Revisado pela última vez em 1º de março de 2018

Anexo de Segurança dos Serviços da Citrix

O presente Anexo de Segurança dos Serviços da Citrix (o Anexo) descreve os controles de segurança técnicos e organizacionais empregados em razão dos serviços do Citrix Cloud, dos serviços de suporte técnico ou dos serviços de consultoria regidos por um contrato de licença, assinatura ou serviços da Citrix. O presente Anexo é incorporado por referência a tais contratos de serviço (os "Contratos"). Este Anexo não se aplica a serviços beta ou lab/tech preview, incluindo o Citrix Cloud Labs.
Os termos em letras maiúsculas têm o significado estabelecido no Contrato ou definido neste documento, incluindo o Artigo 7, Definições, abaixo.

Artigo 1. Controles de Segurança da Citrix

Este artigo descreve os controles físicos, lógicos e administrativos que a Citrix emprega para proteger as obrigações de segurança associadas aos Serviços e ao Cliente. A Citrix emprega o ISO/IEC 27002 como referência em seu programa de segurança de Serviços.

Os controles especificados no Artigo 1.A se aplicam a todos os Serviços. Os controles adicionais especificados na Seção 1.B aplicam-se a todos os Citrix Cloud Services geralmente disponíveis (coletivamente chamados de "Serviços de Nuvem").

A Citrix se reserva o direito de modificar os controles especificados neste Artigo 1, desde que os controles empregados durante um período de serviço pago pelo Cliente protejam o Conteúdo do Cliente pelo menos como os especificados neste Artigo 1 na data de efetivação de tal período.

1.A. Controles de Segurança Empresarial – Todos os Serviços

Área	Controle(s)
Gerenciamento do Programa de Segurança	**Propriedade de Segurança**. A Citrix indicou um ou mais agentes de segurança responsáveis pela coordenação e monitoramento dos controles de segurança dos Serviços. **Funções e Responsabilidades de Segurança**. Os funcionários da Citrix com acesso ao Conteúdo do Cliente estão sujeitos a obrigações de confidencialidade. **Políticas de Segurança do Serviço.** A Citrix mantém uma Estrutura de Segurança Global (GSF) abrangente, que fornece os princípios gerais de segurança e proteção estabelecidos e aprovados pela administração executiva da Citrix. As políticas estabelecem os requisitos de segurança de maneira clara e concisa. Os padrões definem o processo ou a metodologia de

Área	Controle(s)
	cumprimento dos requisitos das políticas. O programa de segurança da GSF passa por revisões e avaliações periódicas. A Citrix mantém um resumo do programa da GSF e o fornecerá aos clientes mediante solicitação. **Gerenciamento de Risco do Produto.** A Citrix realiza avaliações de áreas importantes de risco associadas aos Serviços, incluindo, apenas a título de exemplo e conforme aplicável, avaliações de risco de privacidade, revisões de código aberto e análise de controle de exportação.
Gerenciamento de Ativos	**Inventário de Ativos**. A Citrix mantém um inventário de equipamentos gerenciados pela Citrix usados para executar os Serviços ("Ativos"). Os proprietários de sistemas identificados são responsáveis por manter e atualizar o inventário, conforme necessário. **Tratamento de Ativos e Dados** A Citrix identifica e classifica o Conteúdo do Cliente para garantir que o acesso seja adequadamente restrito. A Citrix impõe restrições à impressão do Conteúdo do Cliente e à eliminação de materiais impressos que contenham Conteúdo do Cliente. Os funcionários da Citrix devem obter autorização antes de armazenar o Conteúdo do Cliente em dispositivos portáteis, acessar remotamente o Conteúdo do Cliente ou processar o Conteúdo do Cliente fora dos locais administrados pela Citrix ou por seus provedores de serviços.
Gerenciamento do Acesso	**Política de Acesso.** A Citrix mantém um registro dos privilégios de segurança de indivíduos com acesso ao Conteúdo do Cliente e segue o princípio do privilégio mínimo. **Autorização de Acesso** A Citrix mantém e atualiza um registro dos funcionários autorizados a acessar os sistemas da Citrix que contêm o Conteúdo do Cliente. O novo acesso aos sistemas é revisado e aprovado pela gerência antes de ser concedido. A Citrix realiza revisões regulares de contas de usuários e permissões atribuídas aos principais sistemas. A Citrix identifica os funcionários que podem conceder, alterar ou cancelar o acesso autorizado a dados e recursos. A Citrix garante que, quando mais de um indivíduo tiver acesso a sistemas que contenham o Conteúdo do Cliente, os indivíduos terão identificadores/logins separados.

Área	Controle(s)
	Privilégios Mínimos A Citrix restringe o acesso ao Conteúdo do Cliente somente àqueles indivíduos que necessitam desse acesso para executar seu trabalho. **Integridade e Confidencialidade** A Citrix exige que os usuários protejam computadores e dados que não estiverem sendo usados. A Citrix exige que as senhas permaneçam ininteligíveis em todo o seu ciclo de vida. **Autenticação** A Citrix usa as práticas padrão do setor para identificar e autenticar usuários que acessam sistemas de informação. Onde os mecanismos de autenticação utilizam senhas, a Citrix segue as práticas padrão do setor em sua manipulação e gerenciamento, incluindo: As senhas são renovadas regularmente, conforme exigido pelos requisitos do sistema e pelos padrões da Citrix As senhas devem atender aos requisitos de tamanho e complexidade, incluindo um tamanho mínimo de 8 caracteres Os funcionários são proibidos de compartilhar senhas Identificadores desativados ou expirados não são concedidos a outros indivíduos A Citrix mantém procedimentos para desativar senhas que foram corrompidas ou reveladas inadvertidamente. A Citrix monitora tentativas repetidas de obter acesso aos Serviços usando uma senha inválida. A Citrix usa práticas concebidas para manter a confidencialidade e a integridade das senhas quando estas são atribuídas, distribuídas e armazenadas.
Prevenção de Perdas	**Software Mal-Intencionado**. A Citrix usa software antivírus e outros controles para evitar que software mal-intencionado obtenha acesso não autorizado ao Conteúdo do Cliente, incluindo softwares mal-intencionados originados de redes públicas. **Descarte de Mídias.** A Citrix descarta mídias quando não são mais necessárias com base na

Área	Controle(s)
	classificação e usando processos seguros de exclusão.
Segurança Física e Ambiental (Controle de Acesso, Controle de Disponibilidade)	**Acesso Físico às Instalações da Citrix** . A Citrix limita a pessoas autorizadas o acesso às suas instalações. Crachás de identificação são necessários para funcionários, empresas contratadas e convidados e devem estar visíveis o tempo todo quando essas pessoas estiverem presentes nas instalações. A Citrix monitora os pontos de entrada das instalações usando vários métodos, incluindo guardas de segurança, detecção de intrusão e câmeras de circuito fechado de televisão. **Proteção contra Interrupções**. A Citrix usa sistemas de proteção contra a perda de dados por falhas no fornecimento de energia ou interferência de linha, incluindo infraestrutura de serviço global e redundante, que é configurada com sites de recuperação de desastres; avaliação de data centers e provedores de serviços de Internet (ISPs) para otimizar o desempenho com relação à largura de banda, à latência e ao isolamento de recuperação de desastres; localização dos data centers em instalações seguras que sejam neutras em relação à operadora de ISP e forneçam segurança física, redundância de energia e redundância de infraestrutura; e contratos de tempo de atividade de fornecedores-chave. **Data Centers Hospedados.** Ao usar data centers colocalizados de terceiros para a prestação dos Serviços, a Citrix exige que o provedor de serviços atenda ou exceda os requisitos de segurança física e ambiental das instalações gerenciadas pela Citrix. Os requisitos mínimos de segurança incluem, entre outros: • Restrições e proteções de acesso físico (autenticação, logs, monitoramento etc.) • Separação adequada de ambientes • Mecanismos de supressão, detecção e prevenção de incêndios • Sistemas de controle climático (temperatura, umidade etc.) **Computação na Nuvem.** Quando a Citrix usa XaaS [Infraestrutura como Serviço (IaaS), Plataforma como Serviço (PaaS), Software como Serviço (SaaS)] para fornecer os Serviços, ela contrata provedores de XaaS que oferecem um nível materialmente semelhante de controle de acesso físico aos seus data centers hospedados.
Segurança de Aplicativo e de Desenvolvimento	**Desenvolvimento e Manutenção do Sistema.** A Citrix mantém um processo Secure by Design (seguro de fábrica), que inclui padrões e procedimentos de controle de alterações criados para atender aos requisitos de segurança dos sistemas de informações, de revisão de código e teste, bem como da segurança relacionada ao uso de dados de teste. Esse processo é gerenciado e monitorado por uma equipe de engenharia de segurança especializada, que também é responsável pela revisão do projeto, modelagem de ameaças, revisão de código e

Área	Controle(s)
	verificações pontuais manual e testes de penetração. **Gerenciamento de Software Livre**. A Citrix usa um sistema de software para gerenciar revisões e aprovações de software livre. Além disso, a Citrix realiza varreduras e auditorias periódicas em seus produtos de software para confirmar a conformidade do software livre. **Gerenciamento de Mudanças.** A Citrix mantém procedimentos de controle de alterações que atendem aos requisitos de segurança de sistemas de informações, testes, aceitação de testes e segurança relacionados ao uso de dados de teste. As alterações em softwares e nas configurações são gerenciadas e rastreadas com sistemas de tíquetes padrão.
Operações Seguras	**Projeto de Rede**. A Citrix implementa mecanismos projetados para aplicar políticas e padrões de gerenciamento de acesso nos Serviços, incluindo controles de rede sobre o acesso ao Conteúdo do Cliente. Isso inclui, conforme apropriado: a configuração de uma zona intermediária não confiável entre a Internet e a rede interna que inclua um mecanismo de segurança para restringir o acesso e o tráfego não autorizado e a separação de servidores da Web e de aplicativos dos servidores de banco de dados correspondentes em uma estrutura em camadas que restrinja o tráfego entre elas.
Gerenciamento de Incidentes	**Resposta a Incidentes**. A Citrix mantém um programa de resposta a incidentes projetado para conter, analisar, remediar e comunicar incidentes de segurança e proteção que afetem as redes e/ou os sistemas gerenciados da Citrix ou o Conteúdo do Cliente. **Notificação de Incidentes**. Se a Citrix determinar que o Conteúdo do Cliente sob seu controle esteve sujeito a um Incidente de Segurança, o Cliente será notificado dentro do período de tempo exigido pela legislação aplicável. **Registro de Incidentes**. A Citrix mantém um registro de Incidentes de Segurança conhecidos, com uma descrição do incidente, o período de tempo, as consequências do incidente, o nome do relator, a quem o incidente foi relatado e o procedimento para recuperar dados e Serviços, conforme aplicável.
Gerenciamento de Fornecedores	**Inclusão**. A Citrix realiza avaliações de segurança de provedores de serviços que terão acesso ao Conteúdo do Cliente e/ou aos componentes dos Serviços que processam o Conteúdo do Cliente. A Citrix exige que os provedores de serviços relacionados aos Serviços cumpram o nível de segurança desta Seção aplicável aos serviços que eles fornecem. Os provedores de serviços que possam acessar o Conteúdo do Cliente sujeito à legislação da União Europeia devem se autocertificar para os programas EU-U.S. e EU-Swiss Privacy Shield ou firmar as Cláusulas Contratuais Padrão.

Área	Controle(s)
	Manutenção Contínua. Os provedores de serviços são avaliados periodicamente, com base na confidencialidade e no risco associados aos seus serviços. **Exclusão.** Após o término de um relacionamento com o fornecedor, o provedor de serviços é obrigado a devolver todo o Conteúdo do Cliente em sua posse ou a certificar que todo o Conteúdo do Cliente foi destruído com segurança.
Continuidade dos Negócios e Recuperação de Desastres	**Continuidade dos Negócios.** A Citrix mantém planos de emergência e contingência para as instalações nas quais estão localizados seus sistemas de informações que processam o Conteúdo do Cliente. **Recuperação de Desastres.** O armazenamento redundante da Citrix e seus procedimentos de recuperação de dados foram concebidos para tentar reconstruir o Conteúdo do Cliente em seu estado original ou no estado replicado pela última vez.
Obrigações de Segurança do Cliente	O cliente é responsável por gerenciar a segurança não incluída expressamente nos Serviços. Isso inclui, entre outros: • Limitar o acesso da Citrix apenas ao Conteúdo do Cliente necessário para o Cliente receber os Serviços. • Proteger seus componentes de rede e serviços contra interferência, incluindo monitoramento e proteção de suas redes e equipamentos de computação. • Baixar o Conteúdo do Cliente quando necessário, tanto durante o prazo dos Serviços quanto no término. • Por padrão, a Citrix criptografa dados em trânsito ou oferece aos clientes meios para criptografá-los. Mais detalhes são fornecidos na documentação dos Serviços. O cliente é responsável por garantir que os dados sejam adequadamente protegidos em trânsito.

1.B. Controles de Segurança Adicionais do Serviços de Nuvem

Área	Controle(s)
Proteção de Dados (Controle de Disponibilidade, Controle de Transmissão, Exclusão de Dados)	**Procedimentos de Failover**. A Citrix implementa mecanismos projetados para lidar com a perda de disponibilidade do Conteúdo do Cliente, incluindo o armazenamento de cópias do Conteúdo do Cliente em um local diferente daquele em que o equipamento principal do computador que processa o Conteúdo do Cliente está localizado. **Dados Além dos Limites**. A Citrix criptografa ou permite que o Cliente criptografe o Conteúdo

Área	Controle(s)
	do Cliente que é transmitido pelas redes públicas que fazem parte de um Serviço. **Retenção.** A Citrix pode reter o Conteúdo do Cliente após o período do Serviço e arquivá-lo para acesso do cliente, quando necessário, para fins legais. A Citrix cumprirá os requisitos deste Anexo até que o Conteúdo do Cliente seja excluído permanentemente. Sujeito à Devolução mencionada abaixo, a Citrix não tem obrigação de reter o Conteúdo do Cliente após o término do Serviço. **Devolução.** Sujeito à disponibilidade e à Descrição dos Serviços aplicável, o Cliente terá 30 (trinta) dias para baixar o Conteúdo do Cliente após a expiração. **Exclusão de Dados**. A Citrix excluirá com segurança o Conteúdo do Cliente quando ele não for mais necessário para um propósito legítimo.
Operações Seguras	**Registro de Logs de Eventos**. Em determinados serviços, a Citrix coleta logs. Os logs podem incluir o ID de acesso, a hora, a autorização concedida ou negada, os dados de diagnóstico, como arquivos de rastreamento e de falha, e outras atividades relevantes. Os logs são usados (**i**) para fornecer, proteger, gerenciar, medir e melhorar os Serviços e a análise associada, (**ii**) conforme orientado ou instruído pelo Cliente e seus Usuários e/ou (**iii**) para manter a conformidade com as políticas da Citrix, a legislação aplicável, o regulamento ou alguma solicitação governamental. Isso pode incluir o monitoramento do desempenho, da estabilidade, do uso e da segurança dos Serviços e dos componentes relacionados. O cliente não pode bloquear ou interferir nesse monitoramento. A Citrix pode complementar os logs com informações coletadas de terceiros para os fins especificados acima. Os logs podem ser usados para fins não especificados neste Anexo somente de forma agregada.
Continuidade dos Negócios e Recuperação de Desastres	**Backups.** Exceto onde indicado de outra forma na respectiva Descrição de Serviços, os Serviços são mantidos em clusters ativo-ativo de alta disponibilidade que abrangem vários sites físicos. Os sistemas que não são mantidos em uma configuração ativa-ativa são salvos em backup de acordo com as Metas de Nível específicas do Serviço.

Artigo 2. **Tratamento de Dados Pessoais**

Dados pessoais são informações sobre um indivíduo identificado ou identificável. O Cliente determina os dados pessoais que são incluídos no Conteúdo do Cliente. Ao executar os Serviços, a Citrix atua como um processador de dados e o Cliente continua sendo o controlador de dados de todos e quaisquer dados pessoais contidos no Conteúdo do Cliente. A Citrix agirá de acordo com as instruções do Cliente em relação ao processamento de tais dados pessoais, conforme especificado no Contrato.

Mais informações sobre o tratamento de dados pessoais sujeitos ao Regulamento Geral sobre a Proteção de Dados (GDPR), incluindo os mecanismos utilizados para a transferência internacional de tais dados, são fornecidas no Anexo I, Termos Gerais de Regulamentação de Proteção de Dados.

Artigo 3. Localização dos Serviços

O Conteúdo do Cliente pode ser transferido, armazenado e/ou processado nos Estados Unidos ou em outros países onde a Citrix e/ou seus provedores de serviços operam. Os requisitos deste Anexo continuam a ser aplicáveis, independentemente de onde a Citrix armazena ou processa o Conteúdo do Cliente.

As partes podem negociar de boa fé quaisquer contratos adicionais de processamento de dados ou transferência de dados necessários para facilitar a transferência legal de dados internacionalmente, em razão do fornecimento dos Serviços pela Citrix.

Artigo 4. Divulgação do Conteúdo do Cliente

O cliente concorda com a divulgação do Conteúdo do Cliente pela Citrix, conforme estabelecido nesta seção.
A Citrix pode usar subcontratados e agentes para executar os Serviços. Todos os subcontratados e agentes terão o direito de acessar o Conteúdo do Cliente somente na forma e extensão necessárias para executar os Serviços e deverão estar vinculados por contratos escritos que exijam que eles forneçam pelo menos o nível de proteção de dados exigido pela Citrix neste Anexo, conforme aplicável. A Citrix permanece responsável, em todos os momentos, pela conformidade de seus subcontratados e agentes com os termos do Contrato, conforme aplicável.

A Citrix também pode divulgar o Conteúdo do Cliente para (a) entidades afiliadas, para fins consistentes com o Contrato; (b) em razão de fusão, aquisição, venda, falência ou outra reorganização prevista ou real de alguns ou de todos os seus negócios, sujeita à obrigação de proteger o Conteúdo do Cliente de acordo com os termos do Contrato; ou (c) para fins legais, incluindo o cumprimento de seus direitos, a detecção e prevenção de fraude, a proteção contra danos aos direitos ou à propriedade da Citrix, dos Clientes, dos Usuários ou do público; e (c) conforme exigido por lei, inclusive em resposta a uma intimação, ordem judicial ou administrativa, ou outro instrumento vinculativo ("Demanda"). Salvo quando a lei proibir, a Citrix notificará imediatamente o Cliente sobre qualquer Demanda e fornecerá ao Cliente a assistência razoavelmente necessária para que ele responda à Demanda em tempo hábil.

Artigo 5. Obrigações do Cliente

1. Disposições Gerais. O Cliente pode usar e acessar os Serviços somente conforme permitido pelo Contrato. O Cliente cumprirá todas as legislações aplicáveis a ele relacionadas ao uso dos Serviços.

2. Permissões. O Cliente é responsável por obter todas as permissões necessárias para a Citrix executar os Serviços, incluindo fornecer eventuais avisos e obter eventuais autorizações ou licenças necessários para que a Citrix acesse e processe o Conteúdo do Cliente, conforme estabelecido neste Anexo.

3. Conformidade Regulatória. O Cliente é responsável por determinar se o Conteúdo do Cliente está sujeito a requisitos adicionais de regulamentação ou segurança além daqueles especificados no Contrato, incluindo este Anexo. O Cliente não deve enviar ou armazenar qualquer Conteúdo do Cliente regido pela regulamentação dos EUA sobre comércio internacional de armas (International Traffic in Arms Regulations — ITAR) ou regulamentos semelhantes de qualquer país que restrinjam a importação ou exportação de artigos ou serviços de defesa. Além

disso, o Cliente não fornecerá nem armazenará qualquer Conteúdo do Cliente sujeito a requisitos regulamentares adicionais, como informações de saúde protegidas ("PHI"), informações de cartão de pagamento ("PCI") ou dados de distribuição controlada nos termos de normas governamentais, salvo quando especificado no Pedido do Cliente e na Descrição de Serviço aplicável e se as partes tiverem firmado contratos adicionais (como Contrato de Parceiro Comercial (BAA)) com antecedência, conforme for necessário para que a Citrix processe tais dados. Os clientes do serviço ShareFile podem entrar em contato com a Citrix pelo email privacy@sharefile.com para solicitar um BAA.

4. Ambiente de Segurança do Cliente. Os Serviços foram desenvolvidos para serem fornecidos somente dentro de um ambiente de segurança maior do Cliente. O Cliente deve garantir a funcionalidade de segurança adequada para todos os componentes não gerenciados de forma expressa pela Citrix, incluindo, entre outros, controles de acesso, firewalls, aplicativos e redes, usados em conjunto com os Serviços. Consulte a Seção 1.A., Obrigações de Segurança do Cliente, acima.

5. Notificação de Segurança. O Cliente é responsável por notificar a Citrix imediatamente sobre todo e qualquer incidente de segurança que envolva os Serviços e/ou o Conteúdo do Cliente, conforme descrito no Artigo VI, Contatos da Citrix, abaixo.

6. Conformidade do Usuário. O cliente é responsável pela conformidade de seus Usuários com os termos do Pedido e do Contrato.

Artigo 6. Contatos da Citrix

FUNÇÃO	CONTATO
Atendimento ao Cliente	https://www.citrix.com/contact/technical-support.html
Relatar um incidente	secure@citrix.com
Vulnerabilidades suspeitas em produtos da Citrix	secure@citrix.com

Artigo 7. Definições

Os termos em maiúsculas no Anexo terão o significado especificado no Contrato ou abaixo. No caso de conflito entre os demais termos do Contrato e qualquer definição abaixo, a definição abaixo será aplicada a este Anexo.

Conteúdo do Cliente significa todos os dados carregados para armazenamento na conta do Cliente ou os dados contidos no ambiente de processamento do Cliente ao qual foi concedido acesso à Citrix para executar os Serviços.

Log significa um registro de eventos relacionados aos Serviços, incluindo registros que medem o desempenho, a estabilidade, o uso, a segurança e o suporte.

Incidente de Segurança significa acesso não autorizado ao Conteúdo do Cliente, resultando na perda de confidencialidade, integridade ou disponibilidade.