticas, filiação a organizações etc.

## 20.8 Conformidade em ambientes regulamentados

Os clientes são responsáveis pela implementação de políticas, procedimentos e outras proteções apropriadas relacionadas ao uso do GoTo Resolve para oferecer suporte a dispositivos em ambientes regulamentados.

# 21 Controles de segurança e privacidade de terceiros

Antes de contratar fornecedores terceirizados que processam o Conteúdo do Cliente ou dados confidenciais, sensíveis ou de funcionários, a GoTo revisa e analisa as práticas de segurança e privacidade do fornecedor usando os canais de Aquisição apropriados. Conforme apropriado, o GoTo pode obter e avaliar periodicamente a documentação ou os relatórios de conformidade dos fornecedores para garantir que seu ambiente de controle e seus padrões continuem sendo suficientes.

A GoTo celebra contratos por escrito com todos os fornecedores terceirizados e utiliza modelos de aquisição aprovados pela GoTo ou negocia os termos e condições padrão desses terceiros para atender aos padrões de privacidade e segurança aceitos pela GoTo quando necessário. As equipes de Finanças, Jurídico, Privacidade e Segurança estão envolvidas no processo de análise de fornecedores e verificam se eles atendem aos requisitos contratuais e de tratamento de dados obrigatórios específicos, conforme necessário e/ou apropriado. As políticas de risco de terceiros da GoTo regem os requisitos de privacidade e segurança dos fornecedores com base no tipo e na duração do processamento de dados e no nível de acesso. Quando apropriado (por exemplo, quando o Conteúdo do Cliente é processado ou armazenado), os contratos com fornecedores incluem requisitos de "conformidade com a lei aplicável", um DPA ou documento semelhante que aborda tópicos como RGPD, CCPA, LGPD e restrições de uso e venda, conforme apropriado. Por exemplo, o DPA do fornecedor da

GoTo tem restrições quanto à "venda" de dados, conforme definido na CCPA. Da mesma forma, adendos de segurança com controles adequados e requisitos de sistemas são implementados com fornecedores relevantes.

# 22 Como entrar em contato com a GoTo

Os clientes podem entrar em contato com a GoTo pelo e-mail support.goto.com para consultas gerais. Caso tenha dúvidas ou solicitações relacionadas à proteção ou segurança de dados, acesse nosso portal IRM ou envie um e-mail para privacy@goto.com.