# Anexo de Segurança dos Serviços da Citrix

Versão 2.1
Em vigor em quinta-feira,
1 de julho de 2021

# Índice

Este Anexo de Segurança dos Serviços da Citrix (o "Anexo") descreve os controles de segurança implementados em conexão com o desempenho dos serviços do Citrix Cloud, serviços de suporte técnico ou serviços de consultoria (os "Serviços") fornecidos sob a licença e/ou contrato de serviços da Citrix relevante e a ordem aplicável aos Serviços (coletivamente, o "Contrato"). Os serviços de demonstração beta ou de laboratório/tecnologia (incluindo o Citrix Cloud Labs) e os sistemas internos de TI da Citrix não envolvidos no fornecimento dos Serviços estão fora do escopo deste Anexo.

Os termos em maiúscula têm o significado estabelecido no Contrato ou conforme aqui definido. "Conteúdo do Cliente" significa quaisquer dados carregados na conta do Cliente para armazenamento ou dados no ambiente de processamento do Cliente ao qual a Citrix possa receber acesso para prestar Serviços. "Logs" significam registros de Serviços, incluindo, entre outros, dados e informações sobre desempenho, estabilidade, uso, segurança, suporte e informações técnicas sobre dispositivos, sistemas, softwares, serviços ou periféricos relacionados ao uso dos Serviços pelo Cliente.

## 1. Escopo

Este Anexo descreve os controles administrativos, físicos e técnicos de segurança que a Citrix emprega para manter a confidencialidade, integridade e disponibilidade de seus serviços. Esses controles aplicam-se aos sistemas e ambientes operacionais e de serviços da Citrix. A Citrix emprega ISO/IEC 27002 como base para seu programa de segurança de serviços e obteve certificações e avaliações do setor para serviços específicos. Informações adicionais estão disponíveis na seção “Privacidade e Conformidade” do Citrix Trust Center.

A Citrix busca fortalecer e melhorar continuamente suas práticas de segurança e, portanto, reserva-se o direito de modificar os controles aqui descritos. Quaisquer modificações não diminuirão o nível de segurança durante o período relevante dos Serviços.

## 2. Programa de Segurança e Estrutura de Política

A Citrix possui um programa de segurança e uma estrutura de políticas que são estabelecidos e aprovados pela gerência sênior e executiva da Citrix, representando várias áreas de negócios em toda a empresa.

### 2.1 Supervisão de Riscos de Segurança

O Comitê de Supervisão de Riscos Cibernéticos da Citrix (CROC) rege as atividades de gerenciamento de riscos de segurança. O CROC consiste em gerenciamento e liderança multifuncional. A equipe de liderança executiva revisa a participação do comitê anualmente para confirmar a cobertura adequada das áreas operacionais e de negócios.

O CROC se reúne trimestralmente e fornece orientação, discernimento e orientação na identificação, na avaliação e no tratamento de riscos de segurança, tanto nas operações corporativas quanto na infraestrutura de prestação de serviços.

### 2.2 Gerenciamento de Riscos de Segurança

A Citrix utiliza um programa de gerenciamento de riscos de segurança (SRM) que identifica ameaças em potencial aos produtos e serviços Citrix e à infraestrutura Citrix, classifica a importância dos riscos associados a essas ameaças, desenvolve estratégias de mitigação de riscos e faz parceria com as equipes de produtos e engenharia da Citrix para implementar essas estratégias.

O programa SRM aplica estruturas reconhecidas pelo setor, como ISO/IEC 31000 e ISO/IEC 27005.

### 2.3 Segurança da Informação

A Citrix nomeou um Diretor de Segurança da Informação (CISO), responsável pela supervisão da segurança e pela estratégia, conformidade e aplicação de políticas. O Diretor de Monitoramento e Resposta de Segurança lidera o processo de resposta a incidentes, incluindo investigação, contenção e correção.

### 2.4 Segurança Física e Ambiental

A equipe de Segurança da Citrix, juntamente com o Gerenciamento de Instalações, supervisiona o acesso físico às instalações da Citrix.

## 3. Controle de Acesso

A Citrix exige o uso de medidas de controle de acesso projetadas para garantir que os privilégios apropriados sejam atribuídos e mantidos para o acesso aos sistemas, ativos, dados e instalações da empresa, a fim de proteger contra possíveis danos, comprometimentos ou perdas. A Citrix segue o Princípio do Mínimo Privilégio, ou segurança baseada em funções, limitando o acesso do usuário apenas ao necessário para desempenhar funções.

Os gerentes projetam funções para fornecer segregação adequada de tarefas, distribuindo tarefas e privilégios entre várias pessoas, a fim de manter a proteção contra fraudes e erros.

### 3.1 Novas Contas, Funções e Solicitações de Acesso

A Citrix requer uma solicitação formal de acesso aos sistemas ou dados da empresa. Cada solicitação de acesso requer uma aprovação mínima do gerente do usuário para confirmar que a função e o acesso do usuário. Os administradores de acesso confirmam que as aprovações necessárias são obtidas antes de conceder acesso aos sistemas ou dados.

### 3.2 Revisão da Conta

A Citrix mantém e atualiza um registro de privilégios de segurança para funcionários e contratados autorizados a acessar sistemas Citrix que contenham Conteúdo do Cliente. O princípio do mínimo privilégio é aplicado.

A Citrix realiza, no mínimo, análises semestrais de contas de usuários e permissões atribuídas para os principais sistemas. Quaisquer alterações necessárias como resultado das análises estão sujeitas a um processo formal de solicitação de acesso para confirmar o usuário e a função do usuário exige acesso ao(s) sistema(s) relevante(s).

### 3.3 Remoção de Conta, Função e Acesso

A Citrix exige que o acesso do usuário seja desabilitado, revogado ou removido imediatamente após a notificação de uma alteração de função (se aplicável), rescisão, conclusão do contrato do usuário ou saída da empresa.

As solicitações de remoção de acesso são documentadas e rastreadas.

### 3.4 Credenciais

A Citrix requer autenticação de vários fatores para acesso remoto aos sistemas da Citrix pelos funcionários e aplica as seguintes práticas de gerenciamento e gerenciamento de senhas:

- As senhas são alternadas regularmente, de acordo com os requisitos do sistema definidos pela Citrix
- As senhas devem atender aos requisitos de comprimento e complexidade, incluindo uma mistura de dígitos, caracteres especiais e letras maiúsculas e minúsculas, um número mínimo de caracteres e a proibição de palavras comuns ou de dicionário
- IDs de usuário desativados ou expirados não são concedidos a outras pessoas
- A Citrix mantém procedimentos para desativar senhas que foram inadvertidamente divulgadas
- A Citrix monitora tentativas repetidas de obter acesso aos Serviços usando uma senha inválida e executa ações automatizadas para bloquear tentativas repetidas

A Citrix usa práticas projetadas para manter a confidencialidade e a integridade das senhas quando elas são atribuídas, distribuídas e armazenadas, como:

- A Citrix exige que as senhas sejam mantidas com hash durante todo o ciclo de vida
- A Citrix proíbe o compartilhamento de senhas

## 4. Desenvolvimento e Manutenção de Sistemas

A Citrix mantém um processo Secure by Design, que inclui procedimentos de padrões e controles de alteração projetados para atender aos requisitos de segurança dos sistemas de informação, revisão e teste de código e segurança em relação ao uso de dados de teste. Esse processo é gerenciado e monitorado por uma equipe de segurança especializada, que também é responsável pela revisão do design, modelagem de ameaças, revisão manual de código e verificações pontuais e testes de penetração.

### 4.1 Princípios de Design Seguro

A Citrix adotou uma metodologia formal de ciclo de vida de desenvolvimento de sistemas (SDLC) que governa o desenvolvimento, a aquisição, a implementação e a manutenção de sistemas de informação computadorizados e requisitos de tecnologia relacionados.

A Citrix usa um sistema baseado em software para gerenciar revisões e aprovações de Código Aberto, o que inclui a realização de verificações e auditorias periódicas de seus produtos de software. A Citrix possui políticas documentadas, disponíveis para todos os funcionários, sobre o uso do código aberto, além de treinamento para desenvolvedores e a respectiva gerência sobre as práticas recomendadas de código aberto.

### 4.2 Gerenciamento de Alterações

O processo de gerenciamento de alterações de infraestrutura e software da Citrix atende aos requisitos de segurança e exige que as alterações de software e infraestrutura sejam autorizadas, formalmente documentadas, testadas (conforme aplicável), revisadas e aprovadas antes da implantação para o

ambiente de produção. As alterações de infraestrutura e software são gerenciadas e rastreadas usando sistemas de gerenciamento de trabalho.

O processo de gerenciamento de alterações é segregado adequadamente, e o acesso para migrar as alterações para a produção é restrito ao pessoal autorizado.

## 5. Gerenciamento de Ativos

### 5.1 Gerenciamento de Ativos Físicos e Virtuais

A Citrix mantém um inventário dinâmico de sistemas físicos e virtuais gerenciados pela Citrix usados para executar os Serviços (''Ativos de Serviço''). Os proprietários do sistema são responsáveis por manter e atualizar seus Ativos de Serviço de acordo com os padrões de segurança da Citrix.

Existem procedimentos formais de descarte para orientar o descarte seguro dos dados da Citrix e do Cliente. A Citrix descarta os dados quando não são mais necessários, com base na classificação e no uso de processos de exclusão projetados para impedir que os dados sejam reconstruídos ou lidos.

Os ativos da tecnologia da Citrix são higienizados e descartados quando não são mais necessários na área designada ou atribuída. Ativos de tecnologia incluem, entre outros, dispositivos de computação individuais, dispositivos de computação multifuncionais, dispositivos de armazenamento, dispositivos de imagem e dispositivos de rede. O descarte é coordenado através dos Serviços de Risco à Segurança Global e Segurança da Informação.

### 5.2 Gerenciamento de Aplicativos e Sistemas

Os proprietários de aplicativos e sistemas são responsáveis por revisar e classificar os dados que armazenam, acessam, descartam ou transmitem. Entre outros controles, os funcionários e contratados devem:

- Classificar o Conteúdo do Cliente entre as duas categorias mais altas de informações confidenciais da Citrix e aplicar as restrições de acesso apropriadas
- Restringir a impressão do Conteúdo do Cliente e descartar os materiais impressos em recipientes seguros
- Não armazenar informações corporativas ou confidenciais em qualquer equipamento ou dispositivo que não atenda aos requisitos das políticas e padrões de segurança da Citrix
- Proteger computadores e dados sem supervisão

### 5.3 Retenção de Dados

O Conteúdo do Cliente armazenado como parte dos serviços do Citrix Cloud pode ser acessado por um período limitado após o término dos Serviços e, em seguida, excluído (exceto cópias de backup) após a confirmação do envio de que a exclusão ocorrerá. Detalhes adicionais são fornecidos na documentação de serviços específicos. O Conteúdo do Cliente também pode ser retido após a conclusão dos serviços, se necessário para fins legais. A Citrix cumprirá os requisitos deste Anexo até que o Conteúdo do Cliente seja excluído permanentemente.

## 6. Segurança de Recursos Humanos

Manter a segurança do Conteúdo do Cliente é um dos principais requisitos para todos os funcionários e contratados da Citrix. O Código de Conduta de Negócios da Citrix exige que todos os funcionários e contratados cumpram as políticas e padrões de segurança da Citrix e aborda especificamente a proteção de informações confidenciais e informações pessoais de clientes, parceiros, fornecedores e funcionários da Citrix.

Todos os funcionários e contratados da Citrix estão sujeitos a contratos de confidencialidade que abrangem as informações do Cliente. A organização de Segurança da Citrix também se comunica regularmente com os funcionários sobre tópicos relacionados a informações e segurança física, a fim de manter o conhecimento de segurança sobre tópicos específicos.

### 6.1 Seleção em Segundo Plano

Atualmente, a Citrix utiliza fornecedores de seleção em segundo plano para todas as novas contratações em todo o mundo e exige o mesmo para o pessoal de terceiros, exceto onde limitado pelas leis locais ou regulamentos de emprego.

### 6.2 Treinamento

Todos os funcionários são obrigados a receber treinamento em proteção de dados e nas políticas da empresa projetadas para proteger a segurança das Informações Confidenciais da Citrix, que incluem as Informações Confidenciais de nossos Clientes, parceiros, fornecedores e funcionários. O treinamento abrange as práticas de privacidade e os princípios que se aplicam ao manuseio de informações pessoais por funcionários, incluindo a necessidade de impor limitações ao uso, acesso, compartilhamento e retenção de informações pessoais. Os membros da organização de Engenharia passam por um treinamento específico, que consiste em desenvolvimento, arquitetura e codificação seguros.

### 6.3 Cumprimento

Todos os funcionários devem cumprir as políticas e os padrões de segurança e privacidade da Citrix. O descumprimento está sujeito a ações disciplinares, incluindo rescisão do contrato de trabalho.

## 7. Segurança de Operações

### 7.1 Segurança de Rede e Sistema

A Citrix documentou os padrões de proteção de rede e sistema projetados para garantir que as redes e os sistemas estejam configurados com segurança. Os procedimentos exigidos sob esses padrões incluem, mas não estão limitados a:

- Alterar ou desabilitar as configurações e/ou contas padrão
- Aplicar banners de login
- Uso controlado do acesso administrativo
- Restringir contas de serviço apenas para a finalidade em que foram criadas
- Definir configurações de log e alerta apropriadas para auditoria

A Citrix requer a implementação de softwares antimalware em servidores e estações de trabalho e verifica a rede em busca de softwares mal-intencionados.

Os controles de rede controlam o acesso ao Conteúdo do Cliente. Isso inclui, conforme aplicável: a configuração de uma zona não confiável intermediária entre a Internet e a rede interna que inclui um mecanismo de segurança para restringir o acesso e o tráfego não autorizado; a segmentação de rede para impedir o acesso não autorizado ao Conteúdo do Cliente; e a separação de servidores da Web e de aplicativos dos servidores de banco de dados correspondentes em uma estrutura em camadas que restringe o tráfego entre as camadas.

### 7.2 Registro em log

A Citrix coleta Logs para confirmar o funcionamento correto de nossos Serviços, para ajudar na solução de problemas do sistema e para proteger nossas redes e o Conteúdo do Cliente. Os Logs podem incluir ID de acesso, horário, autorização concedida ou negada, dados de diagnóstico, como arquivos de rastreamento e falha, e outras informações e atividades relevantes.

Os Logs podem ser usados de uma forma identificável (i) para fornecer, proteger, gerenciar, medir e aprimorar os Serviços e análises associadas, (ii) conforme solicitado pelo Cliente ou seus usuários finais e/ou (iii) para conformidade com as políticas da Citrix, a lei aplicável, o regulamento ou a solicitação do governo. Isso pode incluir o monitoramento do desempenho, estabilidade, uso e segurança dos Serviços e componentes relacionados. Os clientes não podem bloquear ou interferir com esse monitoramento.

Para obter mais informações sobre o Conteúdo do Cliente e a manipulação de Logs, consulte a seção Privacidade e Conformidade do Citrix Trust Center, que contém vários documentos técnicos sobre o Citrix Logging.

### 7.3 Gerenciamento de Certificados, Credenciais e Segredos

A Citrix mantém políticas que abrangem o ciclo de vida de certificados, credenciais e segredos para garantir proteção, disponibilidade e confidencialidade. Os guardiões secretos devem ser documentados e reconhecer formalmente que aceitam as responsabilidades como pessoal de gerenciamento de segredos.

As responsabilidades incluem, mas não estão limitadas a:

- Certificados devem ser emitidos por uma autoridade de certificação aprovada
- Chaves criptográficas não podem ser armazenadas ou transmitidas em texto sem formatação e devem usar protocolos criptográficos fortes e aprovados
- Credenciais e segredos devem ser alternados pelo menos uma vez por ano e armazenados em uma ferramenta de gerenciamento de autenticação com privilégios aprovada

### 7.4 Gerenciamento de Vulnerabilidades

A Citrix monitora aplicativos e sistemas em busca de vulnerabilidades por meio da varredura automatizada de vulnerabilidades e portas regularmente. Varreduras totalmente autenticadas também são realizadas pelo menos uma vez por mês e incluem dispositivos na rede, componentes do servidor de aplicativos, servidores físicos e virtuais e pontos de extremidade.

As vulnerabilidades identificadas devem ser corrigidas em um cronograma que depende da classificação de gravidade e das recomendações do fornecedor. Nos casos em que um patch, atualização ou mitigação permanente não estiver disponível, contramedidas apropriadas serão usadas para reduzir o risco de exploração da vulnerabilidade.

## 8. Criptografia

### 8.1 Proteção de Dados em Trânsito

A Citrix implantou protocolos de transmissão segura para transmissão de informações em redes públicas que fazem parte dos Serviços. Os Serviços são protegidos por criptografia e o acesso via Internet é protegido por conexões TLS.

### 8.2 Proteção de Dados em Repouso

A Citrix requer que todas as estações de trabalho usadas para fornecer serviços sejam criptografadas com um mínimo de criptografia de disco completo de 128 bits. O Conteúdo do Cliente não pode ser armazenado em nenhum dispositivo portátil, a menos que seja criptografado.

Alguns Serviços do Cloud criptografam determinados elementos de dados por padrão e também podem fornecer outros recursos de criptografia para os clientes implementarem. Consulte a documentação aplicável dos Serviços do Cloud em docs.citrix.com para obter detalhes adicionais.

## 9. Segurança Física

### 9.1 Instalações da Citrix

A Citrix mantém os seguintes controles projetados para impedir o acesso não autorizado a qualquer instalação:

- O acesso às instalações é limitado a indivíduos autorizados
- Os visitantes devem se registrar em um registro digital de visitantes e ser acompanhados ou observados o tempo todo
- Crachás de identificação são necessários para funcionários, contratados e convidados e deverão estar visíveis o tempo todo quando estes estiverem nas instalações
- A Segurança gerencia e controla o acesso às instalações após o horário de funcionamento
- Guardas de segurança, detecção de intrusão e/ou câmeras de CFTV monitoram os pontos de entrada do prédio, as docas de carregamento e expedição e as áreas de acesso público (os mecanismos para monitorar o acesso podem diferir entre as instalações, dependendo da instalação e do local)

Além disso, as instalações da Citrix fornecem:

- Sistemas ou dispositivos de supressão e detecção de incêndio
- Sistemas ou dispositivos de controle climático (temperatura, umidade etc.)
- Válvulas de isolamento ou fechamento de registro de água acessíveis
- Fontes de energia alternativas (gerador, sistema no-break etc.)
- Saídas de emergência e rotas de evacuação

As salas de armazenamento de dados localizadas nos escritórios são protegidas por meio de acesso e monitoramento de crachás.

### 9.2 Datacenters

Além dos controles de instalações da Citrix descritos acima, para instalações de propriedade e gerenciadas pela Citrix, a Citrix implementa controles adicionais nos datacenters usados para fornecer os Serviços.

A Citrix usa sistemas projetados para proteger contra a perda de dados devido a falha na fonte de alimentação ou interferência na linha, incluindo infraestrutura de serviço global e redundante configurada com sites de recuperação de desastres. Os datacenters e os provedores de serviços da Internet (ISPs) são avaliados para otimizar o desempenho em relação à largura de banda, latência e isolamento da recuperação de desastres.

Os datacenters estão situados em instalações que são neutras à operadora de ISP e fornecem contratos de segurança física, energia redundante, redundância de infraestrutura e tempo de atividade dos principais fornecedores.

Quando a Citrix usa datacenters ou serviços em nuvem de terceiros para a entrega dos Serviços, a Citrix contrata fornecedores que atendem ou excedem os requisitos de segurança física e ambiental das instalações da Citrix.

## 10. Continuidade dos Negócios e Recuperação de Desastres

### 10.1 Continuidade dos Negócios

A Citrix planeja estrategicamente a continuação das operações de negócios durante situações adversas ou perturbadoras e projeta sistemas para manter os serviços operacionais durante a ocorrência de tais eventos.

A Citrix realiza uma Análise de Impacto nos Negócios (BIA) em nível de departamento pelo menos a cada dois anos, com uma revisão anual a cada ano. A BIA é usada para criar um Plano de Continuidade de Negócios (BCP) de departamento, que identifica e documenta para cada departamento seus requisitos de recursos, parâmetros e métodos de recuperação, necessidades de realocação e as salvaguardas de segurança necessárias ao longo do processo para evitar falhas ou lacunas. A gerência sênior de cada departamento revisa e aprova o BCP anualmente, ou quando ocorrem mudanças organizacionais significativas.

A Citrix mantém planos de emergência e contingência para todas as instalações da Citrix. Caso as instalações não estejam disponíveis, os funcionários terão a opção de trabalhar remotamente em outras instalações da Citrix ou no local de sua escolha. Estratégias de recuperação adicionais estão documentadas nos BCPs, quando aplicável.

### 10.2 Recuperação de Desastres

A Citrix se esforça para minimizar o impacto de interrupções operacionais ou de serviço implementando processos e controles projetados para garantir a restauração e recuperação estáveis e ordenadas dos sistemas e dados de negócios da Citrix. A Citrix implementa redundância para todos os sistemas, dados e infraestrutura de missão crítica. O Plano de Recuperação de Desastres (DRP) usa a avaliação realizada na BIA mencionada acima para identificar e documentar parâmetros de tempo de recuperação, métodos, prioridades e salvaguardas de segurança necessárias ao longo do processo para evitar falhas ou lacunas.

O plano descreve a estrutura geral e a abordagem para restaurar sistemas e dados críticos, incluindo, entre outros:

- Funções e responsabilidades de indivíduos ou equipes
- Informações de contato para pessoal essencial ou terceiros

- Requisitos e planos de treinamento para pessoal essencial
- Objetivos de recuperação, prioridades de restauração e métricas de sucesso
- Esquema de recuperação e restauração completas

A gerência sênior analisa e aprova o DRP anualmente, ou quando ocorrem mudanças organizacionais significativas.

## 11. Resposta a Incidentes

A Citrix mantém um Plano de Resposta a Incidentes de Segurança Cibernética que detalha os processos para detectar, relatar, identificar, analisar e responder a incidentes de segurança que afetam as redes e/ou sistemas gerenciados pela Citrix ou o Conteúdo do Cliente. O treinamento e o teste de resposta a Incidentes de Segurança são realizados pelo menos anualmente.

"Incidente de Segurança" significa acesso não autorizado ao Conteúdo do Cliente, resultando na perda de confidencialidade, integridade ou disponibilidade. Se a Citrix determinar que o Conteúdo do Cliente sob seu controle foi sujeito a um Incidente de Segurança, o Cliente será notificado dentro do prazo exigido por lei. O aviso da Citrix descreverá, onde conhecido, a natureza do incidente, o período e o potencial impacto no Cliente.

A Citrix mantém um registro de cada Incidente de Segurança.

## 12. Gerenciamento de Fornecedores

A Citrix pode usar subcontratados e agentes para prestar os Serviços. Quaisquer subcontratados e agentes terão direito a acessar o Conteúdo do Cliente apenas conforme necessário para prestar os Serviços e ficarão vinculados por acordos escritos que exigem que eles forneçam pelo menos o nível de proteção de dados exigido da Citrix por este Anexo, conforme aplicável. A Citrix permanece responsável o tempo todo pelo cumprimento de seus subcontratados e agentes com os termos do Contrato, conforme aplicável. Uma lista de subprocessadores da Citrix que possam ter acesso ao Conteúdo do Cliente está disponível no Citrix Trust Center.

### 12.1 Integração

O Programa de Gerenciamento de Riscos de Terceiros da Citrix fornece uma abordagem sistemática para gerenciar riscos de segurança representados pelo uso de fornecedores terceirizados. A Citrix trabalha para identificar, analisar e mitigar os riscos de segurança antes de se envolver na aquisição de tais terceiros.

A Citrix firma acordos com fornecedores para documentar medidas e obrigações de segurança relevantes, consistentes com as especificadas neste Anexo.

### 12.2. Avaliação Contínua

A Citrix realiza avaliações periódicas de risco à segurança, projetadas para garantir que as medidas de segurança permaneçam em vigor durante todo o relacionamento com o fornecedor. As alterações nos serviços prestados ou alterações nos contratos existentes exigem uma avaliação de risco de segurança para confirmar que as alterações não apresentam riscos adicionais ou indevidos.

### 12.3 Encerramento

A Citrix se esforça para notificar a organização de compras da empresa 90 dias antes do plano para encerrar um relacionamento com o fornecedor ou antes da expiração do contrato com um fornecedor (a menos que seja necessária uma rescisão antecipada). A organização de compras da empresa coordena o término dos relacionamentos existentes para confirmar se os dados e ativos corporativos da Citrix estão protegidos e tratados adequadamente.

## 13. Conformidade

### 13.1 Tratamento de Dados Pessoais

Dados pessoais são informações relacionadas a um indivíduo identificado ou identificável. O Cliente determina os dados pessoais que inclui no Conteúdo do Cliente. Na execução dos Serviços, a Citrix atua como um processador de dados, e o Cliente permanece o controlador de dados de quaisquer dados pessoais contidos no Conteúdo do Cliente. A Citrix agirá de acordo com as instruções do Cliente em relação ao processamento desses dados pessoais, conforme especificado no Contrato.

Informações adicionais sobre o tratamento de dados pessoais sujeitos ao Regulamento Geral de Proteção de Dados, incluindo os mecanismos empregados para a transferência internacional desses dados, são fornecidas no Contrato de Processamento de Dados da Citrix.

### 13.2 Localização dos Serviços

Os Clientes dos Serviços do Citrix Cloud mantêm o controle sobre a escolha da localização geográfica do seu ambiente dos Serviços do Cloud (*veja também Citrix Cloud Geographical Considerations*). Em nenhum momento durante a assinatura aplicável dos Serviços do Cloud, a Citrix alterará a localização geográfica do ambiente escolhido pelo Cliente sem o consentimento do Cliente. Observe que alguns Serviços do Cloud podem não permitir a escolha de certas localizações geográficas e, como parte da prestação geral dos Serviços, o Conteúdo do Cliente pode ser transferido para os Estados Unidos ou outros países onde a Citrix e/ou seus provedores de serviços operam, conforme necessário para fornecer os Serviços.

### 13.3 Divulgação do Conteúdo do Cliente

A Citrix pode divulgar o Conteúdo do Cliente na medida exigida por lei, inclusive em resposta a uma intimação, ordem judicial ou administrativa ou outro instrumento vinculativo (cada um considerado uma "Demanda"). Exceto onde proibido por lei, a Citrix notificará prontamente o Cliente sobre qualquer Demanda e fornecerá ao Cliente assistência razoavelmente necessária para que o Cliente responda à Demanda em tempo hábil.

### 13.4 Requisitos Regulamentares e de Segurança do Cliente

Os Serviços foram projetados para serem entregues em um ambiente de TI do Cliente maior e, portanto, os Clientes mantêm total responsabilidade por todos os aspectos de segurança não expressamente gerenciados pela Citrix, incluindo, entre outros, integração técnica com os Serviços, gerenciamento e controles de acesso do usuário, e todos os aplicativos e redes nas quais os Clientes podem usar em conjunto com os Serviços.

Os Clientes permanecem responsáveis por determinar se o uso dos Serviços, inclusive fornecendo à Citrix acesso a qualquer Conteúdo do Cliente como parte dos serviços, está sujeito a requisitos regulamentares ou de segurança

além daqueles especificados no Contrato, incluindo este Anexo. Os Clientes devem, portanto, garantir que não enviem ou armazenem qualquer Conteúdo do Cliente que seja regido por leis que impõem controles específicos não incluídos neste Anexo, que podem incluir os Regulamentos Internacionais de Trânsito em Armas dos EUA (ITAR) ou regulamentos similares de qualquer país que restringe a importação ou exportação de artigos ou serviços de defesa, informações de saúde protegidas ("PHI"), informações de cartão de pagamento ("PCI") ou dados de distribuição controlada de acordo com os regulamentos governamentais, a menos que especificado no Contrato e na Descrição do Serviço aplicável e as partes tenham firmado quaisquer contratos adicionais (como um Contrato de Associado Comercial da HIPAA) com antecedência, conforme necessário para a Citrix processar esses dados.

## 14. Auditorias e Consultas de Clientes

Até uma vez por ano, a Citrix responde às solicitações de auditoria na forma de respostas às avaliações de risco do Cliente. Os clientes também podem acessar o pacote Citrix Due Diligence a qualquer momento para obter um pacote de segurança e um questionário atualizados. O Pacote Citrix Security Due Diligence foi criado para consultas de segurança do cliente e fornece informações de segurança prontamente disponíveis, incluindo um questionário Standardized Information Gathering (SIG) Lite completo de Avaliações Compartilhadas para cada produto. O questionário SIG é o questionário mais usado entre nossos clientes e é usado em todos os setores da indústria. O Due Diligence Package pode ser baixado do Citrix Trust Center.

## 15. Contatos da Citrix

| Função | Contato |
|---|---|
| Atendimento ao Cliente | https://www.citrix.com/contact/technical-support.html |
| Relatando um Incidente de Segurança | secure@citrix.com |
| Suspeitas de vulnerabilidades nos produtos da Citrix | https://www.citrix.com/about/trust-center/<br>(Clique no botão "Report a Security Issue" (Relatar um problema de segurança). |

citrix.

**Vendas da Empresa**
América do Norte | 800-424-8749
Mundial | +1 408-790-8000

**Locais**
Sede da Empresa | 851 Cypress Creek Road Fort Lauderdale, FL 33309, United States Silicon Valley | 4988 Great America Parkway Santa Clara, CA 95054, Estados Unidos